Guida per l'amministratore

AWS Client VPN

AWS Client VPN: Guida per l'amministratore

Table of Contents

Che cos'è AWS Client VPN?

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

Argomenti

Caratteristiche del client VPN

Client VPN offre le seguenti caratteristiche e funzionalità:

- Connessioni sicure: fornisce una TLS connessione sicura da qualsiasi posizione utilizzando il VPN client Open.
- Servizio gestito: è un servizio AWS gestito, quindi elimina l'onere operativo dell'implementazione e della gestione di una VPN soluzione di accesso remoto di terze parti.
- Disponibilità ed elasticità elevate: si adatta automaticamente al numero di utenti che si connettono alle tue AWS risorse e alle risorse locali.
- Autenticazione: supporta l'autenticazione client utilizzando Active Directory, l'autenticazione federata e l'autenticazione basata su certificati.
- Controllo granulare: consente di implementare controlli di sicurezza personalizzati tramite la definizione di regole di accesso di rete. Tali regole possono essere configurate a livello di gruppi di Active Directory. Puoi implementare il controllo degli accessi anche utilizzando i gruppi di sicurezza.
- Facilità d'uso: consente di accedere alle AWS risorse e alle risorse locali utilizzando un unico tunnel. VPN

- Gestibilità: consente di visualizzare i log di connessione che forniscono informazioni sui tentativi di connessione dei client. Puoi inoltre gestire le connessioni client attive con la possibilità di terminarle.
- Integrazione profonda: si integra con i AWS servizi esistenti, tra cui AWS Directory Service AmazonVPC.

Componenti del client VPN

Di seguito sono riportati i concetti chiave per ClientVPN:

VPNEndpoint del client

L'VPNendpoint Client è la risorsa creata e configurata per abilitare e gestire le sessioni clientVPN. È il punto di terminazione per tutte le sessioni clientVPN.

Rete target

Una rete di destinazione è la rete associata a un VPN endpoint Client. Una sottorete di a VPC è una rete di destinazione. L'associazione di una sottorete a un VPN endpoint Client consente di stabilire sessioni. VPN È possibile associare più sottoreti a un endpoint Client VPN per un'elevata disponibilità. Tutte le sottoreti devono provenire dalla stessa. VPC Ogni sottorete deve appartenere a una zona di disponibilità diversa.

Route

Ogni VPN endpoint Client dispone di una tabella di routing che descrive le rotte di rete di destinazione disponibili. 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

L'utente finale che si connette all'VPNendpoint Client per stabilire una VPN sessione. Gli utenti finali devono scaricare un VPN client Open e utilizzare il file di VPN configurazione del client creato per stabilire una VPN sessione.

CIDRIntervallo di client

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

VPNPorte client

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

Interfacce di rete client VPN

Quando associ una sottorete all'VPNendpoint Client, creiamo interfacce di VPN rete Client in quella sottorete. Il traffico inviato all'VPNendpoint Client viene inviato tramite un'interfaccia di rete Client. VPC VPN Viene quindi applicata la traduzione dell'indirizzo di rete di origine (SNAT), in cui l'indirizzo IP di origine dell'CIDRintervallo di client viene tradotto nell'indirizzo IP dell'interfaccia di VPN rete del client.

Registrazione delle connessioni

È possibile abilitare la registrazione della connessione per l'VPNendpoint Client per registrare gli eventi di connessione. È possibile utilizzare queste informazioni per eseguire analisi forensi, analizzare come viene utilizzato l'VPNendpoint Client o risolvere problemi di connessione.

Portale self-service

Client VPN fornisce un portale self-service come pagina Web agli utenti finali per scaricare la versione più recente di AWS VPN Desktop Client e l'ultima versione del file di configurazione dell'VPNendpoint Client, che contiene le impostazioni necessarie per connettersi al proprio endpoint. L'amministratore dell'VPNendpoint Client può abilitare o disabilitare il portale self-service per l'endpoint Client. VPN 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 (Stati Uniti occidentali). AWS GovCloud

Lavorare con il cliente VPN

Puoi lavorare con Client VPN in uno dei seguenti modi:

AWS Management Console

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

AWS Command Line Interface (AWS CLI)

AWS CLI Fornisce l'accesso diretto al VPN pubblico del ClienteAPIs. 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 ClientVPN, vedere AWS CLI Command 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 ClientVPN, vedere la Guida di riferimento ai cmdlet.AWS Tools for Windows PowerShell

Query API

Client VPN HTTPS Query API consente l'accesso programmatico a Client VPN e AWS. La HTTPS Query API consente di inviare HTTPS richieste direttamente al servizio. Quando si utilizza il HTTPSAPI, è necessario includere il codice per firmare digitalmente le richieste utilizzando le proprie credenziali. Per ulteriori informazioni, consulta Operazioni di AWS Client VPN.

Prezzi per il cliente VPN

Ti viene addebitato un costo per ogni associazione di endpoint e ogni VPN connessione su base oraria. Per ulteriori informazioni, consulta 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 VPN endpoint Client, 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 abiliti il gestore di connessione client per l'VPNendpoint Client, devi creare e richiamare una funzione Lambda. Per richiamare le funzioni Lambda sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di AWS Lambda.

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

Regole e best practice per l'utilizzo AWS Client VPN

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

- È supportata una larghezza di banda minima di 10 Mbps per connessione utente. La larghezza di banda massima per connessione utente dipende dal numero di connessioni effettuate all'endpoint Client. VPN
- CIDRGli intervalli CIDR di client non possono sovrapporsi a quelli locali VPC in cui si trova la sottorete associata o a qualsiasi route aggiunta manualmente alla tabella di routing dell'VPNendpoint Client.
- CIDRGli intervalli di client devono avere una dimensione del blocco di almeno /22 e non devono essere superiori a /12.
- Una parte degli indirizzi nell'CIDRintervallo di client viene utilizzata per supportare il modello di disponibilità dell'VPNendpoint Client e non può essere assegnata ai client. Pertanto, ti consigliamo di assegnare un CIDR blocco che contenga il doppio del numero di indirizzi IP necessari per abilitare il numero massimo di connessioni simultanee che intendi supportare sull'endpoint Client. VPN
- L'CIDRintervallo di client non può essere modificato dopo aver creato l'endpoint Client. VPN
- Le sottoreti associate a un VPN endpoint Client devono trovarsi nella stessa. VPC
- Non è possibile associare più sottoreti della stessa zona di disponibilità a un endpoint Client. VPN
- Un VPN endpoint Client non supporta le associazioni di sottoreti in una locazione dedicata. VPC
- Il client VPN supporta solo il trafficoIPv4. Vedi IPv6considerazioni per AWS Client VPN per i dettagli riguardantiIPv6.
- Il cliente non VPN è conforme ai Federal Information Processing Standards (FIPS).
- Il portale self-service non è disponibile per i client che eseguono l'autenticazione reciproca.

- Non è consigliabile connettersi a un VPN endpoint Client utilizzando indirizzi IP. Poiché Client VPN è un servizio gestito, occasionalmente si verificheranno cambiamenti negli indirizzi IP a cui viene risolto il DNS nome. Inoltre, vedrai le interfacce di VPN rete Client eliminate e ricreate nei tuoi registri. CloudTrail Ti consigliamo di connetterti all'VPNendpoint del Client utilizzando il nome fornito. DNS
- L'inoltro IP non è attualmente supportato quando si utilizza l' AWS Client VPN applicazione desktop. L'inoltro IP è supportato da altri client.
- Il client VPN non supporta la replica multiregionale in. AWS Managed Microsoft AD L'VPNendpoint del client deve trovarsi nella stessa regione della risorsa. AWS Managed Microsoft AD
- Se l'autenticazione a più fattori (MFA) è disabilitata per Active Directory, le password degli utenti non possono utilizzare il seguente formato.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Non è possibile stabilire una VPN connessione da un computer se ci sono più utenti connessi al sistema operativo.
- Il VPN servizio Client richiede che l'indirizzo IP a cui è connesso il client corrisponda all'IP a cui viene risolto il DNS nome dell'VPNendpoint Client. In altre parole, se si imposta un DNS record personalizzato per l'VPNendpoint Client e quindi si inoltra il traffico all'indirizzo IP effettivo su cui viene risolto il DNS nome 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
- Il VPN servizio Client 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`, o`169.254.0.0/16`. Se viene rilevato che l'intervallo di LAN indirizzi del client non rientra negli intervalli precedenti, l'VPNendpoint Client invierà automaticamente la VPN direttiva Open «redirect-gateway block-local» al client, forzando tutto il traffico a entrare in. LAN VPN Pertanto, se hai bisogno dell'LANaccesso durante VPN le connessioni, ti consigliamo di utilizzare gli intervalli di indirizzi convenzionali sopra elencati per il tuo. LAN Questa regola viene applicata per mitigare le possibilità di un attacco alla rete locale come descritto qui:. TunnelCrack

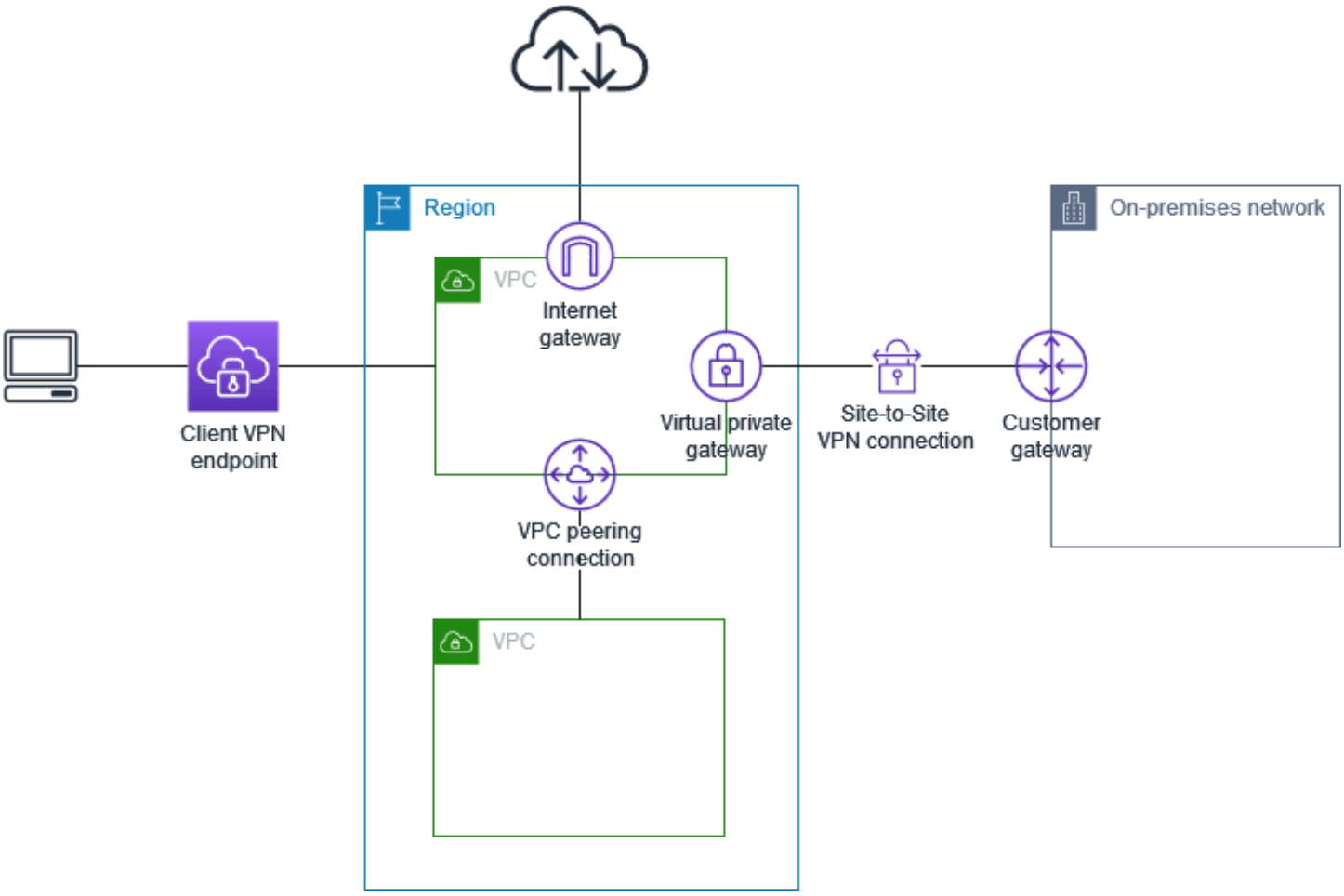
Come AWS Client VPN funziona

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

L'amministratore è responsabile dell'impostazione e della configurazione del servizio. Ciò comporta la creazione dell'VPNendpoint Client, l'associazione della rete di destinazione, la configurazione delle regole di autorizzazione e l'impostazione di percorsi aggiuntivi (se necessario). Dopo aver impostato e configurato l'VPNendpoint Client, l'amministratore scarica il file di configurazione dell'VPNendpoint Client e lo distribuisce ai client che devono accedervi. Il file di configurazione dell'VPNendpoint Client include il DNS nome dell'VPNendpoint Client 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. Questa è la persona che si connette all'VPNendpoint Client per stabilire una sessione. VPN Il client stabilisce la VPN sessione dal proprio computer locale o dispositivo mobile utilizzando un'applicazione VPN client VPN basata su Open. Dopo aver stabilito la VPN sessione, può accedere in modo sicuro alle risorse VPC in cui si trova la sottorete associata. Possono inoltre 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 VPN endpoint Client per stabilire una VPN sessione, consulta la Guida introduttiva nella Guida per l'AWS Client VPN utente.

L'immagine seguente illustra l'architettura Client VPN di base.



Scenari ed esempi per il cliente VPN

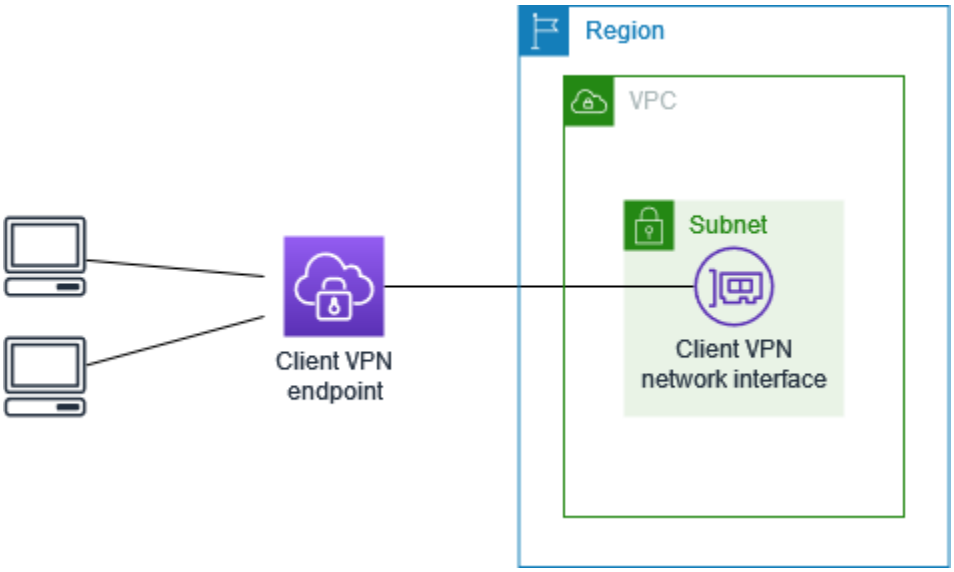
AWS Client VPN è una VPN soluzione di accesso remoto completamente gestita che viene utilizzata per consentire ai client l'accesso sicuro alle risorse sia AWS all'interno della rete locale che a quella locale. Esistono diverse opzioni per la configurazione dell'accesso. Questa sezione fornisce esempi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

Scenari

- the section called “Accedi a VPC”
- the section called “Accedi a un peer VPC”
- 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”

Accedi a un client VPC che utilizza VPN

La AWS Client VPN configurazione per questo scenario include una singola destinazioneVPC. Consigliamo questa configurazione se è necessario consentire ai client l'accesso alle risorse all'interno di una VPC sola configurazione.



Prima di iniziare, esegui queste attività:

- Crea o identifica un VPC file con almeno una sottorete. Identifica la sottorete VPC da associare all'VPNendpoint Client e annotane gli intervalli. IPv4 CIDR
- Identifica un CIDR intervallo adatto per gli indirizzi IP del client che non si sovrapponga a. VPC CIDR
- Rivedi le regole e le limitazioni per gli VPN endpoint del client in. Regole e best practice per l'utilizzo AWS Client VPN

Per implementare questa configurazione

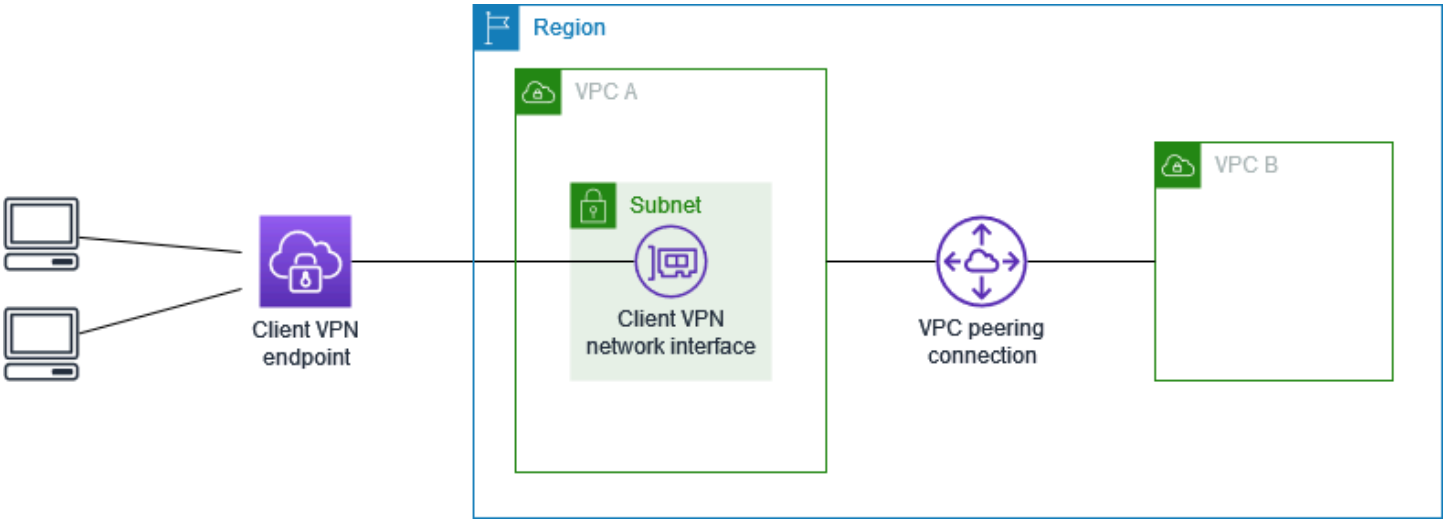
1. Crea un VPN endpoint Client nella stessa regione di. VPC Per eseguire questa operazione, attieniti alla procedura descritta in Creare un AWS Client VPN endpoint.
2. Associa la sottorete all'endpoint ClientVPN. A tale scopo, esegui i passaggi descritti in Associare una rete di destinazione a un AWS Client VPN endpoint e seleziona la sottorete e la sottorete VPC identificate in precedenza.
3. Aggiungere una regola di autorizzazione per consentire ai clienti di accedere a. VPC A tale scopo, eseguire i passaggi descritti inAggiungere una regola di autorizzazione, e per Rete di destinazione, immettere l'IPv4CIDRintervallo diVPC.

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.

Accedi a un client VPC peer-to-peer VPN

La AWS Client VPN configurazione per questo scenario include un target VPC (VPCA) che viene peerizzato con un altro VPC (VPCB). Si consiglia questa configurazione se è necessario consentire ai client l'accesso alle risorse all'interno di una destinazione VPC e ad altre risorse VPCs che la utilizzano in peering (come VPC B).

> **Note**
>
> La procedura per consentire l'accesso a un dispositivo peered VPC (descritta nel diagramma di rete) è necessaria solo se l'VPNendpoint Client è stato configurato per la modalità split-tunnel. In modalità full-tunnel, l'accesso al peered è consentito per impostazione predefinita. VPC



Prima di iniziare, esegui queste attività:

- Crea o identifica un file VPC con almeno una sottorete. Identifica la sottorete VPC da associare all'VPNendpoint Client e annotane gli intervalli. IPv4 CIDR
- Identifica un CIDR intervallo adatto per gli indirizzi IP del client che non si sovrapponga a. VPC CIDR

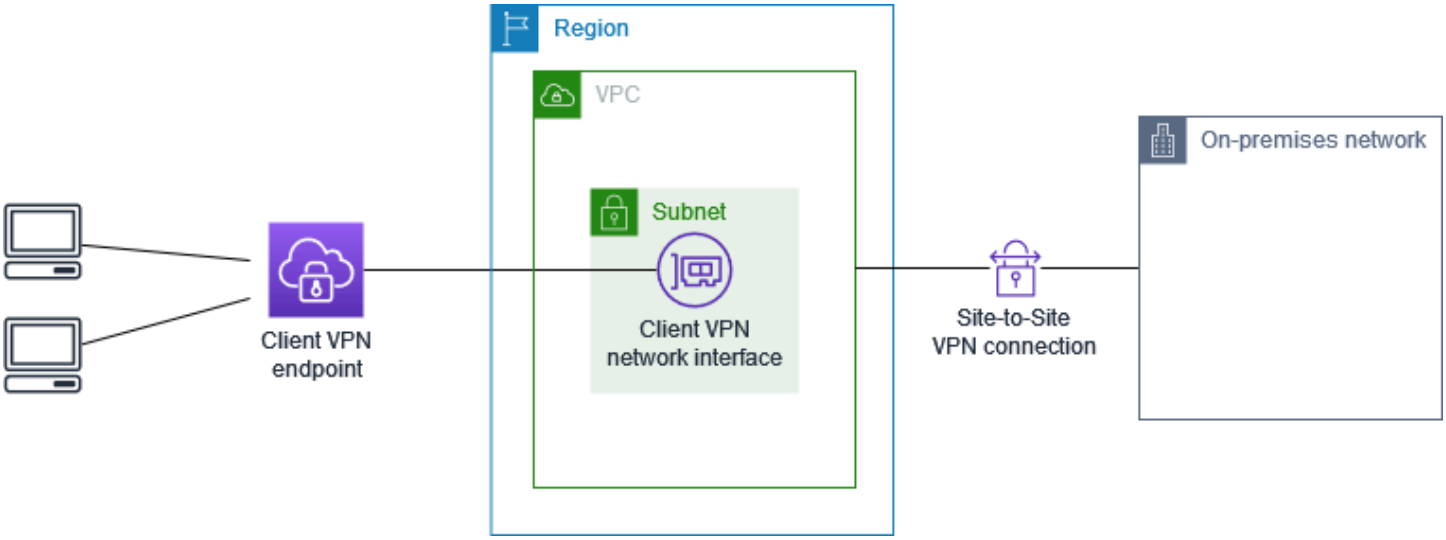
- Rivedi le regole e le limitazioni per gli VPN endpoint del client in. Regole e best practice per l'utilizzo AWS Client VPN

Per implementare questa configurazione

1. Stabilisci la connessione VPC di peering tra. VPCs Segui i passaggi indicati in Creare e accettare una connessione VPC peering nella Amazon VPC Peering Guide. Verifica che le istanze in VPC A possano comunicare con le istanze in VPC B utilizzando la connessione peering.
2. Crea un VPN endpoint Client nella stessa regione della destinazione. VPC Nel diagramma, si tratta di VPC A. Eseguire i passaggi descritti in. Creare un AWS Client VPN endpoint
3. Associate la sottorete che avete identificato all'VPNendpoint Client che avete creato. A tale scopo, esegui i passaggi descritti inAssociare una rete di destinazione a un AWS Client VPN endpoint, selezionando la sottorete VPC e. Per impostazione predefinita, associamo il gruppo di sicurezza predefinito di VPC all'VPNendpoint Client. 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. Aggiunge una regola di autorizzazione per consentire ai client di accedere alla destinazioneVPC. Per eseguire questa operazione, attieniti alla procedura descritta in Aggiungere una regola di autorizzazione. Per abilitare la rete di destinazione, inserisci l'IPv4CIDRintervallo diVPC.
5. Aggiungi un percorso per indirizzare il traffico verso il peer. VPC Nel diagramma, questo è VPC B. A tale scopo, eseguire i passaggi descritti in. Crea un percorso AWS Client VPN endpoint Per la destinazione del percorso, inserisci l'IPv4CIDRintervallo del percorso VPC peered. Per Target VPC Subnet ID, seleziona la sottorete associata all'endpoint Client. VPN
6. Aggiungi una regola di autorizzazione per consentire ai clienti l'accesso al peered. VPC Per eseguire questa operazione, attieniti alla procedura descritta in Aggiungere una regola di autorizzazione. Per la rete di destinazione, inserisci l'IPv4CIDRintervallo del VPC peered.
7. Aggiungi una regola ai gruppi di sicurezza per le tue istanze in VPC A e VPC B per consentire il traffico proveniente dal gruppo di sicurezza a cui è stato applicato l'VPNendpoint Client nel passaggio 3. Per ulteriori informazioni, consulta Gruppi di sicurezza.

Accedi a una rete locale 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:

- Crea o identifica una VPC con almeno una sottorete. Identifica la sottorete VPC da associare all'VPNendpoint Client e annotane gli intervalli. IPv4 CIDR
- Identifica un CIDR intervallo adatto per gli indirizzi IP del client che non si sovrapponga a. VPC CIDR
- Rivedi le regole e le limitazioni per gli VPN endpoint del client in. Regole e best practice per l'utilizzo AWS Client VPN

Per implementare questa configurazione

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

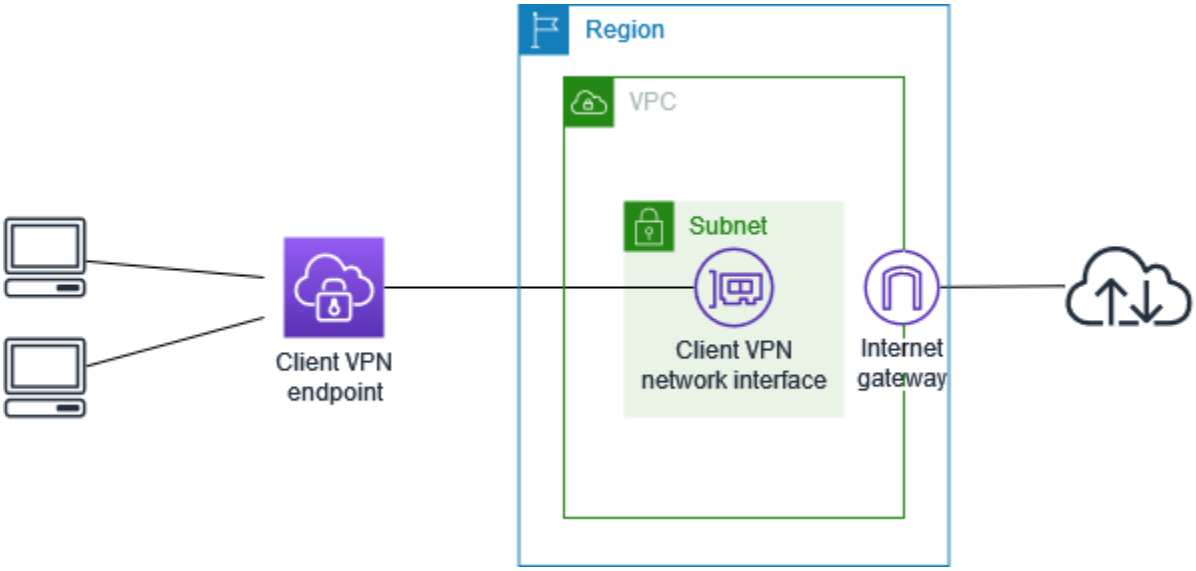
> **Note**
>
> In alternativa, puoi implementare questo scenario utilizzando una AWS Direct Connect connessione tra la tua rete VPC e quella locale. Per ulteriori informazioni, consulta la Guida per l'utente AWS Direct Connect.

2. Verifica la VPN connessione AWS da sito a sito creata nel passaggio precedente. A tale scopo, esegui i passaggi descritti in Verifica della connessione da sito a sito nella Guida per l'utente VPN.AWS Site-to-Site VPN Se la VPN connessione funziona come previsto, procedi con il passaggio successivo.
3. Crea un VPN endpoint client nella stessa regione diVPC. Per eseguire questa operazione, attieniti alla procedura descritta in Creare un AWS Client VPN endpoint.
4. Associate la sottorete identificata in precedenza all'endpoint ClientVPN. A tale scopo, esegui i passaggi descritti in Associare una rete di destinazione a un AWS Client VPN endpoint e seleziona la VPC sottorete.
5. Aggiungi un percorso che consenta l'accesso alla connessione da AWS sito a sitoVPN. A tale scopo, esegui i passaggi descritti inCrea un percorso AWS Client VPN endpoint: per Route destination, inserisci l'IPv4CIDRintervallo della VPN connessione AWS da sito a sito 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 da sito a sito. AWS VPN A tale scopo, esegui i passaggi descritti inAggiungere una regola di autorizzazione a un AWS Client VPN endpoint; per Rete di destinazione, immettete l'intervallo di connessione da sito a AWS sitoVPN. IPv4 CIDR

Accedi a Internet utilizzando Client VPN

La AWS Client VPN configurazione per questo scenario include una singola destinazione VPC e l'accesso a Internet. Consigliamo questa configurazione se è necessario consentire ai client l'accesso alle risorse all'interno di un singolo target VPC 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:

- Crea o identifica un VPC file con almeno una sottorete. Identifica la sottorete VPC da associare all'VPNendpoint Client e annotane gli intervalli. IPv4 CIDR
- Identifica un CIDR intervallo adatto per gli indirizzi IP del client che non si sovrapponga a. VPC CIDR
- Rivedi le regole e le limitazioni per gli VPN endpoint del client in. Regole e best practice per l'utilizzo AWS Client VPN

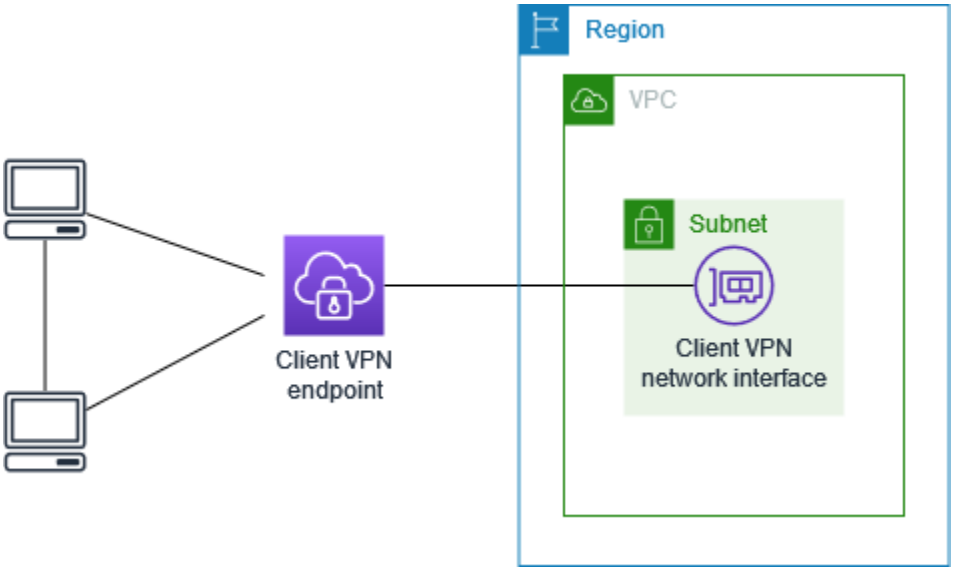
Per implementare questa configurazione

1. Assicurati che il gruppo di sicurezza che utilizzerai per l'VPNendpoint Client consenta il traffico in uscita verso Internet. A tale scopo, aggiungi regole in uscita che consentano il traffico fino a 0.0.0.0/0 per il traffico. HTTP HTTPS
2. Crea un gateway Internet e collegalo al tuo. VPC Per ulteriori informazioni, consulta Creare e collegare un Internet Gateway nella Amazon VPC User Guide.
3. Rendere pubblica la sottorete aggiungendo una route al gateway Internet per instradare la tabella di routing. Nella VPC console, scegli Subnet, seleziona la sottorete che intendi associare all'VPNendpoint Client, scegli Route Table, 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 VPN endpoint Client nella stessa regione del. VPC Per eseguire questa operazione, attieniti alla procedura descritta in Creare un AWS Client VPN endpoint.

5. Associate la sottorete identificata in precedenza all'endpoint ClientVPN. A tale scopo, esegui i passaggi descritti in Associare una rete di destinazione a un AWS Client VPN endpoint e seleziona la VPC sottorete.
6. Aggiungere una regola di autorizzazione per consentire ai clienti di accedere a. VPC A tale scopo, esegui i passaggi descritti inAggiungere una regola di autorizzazione; e per abilitare la rete di destinazione, inserisci l'IPv4CIDRintervallo diVPC.
7. Aggiungere una route che consenta il traffico verso Internet. A tale scopo, esegui i passaggi descritti inCrea un percorso AWS Client VPN endpoint: per Route destination, inserisci e`0.0.0.0/0`, per Target VPC Subnet ID, seleziona la sottorete associata all'endpoint ClientVPN.
8. Aggiungere una regola di autorizzazione per concedere ai client l'accesso a Internet. Per eseguire questa operazione attieniti alla procedura descritta in Aggiungere una regola di autorizzazione. Per Destination network (Rete di destinazione) immetti `0.0.0.0/0`.
9. Assicurati che i gruppi di sicurezza per le risorse del tuo computer VPC abbiano una regola che consenta l'accesso dal gruppo di sicurezza associato all'endpoint Client. VPN Ciò consente ai tuoi clienti di accedere alle risorse del tuoVPC.

lient-to-client Accesso C tramite Client VPN

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



Prima di iniziare, esegui queste attività:

- Crea o identifica un VPC con almeno una sottorete. Identifica la sottorete VPC da associare all'VPNendpoint Client e annotane gli intervalli. IPv4 CIDR
- Identifica un CIDR intervallo adatto per gli indirizzi IP del client che non si sovrapponga a. VPC CIDR
- Rivedi le regole e le limitazioni per gli VPN endpoint del client in. Regole e best practice per l'utilizzo AWS Client VPN

> **Note**
>
> Le regole di autorizzazione basate sulla rete che utilizzano gruppi Active Directory o gruppi SAML IdP basati su Active Directory non sono supportate in questo scenario.

Per implementare questa configurazione

1. Crea un VPN endpoint Client nella stessa regione di. VPC Per eseguire questa operazione, attieniti alla procedura descritta in Creare un AWS Client VPN endpoint.
2. Associate la sottorete identificata in precedenza all'endpoint ClientVPN. A tale scopo, esegui i passaggi descritti in Associare una rete di destinazione a un AWS Client VPN endpoint e seleziona la VPC 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 Route destination, inserisci l'CIDRintervallo di client e, per Target VPC Subnet ID, specifica. `local`
4. Aggiungi una regola di autorizzazione per consentire ai clienti di accedere a. VPC Per eseguire questa operazione, attieniti alla procedura descritta in Aggiungere una regola di autorizzazione. Per abilitare la rete di destinazione, inserisci l'IPv4CIDRintervallo diVPC.
5. Aggiungi una regola di autorizzazione per consentire ai client di accedere all'CIDRintervallo di client. Per eseguire questa operazione, attieniti alla procedura descritta in Aggiungere una regola di autorizzazione. Per abilitare la rete di destinazione, inserisci l'CIDRintervallo di client.

Limita l'accesso alla tua rete utilizzando Client VPN

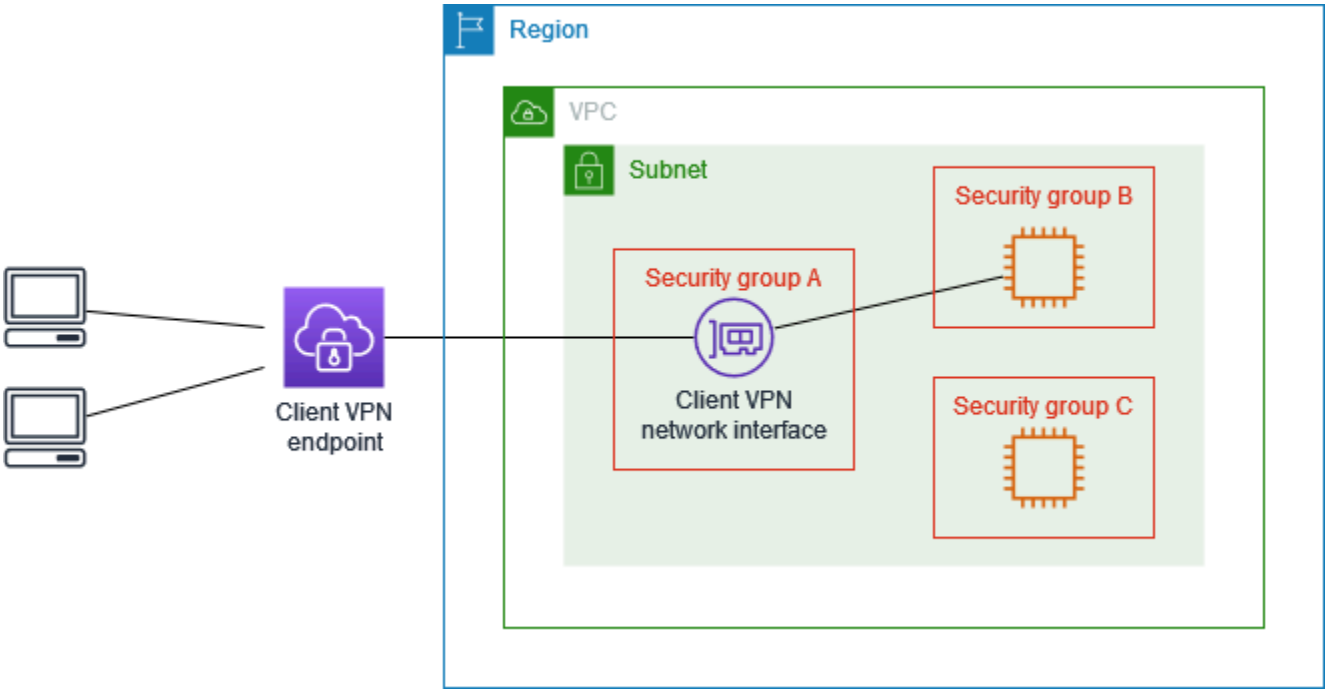
Puoi configurare il tuo AWS Client VPN endpoint per limitare l'accesso a risorse specifiche del tuoVPC. Per l'autenticazione basata sull'utente, puoi anche limitare l'accesso a parti della rete, in base al gruppo di utenti che accede all'endpoint Client. VPN

Limitare l'accesso utilizzando i gruppi di sicurezza

È possibile concedere o negare l'accesso a risorse specifiche della rete aggiungendo o rimuovendo le regole del gruppo di sicurezza che fanno riferimento al gruppo di sicurezza applicato all'associazione di rete di destinazione (il gruppo di sicurezza ClientVPN). VPC Questa configurazione espande lo scenario illustrato i Accedi a un client VPC che utilizza 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 consenta il traffico proveniente dal gruppo di VPN sicurezza Client.

Nel diagramma seguente, il gruppo di sicurezza A è il gruppo di VPN sicurezza Client, il gruppo di sicurezza B è associato a un'EC2istanza e il gruppo di sicurezza C è associato a un'EC2istanza. 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 VPN di sicurezza Client è associato ad altre risorse del tuoVPC. Se aggiungi o rimuovi regole che fanno riferimento al gruppo VPN di sicurezza Client, puoi concedere o negare l'accesso anche alle altre risorse associate. Per evitare che ciò accada, utilizzate un gruppo di sicurezza creato appositamente per l'uso con l'VPNendpoint Client.

Per creare una regola per il gruppo di sicurezza

1. Apri la VPC console Amazon 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.
   - Per Origine, scegli Personalizzato, quindi inserisci o scegli l'ID del gruppo di VPN sicurezza Client.
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 proveniente dal gruppo VPN di sicurezza Client, eliminala.

Per verificare le regole del gruppo di sicurezza

1. Apri la VPC console Amazon 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 è il gruppo di VPN sicurezza Client, scegli Modifica regole e scegli Elimina (l'icona x) come regola. Scegliere Salva regole.

Limitare l'accesso in base ai gruppi di utenti

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

1. Configura utenti e gruppi nel AWS 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 SAML
2. Crea una regola di autorizzazione per l'VPNendpoint Client che consenta a un gruppo specifico di accedere a tutta o parte della tua rete. Per ulteriori informazioni, consulta AWS Client VPN regole di autorizzazione.

Se l'VPNendpoint Client è configurato per l'autenticazione reciproca, non è possibile configurare 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, è possibile creare più VPN endpoint Client. 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 VPN endpoint Client. 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 VPN endpoint Client utilizzato dagli amministratori, è possibile creare una regola di autorizzazione che garantisca l'accesso all'intera rete. Per ulteriori informazioni, consulta Aggiungere una regola di autorizzazione.

Autenticazione client in AWS Client VPN

L'autenticazione del client viene implementata al primo punto di ingresso nel AWS Cloud. Viene utilizzata per determinare se i client sono autorizzati a connettersi all'VPNendpoint Client. Se l'autenticazione ha esito positivo, i client si connettono all'VPNendpoint Client e stabiliscono una sessione. VPN Se l'autenticazione fallisce, la connessione viene negata e al client viene impedito di stabilire una sessione. VPN

Il 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 SAML basata) (basata sull'utente)

È possibile utilizzare solo uno dei metodi precedenti oppure è possibile 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 VPN endpoint Client, 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.

Autenticazione Active Directory in Client VPN

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

Il client VPN supporta l'autenticazione a più fattori (MFA) quando è abilitata per AWS Managed Microsoft AD o AD Connector. Se MFA è abilitata, i client devono inserire un nome utente, una password e un MFA codice quando si connettono a un VPN endpoint Client. Per ulteriori informazioni sull'attivazioneMFA, consulta Enable Multi-Factor Authentication for AWS Managed Microsoft AD e Enable Multi-Factor Authentication for AD Connector nella AWS Directory Service Administration Guide.

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 il client e il 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'VPNendpoint Client. 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 ClientVPN. Quando si carica il certificato del server suACM, si specifica anche l'autorità di certificazione (CA). È necessario caricare il certificato client solo ACM quando la CA del certificato client è diversa dalla CA del certificato del server. Per ulteriori informazioni in meritoACM, consulta la Guida AWS Certificate Manager per l'utente.

È possibile creare un certificato e una chiave client separati per ogni client che si connetterà all'VPNendpoint Client. Questo consente di revocare un certificato client specifico se un utente lascia l'organizzazione. In questo caso, quando si crea l'VPNendpoint Client, è possibile specificare il

certificato server ARN per il certificato client, a condizione che il certificato client sia stato emesso dalla stessa CA del certificato server.

> **Note**
>
> Un VPN endpoint Client supporta solo chiavi di dimensioni pari a 1024 bit e RSA 2048 bit. Inoltre, il certificato client deve avere l'attributo CN nel campo Subject (Oggetto). Quando i certificati utilizzati con il VPN servizio Client vengono aggiornati, tramite ACM rotazione automatica, importazione manuale di un nuovo certificato o aggiornamenti dei metadati in IAM Identity Center, il VPN servizio Client aggiornerà automaticamente l'VPNendpoint Client con il certificato più recente. Questo è un processo automatizzato che può richiedere fino a 24 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 Linux/macOS o Windows.

Linux/macOS

La procedura seguente utilizza Open VPN easy-rsa per generare i certificati e le chiavi del server e del client, quindi carica il certificato e la chiave del server su. ACM Per ulteriori informazioni, vedere Easy - 3 Quickstart. RSA README

Per generare i certificati e le chiavi del server e del client e caricarli su ACM

1. Clona il repository Open VPN easy-rsa sul tuo computer locale e vai alla cartella. `easy-rsa/easyrsa3`

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

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

2. Inizializza 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 del server e il certificato e la chiave del client suACM. Assicurati di caricarli nella stessa regione in cui intendi creare l'VPNendpoint Client. I seguenti comandi utilizzano l'interfaccia a riga di comando di AWS CLI per caricare i certificati. Per caricare invece i certificati utilizzando la ACM console, consulta Importare un certificato nella Guida per l'AWS Certificate Manager utente.

```
$ 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 necessariamente il certificato client suACM. Se i certificati server e client sono stati emessi dalla stessa Autorità di Certificazione (CA), puoi utilizzare il certificato server sia ARN per il server che per il client quando crei l'VPNendpoint 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 RSA Easy-3.x e lo utilizza per generare certificati e chiavi per server e client.

Per generare certificati e chiavi server e client e caricarli su ACM

1. Apri la pagina Easy RSA releases e scarica il ZIP file per la 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. Esegui il seguente comando per aprire la shell Easy RSA 3.

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

4. Inizializza un nuovo PKI ambiente.

```
# ./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 Easy RSA 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 del server e il certificato e la chiave del client suACM. Assicurati di caricarli nella stessa regione in cui intendi creare l'VPNendpoint Client. I seguenti comandi utilizzano AWS CLI per caricare i certificati. Per caricare invece i certificati utilizzando la ACM console, consulta Importare un certificato nella Guida per l'AWS Certificate Manager utente.

```
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 necessariamente il certificato client suACM. Se i certificati server e client sono stati emessi dalla stessa Autorità di Certificazione (CA), puoi utilizzare il certificato server sia ARN per il server che per il client quando crei l'VPNendpoint 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 VPN server Client scaduto. A seconda della versione di Open VPN easy-rsa in uso, la procedura può variare. Per maggiori dettagli, consulta la documentazione per il rinnovo e la revoca dei certificati 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- versione 3.2.x RSA
     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 inACM. Assicurati di importarli nella stessa regione dell'VPNendpoint Client.

```
$ 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 2.0, in Client SAML VPN

AWS Client VPN supporta la federazione delle identità con Security Assertion Markup Language 2.0 (SAML2.0) per gli endpoint Client. VPN È possibile utilizzare provider di identità (IdPs) che supportano la SAML versione 2.0 per creare identità utente centralizzate. È quindi possibile configurare un VPN endpoint Client per utilizzare l'autenticazione federata SAML basata e associarlo all'IdP. Gli utenti si connettono quindi all'VPNendpoint Client utilizzando le proprie credenziali centralizzate.

Argomenti

Abilita SAML per AWS Client VPN

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

Per consentire al tuo IdP SAML basato di funzionare con un VPN endpoint Client, devi fare quanto segue.

1. Crea un'app SAML basata sull'IdP prescelto da utilizzare con AWS Client VPN o usa un'app esistente.
2. Configura il tuo IdP per stabilire una relazione di fiducia con AWS. Per le risorse, vediSAMLrisorse di configurazione IdP basate.
3. Nel provider di identità, generare e scaricare un documento di metadati della federazione che descrive l'organizzazione come un provider di identità.

   Questo XML documento firmato viene utilizzato per stabilire la relazione di fiducia tra AWS e l'IdP.
4. Crea un provider di IAM SAML identità nello stesso AWS account come VPN endpoint del client.

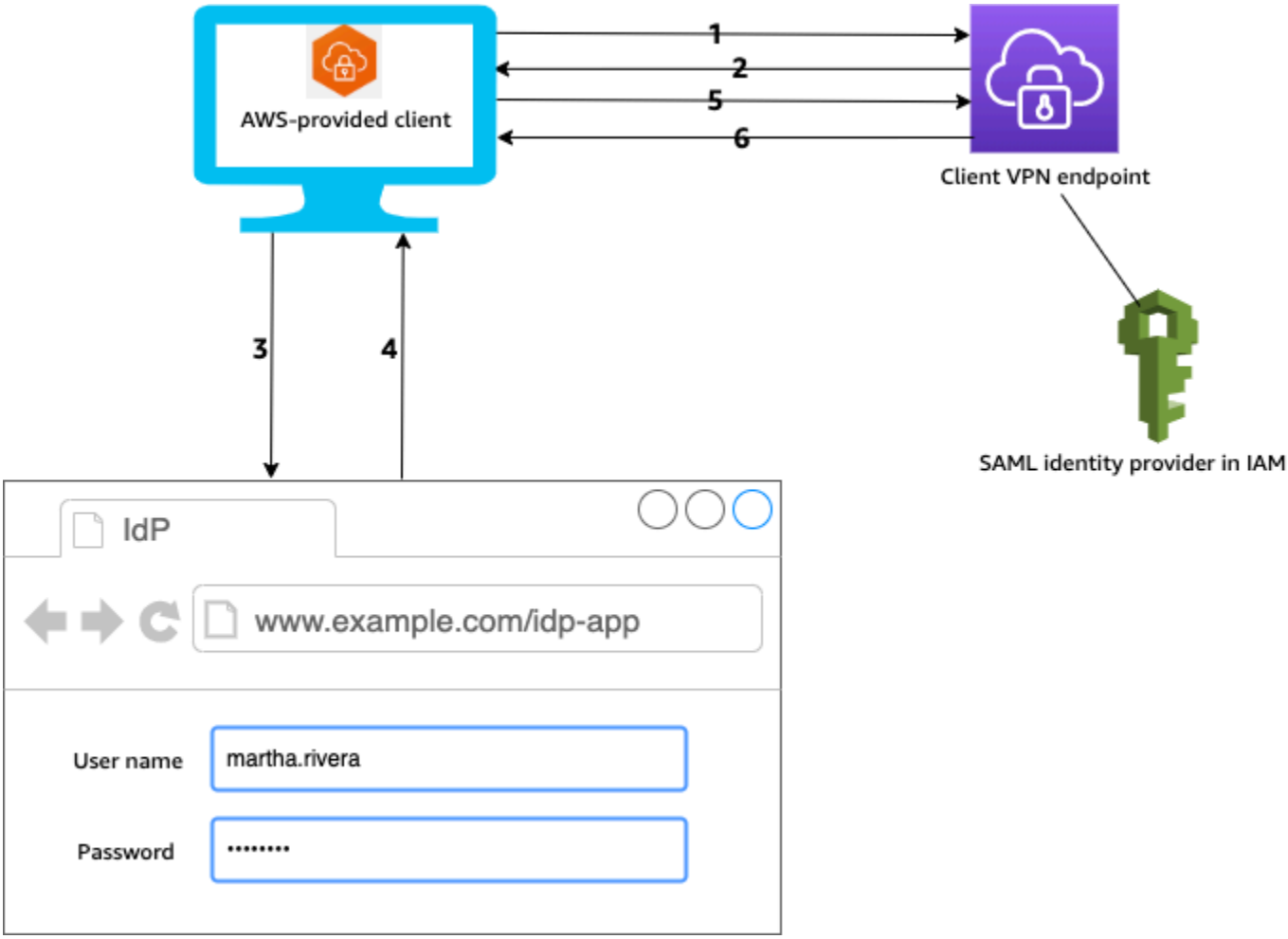
   Il provider di IAM SAML identità definisce l'IdP dell'organizzazione su AWS relazione di fiducia utilizzando il documento di metadati generato dall'IdP. Per ulteriori informazioni, consulta Creazione di provider di IAM SAML identità nella Guida per l'IAMutente. Se successivamente aggiorni la configurazione dell'app nell'IdP, genera un nuovo documento di metadati e aggiorna il tuo IAM SAML provider di identità.

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

   Specificate l'autenticazione federata come tipo di autenticazione e specificate il provider di IAM SAML identità che avete creato. Per ulteriori informazioni, consulta Creare un AWS Client VPN endpoint.
6. Esportare il file di configurazione del client e distribuirlo agli utenti. Chiedi ai tuoi utenti di scaricare la versione più recente di AWS client fornito e utilizzarlo per caricare il file di configurazione e connettersi all'VPNendpoint del client.

Flusso di lavoro di autenticazione

Il diagramma seguente fornisce una panoramica del flusso di lavoro di autenticazione per un VPN endpoint Client che utilizza l'autenticazione federata basata. SAML Quando si crea e si configura l'VPNendpoint Client, si specifica il provider di identità. IAM SAML



1. L'utente apre il client AWS fornito sul proprio dispositivo e avvia una connessione all'endpoint ClientVPN.
2. L'VPNendpoint Client invia un URL IdP e una richiesta di autenticazione al client, in base alle informazioni fornite IAM SAML nel provider di identità.
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 inserisce le proprie credenziali nella pagina di accesso e l'IdP invia un'asserzione SAML firmata al client.
5. Il client AWS fornito invia l'SAMLasserzione all'endpoint Client. VPN

6. L'VPNendpoint Client convalida l'asserzione e consente o nega l'accesso all'utente.

Requisiti e considerazioni per l'autenticazione federata basata SAML

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

- Per le quote e le regole per la configurazione di utenti e gruppi in un SAML IdP basato, vedere. Quote di utenti e gruppi
- La SAML dichiarazione e i SAML documenti devono essere firmati.
- AWS Client VPN supporta solo le condizioni AudienceRestriction "" e "NotBefore e NotOnOrAfter" nelle SAML asserzioni.
- La dimensione massima supportata per SAML le risposte è 128 KB.
- AWS Client VPN non fornisce richieste di autenticazione firmate.
- SAMLil logout singolo non è supportato. Gli utenti possono disconnettersi disconnettendosi dal client AWS fornito oppure è possibile interrompere le connessioni.
- Un VPN endpoint Client supporta un solo IdP.
- L'autenticazione a più fattori (MFA) è supportata quando è abilitata nel tuo IdP.
- Gli utenti devono utilizzare il client AWS fornito per connettersi all'endpoint ClientVPN. 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 TCP porta 35001 sui dispositivi degli utenti per la SAML risposta.
- Se il documento di metadati del provider di IAM SAML identità viene aggiornato con un documento errato o dannosoURL, ciò può causare problemi di autenticazione per gli utenti o provocare attacchi di phishing. Pertanto, si consiglia di AWS CloudTrail utilizzarlo per monitorare gli aggiornamenti apportati al provider di IAM SAML identità. Per ulteriori informazioni, vedere Registrazione IAM e AWS STS chiamate con AWS CloudTrail nella Guida per l'IAMutente.
- AWS Client VPN invia una richiesta AuthN all'IdP tramite un'associazione di reindirizzamento. HTTP Pertanto, l'IdP dovrebbe supportare l'associazione HTTP Redirect e dovrebbe essere presente nel documento di metadati dell'IdP.
- Per l'SAMLasserzione, è necessario utilizzare un formato di indirizzo e-mail per l'attributo. `NameID`

SAMLrisorse di configurazione IdP basate

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

IdP	Risorsa
Okta	Autentica gli utenti con AWS Client VPN SAML
Microsoft Azure Active Directory	Per altre informazioni, vedi Tutorial: integrazione single sign-on (SSO) di Azure Active Directory con AWS Client VPN nel sito Web della documentazione Microsoft.
JumpCloud	Single Sign-On () con SSO 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 SAML basata su un IdP non elencato nella tabella precedente, utilizza le seguenti informazioni per configurare le informazioni sul fornitore di AWS Client VPN servizi.

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

Almeno un attributo deve essere incluso nella SAML risposta 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'`memberOf`attributo è necessario per utilizzare le regole di autorizzazione basate su 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 il tuo VPN endpoint Client, gli utenti accedono al portale utilizzando le proprie credenziali SAML IdP basate.

Se il tuo IdP supporta più Assertion Consumer Service (ACS)URLs, aggiungi quanto segue ACS URL alla tua app.

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

Se utilizzi l'VPNendpoint Client in una GovCloud regione, utilizza invece quanto segue. ACS URL Se utilizzi la stessa IDP app 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 di uno ACSURLs, procedi come segue:

1. Crea un'app SAML basata aggiuntiva nel tuo IdP e specifica quanto segue. ACS URL

   ```
   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 IAM SAML identità nello stesso AWS account dell'VPNendpoint Client. Per ulteriori informazioni, consulta Creazione di provider di IAM SAML identità nella Guida per l'IAMutente.

> **Note**
>
> Questo provider di IAM SAML identità viene creato in aggiunta a quello creato per l'app principale.

4. Crea l'VPNendpoint Client e specifica entrambi i provider di IAM SAML identità che hai creato.

Autorizzazione del cliente in AWS Client VPN

Il client VPN supporta due tipi di autorizzazione client: gruppi di sicurezza e autorizzazione basata sulla rete (utilizzando regole di autorizzazione).

Gruppi di sicurezza

Quando si crea un VPN endpoint Client, è possibile specificare i gruppi di sicurezza da applicare VPC all'endpoint Client. VPN Quando associ una sottorete a un VPN endpoint Client, applichiamo automaticamente il gruppo di sicurezza predefinito VPC dell'endpoint. Puoi modificare i gruppi di sicurezza dopo aver creato l'endpoint ClientVPN. 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 VPN rete Client.

È possibile consentire VPN agli utenti Client di accedere alle applicazioni in un modo VPC mediante l'aggiunta di una regola ai gruppi di sicurezza delle applicazioni per consentire il traffico proveniente dal gruppo di sicurezza applicato all'associazione.

Al contrario, è possibile limitare l'accesso per VPN gli utenti Client non specificando il gruppo di sicurezza applicato all'associazione o rimuovendo la regola che fa riferimento al gruppo di sicurezza degli endpoint ClientVPN. Le regole del gruppo di sicurezza richieste potrebbero dipendere anche dal tipo di VPN accesso che desideri configurare. Per ulteriori informazioni, consulta Scenari ed esempi per il cliente VPN.

Per ulteriori informazioni sui gruppi di sicurezza, consulta la sezione Gruppi di sicurezza per te VPC nella Amazon VPC User Guide.

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 specifica, si configura il gruppo Active Directory o il gruppo IdP SAML basato a cui è consentito l'accesso. Solo gli utenti che appartengono al gruppo specificato sono in grado di accedere alla rete specificata. Se non utilizzi Active Directory o l'autenticazione federata SAML basata o desideri aprire l'accesso a 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

- Crea un AWS Client VPN regola del gruppo di sicurezza degli endpoint

Crea un AWS Client VPN regola del gruppo di sicurezza degli endpoint

Il gruppo di sicurezza predefinito VPC applicato quando si associa una sottorete a un Client VPN potrebbe limitare il traffico proveniente dal 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 VPN degli endpoint Client 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 e su come funzionano, consulta Security groups for your VPC nella Amazon VPC User Guide.

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

1. Apri la VPC console Amazon 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, puoi limitare l'accesso a un tipo specifico di traffico, ad esempio SSH.

   Per Source, specifica l'ID del gruppo di sicurezza associato alla rete di destinazione (subnet) per l'VPNendpoint Client.
6. Scegliere Salva regole.

Autorizzazione della connessione in AWS Client VPN

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

Per configurare un gestore di connessione client per l'VPNendpoint Client, create una AWS Lambda funzione che prenda come input gli attributi di dispositivo, utente e connessione e restituisca al VPN servizio Client la decisione di consentire o negare una nuova connessione. Specificate la funzione Lambda nell'endpoint ClientVPN. Quando i dispositivi si connettono all'VPNendpoint Client, il VPN servizio Client richiama la funzione Lambda per conto dell'utente. Solo le connessioni autorizzate dalla funzione Lambda possono connettersi all'endpoint ClientVPN.

> **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 ClientVPN.
- 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 VPN servizio Client non riceve una risposta prevista dalla funzione, il VPN servizio Client nega 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'VPNendpoint Client non ne risentono. 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'VPNendpoint Client, 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 utente e gli attributi di connessione come input dal servizio Client. VPN Deve quindi restituire al VPN servizio Client la decisione se consentire o negare la connessione.

Schema di richiesta

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

```
{
    "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 del client all'endpoint del clientVPN.
- `endpoint-id`— L'ID dell'VPNendpoint del client.
- `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 SAML basata, 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 VPN servizio Client fornisce un valore quando la `--push-peer-info` direttiva è presente nella configurazione Open VPN client, quando i client si connettono a un VPN endpoint Client e quando il client esegue la piattaforma Windows.
- `public-ip`: l'indirizzo IP pubblico del dispositivo di connessione.
- `client-openvpn-version`— La VPN versione Open utilizzata dal client.
- `aws-client-version`— La versione AWS del client.
- `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 SAML basata, si tratterà di un elenco di gruppi di provider di identità (IdP). Per l'autenticazione reciproca, questo campo è vuoto.
- `schema-version`: la versione dello schema. Il valore di default è `v3`.

Schema di risposta

La funzione Lambda deve restituire i seguenti campi.

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

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

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

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

È possibile utilizzare la stessa funzione Lambda per più VPN endpoint Client 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

È possibile utilizzare il gestore di connessione client per integrare l'VPNendpoint Client con la soluzione di gestione dei dispositivi esistente per valutare la conformità posturale dei dispositivi di connessione. Affinché la funzione Lambda funzioni come gestore delle autorizzazioni 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 (trasmesso dal VPN servizio Client) per identificare il dispositivo e recuperarne lo stato di conformità alla postura dalla soluzione di gestione dei dispositivi. 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, è possibile valutare i `platform-version` campi `platform` and che vengono passati alla funzione Lambda dal servizio ClientVPN.

> **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 il gestore di connessione client, crea o modifica un VPN endpoint Client 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

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

Quando il gestore Client Connect viene utilizzato per la valutazione della postura, è inoltre possibile visualizzare gli stati di conformità alla postura dei dispositivi che si connettono all'VPNendpoint Client nei log di connessione. 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:

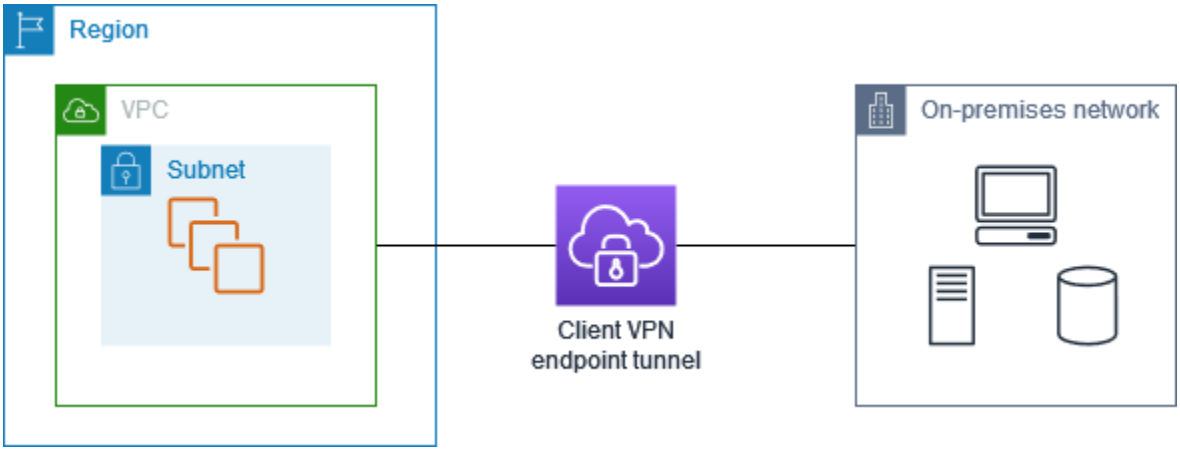
- `client-connect-failed`: la funzione Lambda ha impedito di stabilire la connessione.
- `client-connect-handler-timed-out`: si è verificato il timeout della funzione Lambda.
- `client-connect-handler-other-execution-error`: la funzione Lambda ha riscontrato un errore imprevisto.
- `client-connect-handler-throttled`: 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 del client VPN

Per impostazione predefinita, quando si dispone di un VPN endpoint Client, tutto il traffico proveniente dai client viene instradato sul tunnel Client. VPN Quando abiliti lo split-tunnel sull'VPNendpoint Client, inviamo le route dalla tabella di routing dell'VPNendpoint Client al dispositivo connesso all'endpoint Client. VPN Ciò garantisce che solo il traffico con una destinazione verso la rete che corrisponde a una route della tabella di routing dell'VPNendpoint Client venga instradato sul tunnel Client. VPN

È possibile utilizzare un VPN endpoint Client a tunnel diviso quando non si desidera che tutto il traffico utente venga instradato attraverso l'endpoint Client. VPN

Nell'esempio seguente, split-tunnel è abilitato sull'endpoint Client. VPN Solo il traffico destinato a VPC (`172.31.0.0/16`) viene instradato sul tunnel Client. VPN Il traffico destinato alle risorse locali non viene instradato sul tunnel Client. VPN



Vantaggi dello split-tunnel

Split-tunnel sugli endpoint Client offre i seguenti vantaggi: VPN

- 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 rotte nella tabella di routing dell'VPNendpoint Client vengono aggiunte alla tabella delle rotte del client quando viene stabilita la connessione. VPN Questa operazione è diversa dal comportamento predefinito, che sovrascrive la tabella delle rotte del client con la voce `0.0.0.0/0` per instradare tutto il traffico su. VPN

> **Note**
>
> Non è consigliabile aggiungere un `0.0.0.0/0` percorso alla tabella delle rotte dell'VPNendpoint Client quando si utilizza la modalità split-tunnel.

- Quando la modalità split-tunnel è abilitata, qualsiasi modifica alla tabella di routing dell'VPNendpoint Client comporterà il ripristino di tutte le connessioni client.

Abilitazione dello split-tunnel

È possibile abilitare lo split-tunnel su un endpoint Client nuovo o esistente. VPN 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 registri di connessione per l'endpoint Client. VPN

Un registro delle connessioni 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 È possibile utilizzare queste informazioni per eseguire analisi forensi, analizzare come viene utilizzato l'VPNendpoint Client o eseguire il debug di problemi di connessione.

La registrazione della connessione è disponibile in tutte le regioni in cui è disponibile. AWS Client VPN 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 del registro di connessione è un blob in JSON formato -format 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'VPNendpoint Client 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'IPv4CIDRintervallo di client per l'endpoint ClientVPN.
- `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 si utilizza l'autenticazione basata sull'utente (AD oSAML) 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 sulla VPN scalabilità dei client

Quando crei un VPN endpoint Client, considera il numero massimo di VPN connessioni simultanee che intendi supportare. È necessario tenere conto del numero di client attualmente supportati e della possibilità di scalare l'VPNendpoint Client per soddisfare la domanda aggiuntiva, se necessario.

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

Dimensione dell'intervallo di client CIDR

Quando si crea un VPN endpoint Client, è necessario specificare un CIDR intervallo di client, che è un IPv4 CIDR blocco compreso tra una netmask /12 e /22. A ogni VPN connessione all'VPNendpoint Client viene assegnato un indirizzo IP univoco dall'intervallo di client. CIDR Una parte degli indirizzi nell'CIDRintervallo client viene utilizzata anche per supportare il modello di disponibilità dell'VPNendpoint Client e non può essere assegnata ai client. Non è possibile modificare l'CIDRintervallo di client dopo aver creato l'VPNendpoint Client.

In generale, ti consigliamo di specificare un CIDR intervallo di client che contenga il doppio del numero di indirizzi IP (e quindi di connessioni simultanee) che intendi supportare sull'endpoint ClientVPN.

Numero di subnet associate

Quando si associa una sottorete a un VPN endpoint Client, si consente agli utenti di stabilire VPN sessioni sull'endpoint Client. VPN È possibile associare più sottoreti a un VPN endpoint Client per un'elevata disponibilità e per abilitare una capacità di connessione aggiuntiva.

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

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 della 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 prevedi di supportare 8.000 VPN connessioni all'VPNendpoint Client, specifica una dimensione minima dell'CIDRintervallo di client di `/18` (16.384 indirizzi IP) e associa almeno 2 sottoreti all'endpoint Client. VPN

Se non sei sicuro del numero di VPN connessioni previste per l'VPNendpoint Client, ti consigliamo di specificare un blocco di dimensioni pari o superiori. `/16` CIDR

Per ulteriori informazioni sulle regole e le limitazioni per l'utilizzo di CIDR intervalli di client e reti di destinazione, consulta. Regole e best practice per l'utilizzo AWS Client VPN

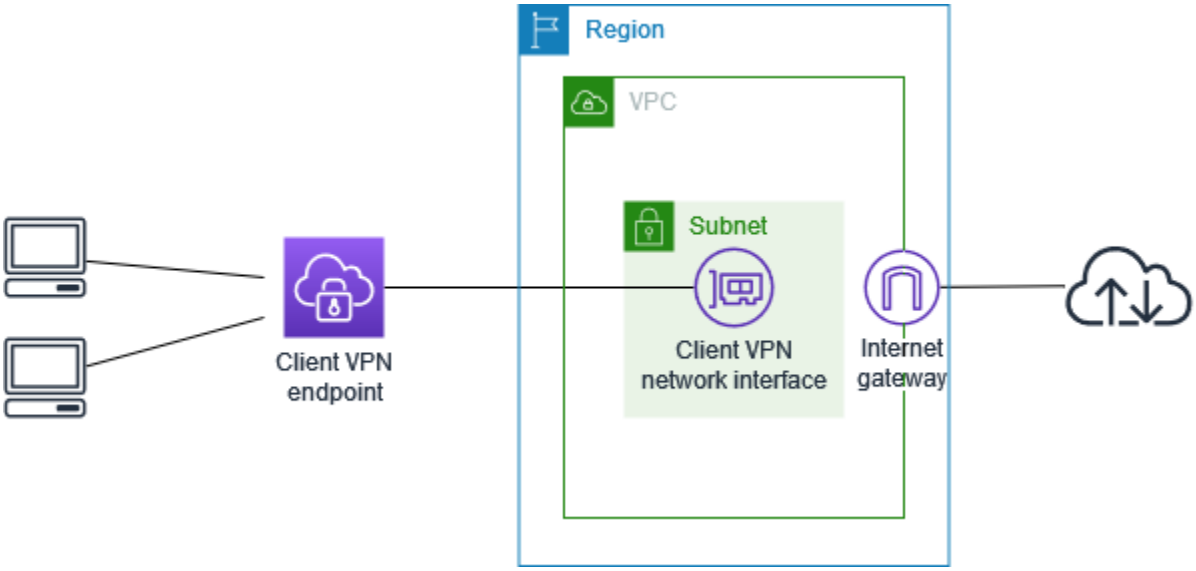
Per ulteriori informazioni sulle quote per l'VPNendpoint Client, consulta. AWS Client VPN quote

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 singoloVPC.
- Fornisce a tutti i clienti l'accesso a Internet.
- Utilizza l'autenticazione reciproca.

Il diagramma seguente rappresenta la configurazione dell'VPNendpoint tuo VPC e del client 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 VPC
- Fase 5: Fornire l'accesso a Internet.
- Fase 6: Verificare i requisiti del gruppo di sicurezza
- Passaggio 7: scarica il file di configurazione dell'VPNendpoint del client
- Fase 8: Connect all'VPNendpoint Client

Prerequisiti

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

- Le autorizzazioni necessarie per lavorare con gli VPN endpoint del Client.
- Le autorizzazioni necessarie per importare i certificati in AWS Certificate Manager.
- A VPC con almeno una sottorete 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, Client VPN utilizza i certificati per eseguire l'autenticazione tra i client e l'VPNendpoint Client. È necessario creare un certificato server e una chiave e almeno un certificato client e una chiave. Come minimo, il certificato del server dovrà essere importato in AWS Certificate Manager (ACM) e specificato quando si crea l'VPNendpoint Client. L'importazione del certificato client in ACM è facoltativa.

Se non disponi già di certificati da utilizzare per questo scopo, è possibile crearli utilizzando l'utilità Open VPN easy-rsa. Per i passaggi dettagliati per generare i certificati e le chiavi del server e del client utilizzando l'utilità Open VPN easy-rsa e importarli in see. ACM 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 verrà creato l'endpoint Client. VPN

Fase 2: Creare un endpoint Client VPN

L'VPNendpoint Client è la risorsa che crei e configuri per abilitare e gestire le sessioni clientVPN. È il punto di terminazione per tutte le sessioni clientVPN.

Per creare un endpoint Client VPN

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints, quindi scegli Crea VPN endpoint Client.

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

> **Note**
>
> L'intervallo di indirizzi non può sovrapporsi all'intervallo di indirizzi di rete di destinazione, all'intervallo di VPC indirizzi o a nessuno dei percorsi che verranno associati all'endpoint Client. VPN L'intervallo di indirizzi del client deve essere minimo /22 e non superiore alla dimensione del blocco CIDR /12. Non è possibile modificare l'intervallo di indirizzi del client dopo aver creato l'endpoint ClientVPN.

5. Per Certificato server ARN, seleziona il certificato ARN del server che hai generato nel passaggio 1.
6. In Opzioni di autenticazione, scegli Usa autenticazione reciproca, quindi per Certificato client ARN, seleziona il ARN certificato che desideri utilizzare come certificato client.

   Se i certificati server e client sono firmati dalla stessa autorità di certificazione (CA), hai la possibilità di specificare il certificato del server sia ARN per i certificati client che per quelli server. In questo scenario, qualsiasi certificato client corrispondente al certificato del server può essere utilizzato per l'autenticazione.
7. (Facoltativo) Specificate quali DNS server utilizzare per la DNS risoluzione. Per utilizzare DNS server personalizzati, per l'indirizzo IP DNS del DNS server 1 e l'indirizzo IP del server 2, specificare gli indirizzi IP dei DNS server da utilizzare. Per utilizzare il VPC DNS server, per l'indirizzo IP DNS del DNS Server 1 o dell'indirizzo IP del Server 2, specificare gli indirizzi IP e aggiungere l'indirizzo IP del VPC DNS server.

> **Note**
>
> Verificate che i DNS server possano essere raggiunti dai client.

8. Mantieni le altre impostazioni predefinite e scegli Create Client VPN Endpoint.

Dopo aver creato l'VPNendpoint Client, il suo stato è. `pending-associate` I client possono stabilire una VPN connessione solo dopo aver associato almeno una rete di destinazione.

Per ulteriori informazioni sulle opzioni che è possibile specificare per un VPN endpoint Client, vedereCreare un AWS Client VPN endpoint.

Fase 3: Associazione di una rete target

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

Per associare una rete di destinazione all'endpoint Client VPN

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client che hai creato nella procedura precedente, quindi scegli Associazioni di rete di destinazione, Associa rete di destinazione.
4. Per VPC, scegli la rete VPC in cui si trova la sottorete.
5. Per Scegli una sottorete da associare, scegli la sottorete da associare all'endpoint Client. VPN
6. Scegli Associa rete tdi destinazione.
7. Se le regole di autorizzazione lo consentono, un'associazione di sottorete è sufficiente per consentire ai client di accedere all'intera rete. VPC Puoi associare sottoreti aggiuntive per fornire un'elevata disponibilità nel caso in cui una delle zone di disponibilità sia danneggiata.

Quando si associa la prima sottorete all'VPNendpoint Client, si verifica quanto segue:

- Lo stato dell'VPNendpoint Client cambia in. `available` I client possono ora stabilire una VPN connessione, ma non possono accedere a nessuna risorsa VPC fino a quando non vengono aggiunte le regole di autorizzazione.
- La route locale di VPC viene aggiunta automaticamente alla tabella di routing dell'VPNendpoint Client.
- Il gruppo VPC di sicurezza predefinito viene applicato automaticamente all'VPNendpoint Client.

Fase 4: Aggiungere una regola di autorizzazione per VPC

Affinché i client possano accedere aVPC, è necessario che VPC nella tabella di routing dell'endpoint Client sia presente un percorso verso la tabella di VPN routing dell'endpoint Client e una regola di

autorizzazione. Il percorso è già stato aggiunto automaticamente nella fase precedente. Per questo tutorial, vogliamo concedere a tutti gli utenti l'accesso a. VPC

Per aggiungere una regola di autorizzazione per VPC

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client a cui aggiungere la regola di autorizzazione. Scegli Regole di autorizzazione, quindi scegli Add authorization rule (Aggiungi regola di autorizzazione).
4. Per consentire l'accesso alla rete CIDR di destinazione, inserisci la rete a cui desideri consentire l'accesso. Ad esempio, per consentire l'accesso all'intera reteVPC, specificate il IPv4 CIDR blocco diVPC.
5. In Grant access to (Consenti accesso a), scegliere Allow access to all users (Consenti accesso a tutti gli utenti).
6. (Opzionale) In Descrizione immettere una breve descrizione della regola di autorizzazione.
7. Scegliere Add authorization rule (Aggiungi regola di autorizzazione).

Fase 5: Fornire l'accesso a Internet.

È possibile fornire l'accesso a reti aggiuntive connesse aVPC, ad esempio, AWS serviziVPCs, reti peer-to-premise e Internet. Per ogni rete aggiuntiva, si aggiunge una route alla rete nella tabella di routing dell'VPNendpoint Client e si configura una regola di autorizzazione per consentire ai client l'accesso.

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

Fornire l'accesso a Internet

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client che hai 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 è stato specificato alcun gruppo di sicurezza durante la creazione dell'VPNendpoint Client nel passaggio 2. Ciò significa che il gruppo di sicurezza predefinito per il VPC viene applicato automaticamente all'VPNendpoint Client quando viene associata una rete di destinazione. Di conseguenza, il gruppo di sicurezza predefinito per il VPC dovrebbe ora essere associato all'VPNendpoint Client.

Verifica i seguenti requisiti del gruppo di sicurezza

- Il fatto che il gruppo di sicurezza associato alla sottorete attraverso cui state indirizzando il traffico (in questo caso il gruppo di VPC sicurezza predefinito) consenta 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`.
- Che i gruppi di sicurezza per le risorse presenti VPC abbiano una regola che consenta l'accesso dal gruppo di sicurezza applicato all'VPNendpoint Client (in questo caso il gruppo di sicurezza predefinitoVPC). Ciò consente ai tuoi clienti di accedere alle risorse del tuoVPC.

Per ulteriori informazioni, consulta Gruppi di sicurezza.

Passaggio 7: scarica il file di configurazione dell'VPNendpoint del client

Il passaggio successivo consiste nel scaricare e preparare il file di configurazione dell'VPNendpoint del client. Il file di configurazione include i dettagli dell'VPNendpoint del Client e le informazioni sul certificato necessarie per stabilire una VPN connessione. Fornisci questo file agli utenti finali che devono connettersi all'VPNendpoint Client. L'utente finale utilizza il file per configurare la propria applicazione VPN client.

Per scaricare e preparare il file di configurazione dell'VPNendpoint del client

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client che hai creato per questo tutorial e scegli Scarica la configurazione del client.
4. Individuare il certificato client e la chiave che sono stati generati nel passaggio 1. Il certificato e la chiave del client sono disponibili nelle seguenti posizioni nel repository Open VPN 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'VPNendpoint del client 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'VPNendpoint del client.
7. Distribuisci il file di configurazione dell'VPNendpoint Client agli utenti finali.

Per ulteriori informazioni sul file di configurazione dell'VPNendpoint del client, vedere. AWS Client VPN esportazione del file di configurazione dell'endpoint

Fase 8: Connect all'VPNendpoint Client

È possibile connettersi all'VPNendpoint Client utilizzando il client AWS fornito o un'altra applicazione client VPN basata su Open 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 ClientVPN:

- Accesso al portale self-service: configura l'accesso al portale VPN self-service Client in modo che i client possano scaricare autonomamente il file di configurazione degli VPN endpoint Client. 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: utilizzate 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, vedere. the section called “Elenchi di revoche di certificati client”
- Connessioni client: visualizza o termina una connessione client a un endpoint clientVPN. Per informazioni sulla visualizzazione o l'interruzione di una connessione client, vedere. the section called “Connessioni client”
- Banner di accesso del client: aggiunge un banner di testo su un'applicazione VPN desktop Client quando viene stabilita una VPN sessione. 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”.
- VPNEndpoint client: configura gli VPN endpoint client 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 VPN endpoint Client nuovi o esistenti per iniziare ad acquisire 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 VPN client di cui i client hanno bisogno per stabilire VPN le connessioni. 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 VPN route client 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 VPN endpoint Client per consentire ai client di connettersi ad esso e stabilire una VPN connessione. Per informazioni sulle reti di destinazione, consultathe section called “Reti target”.
- Durata massima VPN della sessione: imposta le opzioni per la durata massima VPN della sessione per soddisfare i requisiti di sicurezza e conformità. Per informazioni sulla durata massima VPN della sessione, consultathe section called “durata massima VPN della sessione”.

AWS Client VPN accesso al portale self-service

Se hai abilitato il portale self-service per il tuo VPN endpoint Client, puoi fornire ai tuoi clienti un portale self-service. URL 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'VPNendpoint Client e possono scaricare la versione più recente del client fornito. AWS

Si applicano le regole seguenti:

- Il portale self-service non è disponibile per i client che eseguono l'autenticazione reciproca.
- Il file di configurazione disponibile nel portale self-service è lo stesso file di configurazione che esporti utilizzando la VPC console Amazon 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'VPNendpoint Client, altrimenti i clienti non potranno accedere al portale. Se questa opzione non è abilitata, puoi modificare l'VPNendpoint Client 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 questa opzioneURL, devono inserire l'ID dell'VPNendpoint Client prima di poter accedere.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Replace (Sostituisci) `<endpoint-id>` nel precedente URL con l'ID dell'VPNendpoint Client, ad esempio,. `cvpn-endpoint-0123456abcd123456`

È inoltre possibile visualizzare il URL relativo portale self-service nell'output del comando. describe-client-vpn-endpoints AWS CLI In alternativa, URL è disponibile nella scheda Dettagli della pagina Client VPN Endpoints nella VPC console Amazon.

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. È possibile aggiungere regole di autorizzazione a un VPN endpoint Client utilizzando la console e il AWS CLI.

> **Note**
>
> Il client VPN utilizza la corrispondenza dei prefissi più lunga durante la valutazione delle regole di autorizzazione. Per maggiori dettagli, consulta l'argomento sulla risoluzione dei problemi Risoluzione dei problemi AWS Client VPN: le regole di autorizzazione per i gruppi di Active Directory non funzionano come previsto e la priorità del percorso nella Amazon VPC User Guide.

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.
- `0.0.0.0/0`CIDRViene gestito come un caso speciale. Viene elaborato per ultimo, a prescindere dall'ordine di creazione delle regole di autorizzazione.
- `0.0.0.0/0`CIDRPuò essere considerata 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

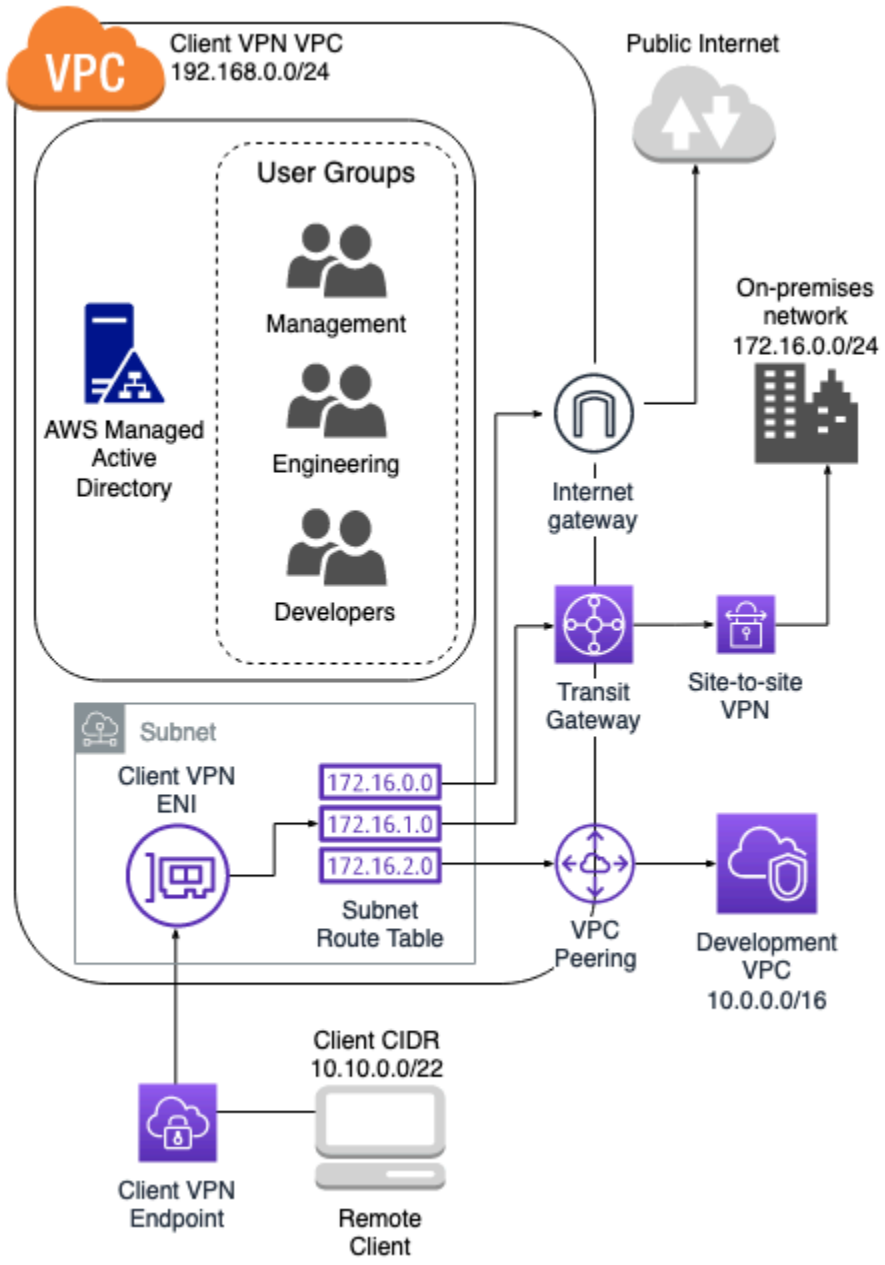
Scenari di esempio per le regole di VPN autorizzazione del cliente

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

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	Destinazione CIDR
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	Destinazione CIDR
l'accesso alla rete on-premise			
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	S-xxxxx15	False	10.0.0.0/16
Fornisci l'accesso al gruppo di manager al Client VPN VPC	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 il resto del traffico viene interrotto dall'VPNendpoint del Client.

> **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	Destinazione CIDR
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	Destinazione CIDR
l'accesso alla rete on-premise			
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	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	Destinazione CIDR
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	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
Fornisci al gruppo di manager l'accesso a un singolo host in fase di sviluppo VPC	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 e a un singolo host (`10.0.2.119/32`) all'interno dello sviluppoVPC, ma non ha accesso a `172.16.0.0/24` nessuno degli host rimanenti nello sviluppo. `192.168.0.0/24` VPC

> **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`.

Sovrapposizione CIDR (stesso gruppo)

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	Destinazione CIDR
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	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
Fornisci ai gruppi di manager l'accesso a un singolo host in fase di sviluppo VPC	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	Destinazione CIDR
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	Destinazione CIDR
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	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	Destinazione CIDR
Fornisci ai gruppi di manager l'accesso a un singolo host in fase di sviluppo VPC			
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	Destinazione CIDR
Fornisce al gruppo di progettazione l'accesso alla rete on-premise	S-xxxxx14	False	172.16.0.0/24
Fornire ai gruppi di sviluppo l'accesso allo sviluppo VPC	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
Fornisci ai gruppi di manager l'accesso a un singolo host in fase di sviluppo VPC	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	Destinazione CIDR
Fornisci l'accesso al gruppo di manager al Client VPN VPC	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.

Accesso per tutti i gruppi di utenti

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

Descrizione della regola	ID gruppo	Consente l'accesso a tutti gli utenti	Destinazione CIDR
Fornisce al gruppo di manager l'accesso a qualsiasi destinazione	S-xxxxx16	False	0.0.0.0/0
Fornisci ai gruppi di manager l'accesso a un singolo host in fase di sviluppo VPC	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
Fornisci l'accesso al gruppo di manager al Client VPN VPC	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 VPN endpoint Client utilizzando il AWS Management Console. Una regola di autorizzazione può essere aggiunta a un VPN endpoint Client utilizzando la VPC console Amazon o utilizzando la riga di comando oAPI.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client a cui aggiungere la regola di autorizzazione, scegli Regole di autorizzazione e scegli Aggiungi regola di autorizzazione.
4. Affinché la rete di destinazione consenta l'accesso, inserisci l'indirizzo IP, in CIDR notazione, della rete a cui desideri che gli utenti accedano (ad esempio, il CIDR blocco della tuaVPC).
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 l'ID/nome di un gruppo definito in un provider di identità SAML basato (IdP).
     - (Active Directory) Per ottenere ilSID, 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 SAML basata) L'ID/nome del gruppo 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 Client (VPN AWS CLI)

Usa il authorize-client-vpn-ingresscomando.

Rimuovere una regola di autorizzazione da un AWS Client VPN endpoint

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

Per rimuovere le regole di autorizzazione (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client 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)

Usa il revoke-client-vpn-ingresscomando.

Visualizza le regole di AWS Client VPN autorizzazione

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

Per visualizzare le regole di autorizzazione (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client per il quale visualizzare le regole di autorizzazione e scegli Regole di 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 VPN client client vengono utilizzati per revocare l'accesso a un endpoint Client per certificati client VPN specifici. È possibile generare l'elenco delle revoche e importare un elenco esistente o esportare l'elenco corrente in un file di elenco delle revoche. La generazione di un elenco viene eseguita utilizzando il VPN software Open su Linu/macOS o su Windows. L'importazione e l'esportazione possono essere eseguite utilizzando la VPC console Amazon o utilizzando il. AWS CLI

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

Puoi 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 per i clienti VPN

Attività

- Genera un AWS Client VPN elenco di revoca dei certificati 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

Genera un AWS Client VPN elenco di revoca dei certificati client

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

Linux/macOS

Nella procedura seguente, si genera un elenco di revoca dei certificati client utilizzando l'utilità da riga di comando Open VPN easy-rsa.

Per generare un elenco di revoca dei certificati client utilizzando Open easy-rsa VPN

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 VPN software Open per generare un elenco di revoche dei client. Si presuppone che siano stati seguiti i passaggi per l'utilizzo del VPN software Open per generare i certificati e le chiavi del client e del server.

Per generare un elenco di revoca dei certificati client utilizzando la versione Easy 3.x.x RSA

1. Apri un prompt dei comandi e accedi alla directory Easy RSA -3.x.x, che dipenderà da dove è installato sul tuo sistema.

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

2. Esegui il `EasyRSA-Start.bat` file per avviare la shell Easy. RSA

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

3. Nella RSA shell Easy, revoca il certificato del 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 dei certificati client utilizzando le versioni precedenti di Easy RSA

1. Aprire un prompt dei comandi e accedere alla directory 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 con l'elenco delle revoche dei certificati VPN client Client da importare. Per ulteriori informazioni sulla creazione di un elenco di revoche di certificati client, consulta Genera un AWS Client VPN elenco di revoca dei certificati 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 VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client per il quale importare l'elenco delle revoche dei certificati client.
4. Scegli Azioni e scegli Importa certificato client. CRL
5. Per Elenco delle revoche dei certificati, inserisci il contenuto del file dell'elenco delle revoche dei certificati client e scegli Importa certificato client. CRL

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

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

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

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

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client per il quale esportare l'elenco delle revoche dei certificati client.
4. Scegli Azioni, scegli Esporta certificato CRL client e scegli Esporta certificato client. CRL

Per esportare una revoca di certificato client (AWS CLI)

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

AWS Client VPN connessioni client

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

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 CIDR blocchi client, l'ID dell'endpoint e il timestamp. L'interruzione di una sessione termina la VPN connessione specificata all'endpoint. La visualizzazione e la chiusura delle sessioni possono essere eseguite utilizzando la VPC console Amazon o il AWS CLI. 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 VPN connessioni client attive utilizzando la VPC console Amazon o il AWS CLI.

Per visualizzare le connessioni VPN dei client client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client per il quale 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 dei VPN client client ()AWS CLI

Usa il describe-client-vpn-connectionscomando.

Interrompere una connessione AWS Client VPN client

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

Per interrompere una connessione VPN client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client 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 () VPN AWS CLI

Usa il terminate-client-vpn-connectionscomando.

AWS Client VPN banner di accesso al cliente

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

> **Note**
>
> Quando un banner di accesso client è stato abilitato, verrà visualizzato solo VPN nelle sessioni appena create. VPNLe sessioni esistenti non vengono interrotte, tuttavia il banner verrà visualizzato quando viene ristabilita una sessione esistente.

Consulta le note di rilascio per il client AWS fornito nella Guida per l'AWS Client VPN utente per i dettagli sulle applicazioni desktop client.

Creazione di banner

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

Utilizza i seguenti passaggi per configurare un banner di accesso client per un VPN endpoint Client esistente.

Abilita il banner di accesso del client su un VPN endpoint client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client 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 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 VPN sessione. Utilizza solo UTF -8 caratteri codificati, con un massimo di 1400 caratteri consentiti.
7. Scegli Modifica endpoint client VPN.

Abilita il banner di accesso del client su un VPN endpoint client ()AWS CLI

Usa il modify-client-vpn-endpointcomando.

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

Utilizza i seguenti passaggi per disattivare un banner di accesso client per un endpoint Client VPN esistente.

Disattiva il banner di accesso del client su un VPN endpoint client (console)

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

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

Usa 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 VPN del cliente.

Modifica il testo del banner esistente su un dispositivo VPN Client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client che desideri modificare, scegli Azioni, quindi scegli Modifica 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 VPN sessione. Utilizza solo UTF -8 caratteri codificati, con un massimo di 1400 caratteri.
6. Scegli Modifica endpoint client VPN.

Modifica il banner di accesso del client su un VPN endpoint client ()AWS CLI

Usa il modify-client-vpn-endpointcomando.

Visualizza un banner di AWS Client VPN accesso attualmente configurato

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint del client che desideri 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.

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

Usa il describe-client-vpn-endpointscomando.

AWS Client VPN punti finali

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

Requisiti per la creazione di endpoint Client VPN

> **Important**
>
> Un VPN endpoint Client deve essere creato nello stesso AWS account in cui viene fornito il provisioning della rete di destinazione prevista. È inoltre necessario 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.

Modifica dell'endpoint

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

- Descrizione
- Certificato del server
- Opzioni di registrazione della connessione client
- L'opzione dell'handler di connessioni client
- I DNS server
- Opzione split-tunnel
- Route (quando si utilizza l'opzione split-tunnel)
- Elenco di revoca dei certificati () CRL
- Regole di autorizzazione
- Le VPC e le associazioni dei gruppi di sicurezza
- Il numero di VPN porta
- L'opzione del portale self-service
- La durata massima VPN della sessione
- Abilitare o disabilitare il testo del banner di accesso client
- Testo del banner di accesso client

> **Note**
>
> Le modifiche agli VPN endpoint del Cliente, incluse le modifiche all'Elenco di revoca dei certificati (CRL), avranno effetto fino a 4 ore dopo l'accettazione della richiesta da parte del servizio Clienti. VPN
>
> Non è possibile modificare l'IPv4CIDRintervallo di client, le opzioni di autenticazione, il certificato client o il protocollo di trasporto dopo la creazione dell'VPNendpoint Client.

Quando si modifica uno dei seguenti parametri su un VPN endpoint Client, la connessione viene ripristinata:

- Certificato del server
- I server DNS
- Opzione tunnel diviso (attivazione o disattivazione del support)
- Percorsi (quando si utilizza l'opzione del tunnel diviso)
- Elenco di revoca dei certificati () CRL
- Regole di autorizzazione
- Il numero di VPN porta

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 VPN endpoint client per consentire ai tuoi clienti di stabilire una VPN sessione utilizzando la VPC console Amazon o il AWS CLI.

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

Per creare un VPN endpoint client (console)

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

> **Note**
>
> L'intervallo di indirizzi non può sovrapporsi all'intervallo di indirizzi di rete di destinazione, all'intervallo di VPC indirizzi o a nessuno dei percorsi che verranno associati all'endpoint Client. VPN L'intervallo di indirizzi del client deve essere minimo /22 e non superiore alla dimensione del blocco CIDR /12. Non è possibile modificare l'intervallo di indirizzi del client dopo aver creato l'endpoint ClientVPN.

5. Per il certificato del server ARN, specificare il ARN TLS certificato che deve essere utilizzato dal server. I client utilizzano il certificato del server per autenticare l'VPNendpoint Client 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 ClientVPN. Il certificato può essere fornito ACM o importato in. ACM

6. Specificare il metodo di autenticazione da utilizzare per autenticare i client quando stabiliscono una VPN connessione. 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: scegli questa opzione per l'autenticazione federata SAML basata.

       Per SAMLprovider ARN, specificare il provider ARN di IAM SAML identità.

       (Facoltativo) Per il SAMLprovider self-service ARN, specificare il provider ARN di IAM SAML identità creato per supportare il portale self-service, se applicabile.
   - Per utilizzare l'autenticazione reciproca tramite certificato, seleziona Usa autenticazione reciproca, quindi per Certificato client ARN, specifica il ARN certificato client fornito in AWS Certificate Manager (). ACM

> **Note**
>
> Se i certificati server e client sono stati emessi dalla stessa autorità di certificazione (CA), puoi utilizzare il certificato server sia ARN per il server che per il client. Se il certificato client è stato emesso da un'altra CA, è ARN necessario specificare il certificato client.

7. (Facoltativo) Per la registrazione delle connessioni, specifica se registrare i dati sulle connessioni client utilizzando Amazon CloudWatch Logs. Attivare Abilita i dettagli del registro sulle connessioni client. Per il nome del gruppo di log CloudWatch Logs, inserisci il nome del gruppo di log da utilizzare. Per CloudWatch Logs log stream name, inserisci il nome del log stream da utilizzare o lascia vuota questa opzione per consentirci di creare un flusso di log per te.
8. (Facoltativo) Per Client Connect Handler, attiva Enable client connect handler per eseguire codice personalizzato che consente o nega una nuova connessione all'endpoint Client. VPN Per Client Connect Handler ARN, specifica Amazon Resource Name (ARN) della funzione Lambda che contiene la logica che consente o nega le connessioni.
9. (Facoltativo) Specificare quali DNS server utilizzare per la risoluzione. DNS Per utilizzare DNS server personalizzati, per l'indirizzo IP DNS del DNS Server 1 e l'indirizzo IP del Server 2, specificare gli indirizzi IP dei DNS server da utilizzare. Per utilizzare il VPC DNS server, per l'indirizzo IP DNS del DNS Server 1 o dell'indirizzo IP del Server 2, specificare gli indirizzi IP e aggiungere l'indirizzo IP del VPC DNS server.

   > **Note**
   >
   > Verificate che i DNS server possano essere raggiunti dai client.

10. (Facoltativo) Per impostazione predefinita, l'VPNendpoint Client utilizza il protocollo di `UDP` trasporto. Per utilizzare invece il protocollo `TCP` di trasporto, per Transport Protocol, seleziona TCP.

    > **Note**
    >
    > UDPin genere offre prestazioni migliori rispetto aTCP. Non è possibile modificare il protocollo di trasporto dopo aver creato l'VPNendpoint Client.

11. (Facoltativo) Per fare in modo che l'endpoint sia un VPN endpoint Client con tunnel diviso, attiva Abilita split-tunnel. Per impostazione predefinita, lo split-tunnel su un endpoint Client è disabilitato. VPN
12. (Facoltativo) Per VPCID, scegli VPC da associare all'endpoint Client. VPN Per Security Group IDs, scegli uno o più gruppi VPC di sicurezza da applicare all'VPNendpoint Client.
13. (Facoltativo) Per la VPNporta, scegli il numero di VPN porta. Il valore predefinito è 443.
14. (Facoltativo) Per generare un portale self-service URL per i clienti, attiva Abilita il portale self-service.
15. (Facoltativo) Per le ore di timeout della sessione, scegli la durata massima VPN della sessione desiderata, in ore, tra le opzioni disponibili, oppure lascia impostato il valore predefinito di 24 ore.
16. (Facoltativo) Specificare se abilitare il testo del banner di accesso client. Attiva Enable client login banner (Abilita il banner di accesso client). Per il testo del banner di accesso del cliente, inserisci il testo che verrà visualizzato in un banner sui client AWS forniti quando viene stabilita una VPN sessione. UTFSolo -8 caratteri codificati. Massimo 1400 caratteri.
17. Scegli Crea VPN endpoint client.

Dopo aver creato l'VPNendpoint Client, procedi come segue per completare la configurazione e consentire ai client di connettersi:

- Lo stato iniziale dell'VPNendpoint Client è. `pending-associate` I client possono connettersi all'VPNendpoint Client 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'VPNendpoint Client da distribuire ai tuoi client.
- Chiedi ai tuoi clienti di utilizzare il client AWS fornito o un'altra applicazione client VPN basata su Open per connettersi all'endpoint ClientVPN. Per ulteriori informazioni, consulta la Guida per l'utente AWS Client VPN.

Per creare un VPN endpoint Client ()AWS CLI

Usa il create-client-vpn-endpointcomando.

Visualizza gli AWS Client VPN endpoint

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

Per visualizzare gli VPN endpoint del client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint del client da visualizzare.
4. Utilizza le schede Dettagli, Associazioni di rete Target, Gruppi di sicurezza, Regole di autorizzazione, tabella di percorso, Connessioni e Tag per visualizzare le informazioni sugli endpoint Client VPN esistenti.

   È possibile utilizzare i filtri per migliorare la ricerca.

Per visualizzare gli VPN endpoint del client ()AWS CLI

Usa il describe-client-vpn-endpointscomando.

Modificare un AWS Client VPN endpoint

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

> **Note**
>
> Le modifiche agli VPN endpoint del client, incluse le modifiche all'elenco di revoca dei certificati (CRL), avranno effetto fino a 4 ore dopo l'accettazione della richiesta da parte del servizio clienti. VPN
> Non è possibile modificare l'IPv4CIDRintervallo di client, le opzioni di autenticazione, il certificato client o il protocollo di trasporto dopo la creazione dell'VPNendpoint Client.

Per modificare un VPN endpoint Client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client da modificare, scegli Azioni, quindi scegli Modifica endpoint client VPN.
4. Per Descrizione, inserisci una breve descrizione per l'endpoint ClientVPN.

5. Per Certificato server ARN, specificare ARN il TLS certificato che deve essere utilizzato dal server. I client utilizzano il certificato del server per autenticare l'VPNendpoint Client 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 ClientVPN. Il certificato può essere fornito ACM o importato in. ACM

6. Specificare se registrare i dati sulle connessioni client utilizzando Amazon CloudWatch Logs. Per Do you want to log the details on client connections? (Vuoi registrare i dettagli sulle connessioni client?), procedere in uno dei seguenti modi:

   - Per attivare la registrazione delle 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.

7. Per Handler di connessioni client, per attivare l'handler di connessioni client attivare Enable client connect handler (Abilita l'handler delle connessioni client). Per Client Connect Handler ARN, specifica Amazon Resource Name (ARN) della funzione Lambda che contiene la logica che consente o nega le connessioni.

8. Attiva o disattiva Abilita server. DNS Per utilizzare DNS server personalizzati, per l'indirizzo IP DNS del DNS Server 1 e l'indirizzo IP del Server 2, specificare gli indirizzi IP dei DNS server da utilizzare. Per utilizzare il VPC DNS server, per l'indirizzo IP DNS del DNS Server 1 o dell'indirizzo IP del Server 2, specificare gli indirizzi IP e aggiungere l'indirizzo IP del VPC DNS server.

> **Note**
>
> Verificate che i DNS server possano essere raggiunti dai client.

9. Attivare o disattivare Enable split-tunnel (Abilita split-tunnel). Per impostazione predefinita, lo split-tunnel su un VPN endpoint è disattivato.

10. Per VPCID, scegli da associare VPC all'endpoint Client. VPN Per Security Group IDs, scegli uno o più gruppi VPC di sicurezza da applicare all'VPNendpoint Client.
11. Per VPNporta, scegli il numero di VPN porta. Il valore predefinito è 443.
12. Per generare un portale self-service URL per i clienti, attiva Abilita il portale self-service.
13. Per le ore di timeout della sessione, scegli la durata massima della VPN sessione desiderata, in ore, tra le opzioni disponibili, oppure lascia impostato il valore predefinito di 24 ore.
14. Abilitare o disabilitare Enable client login banner (Abilita il banner di accesso client. Se desideri utilizzare il banner di accesso del cliente, inserisci il testo che verrà visualizzato in un banner sui client AWS forniti quando viene stabilita una VPN sessione. UTFSolo -8 caratteri codificati. Massimo 1400 caratteri.
15. Scegli Modifica VPN endpoint client.

Per modificare un VPN endpoint client ()AWS CLI

Usa il modify-client-vpn-endpointcomando.

Eliminare un AWS Client VPN endpoint

È necessario dissociare tutte le reti di destinazione prima di poter eliminare un endpoint ClientVPN. Quando si elimina un VPN endpoint Client, il relativo stato viene modificato in `deleting` e i client non possono più connettersi ad esso.

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

Per eliminare un VPN endpoint client (console)

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

Per eliminare un VPN endpoint client ()AWS CLI

Usa il delete-client-vpn-endpointcomando.

AWS Client VPN registri di connessione

È possibile abilitare la registrazione delle connessioni per un VPN endpoint Client nuovo o esistente e iniziare ad acquisire i 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 si specifica un flusso di log, il VPN servizio Client ne crea uno automaticamente. La registrazione della connessione 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 delle VPN connessioni dei client possono essere creati utilizzando la VPC console Amazon o il AWS CLI.

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

È possibile abilitare la registrazione delle connessioni quando si crea un nuovo VPN endpoint Client utilizzando la console o la riga di comando.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints, quindi scegli Crea VPN endpoint Client.

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. Scegliete Crea endpoint client VPN.

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

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

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

Abilitare la registrazione delle connessioni per un endpoint AWS Client VPN esistente

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

Per abilitare la registrazione della connessione per un VPN endpoint Client esistente utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client, scegli Azioni, quindi scegli Modifica endpoint client VPN.
4. In Registrazione delle connessioni, attiva Enable log details on client connections (Abilita i dettagli del registro sulle connessioni client).

5. Per 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. Scegliete Modifica endpoint del client VPN.

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

Utilizzate il modify-client-vpn-endpointcomando e specificate il `--connection-log-options` parametro. È possibile specificare le informazioni dei registri di connessione in JSON formato, come illustrato nell'esempio seguente.

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

Visualizza i registri delle AWS Client VPN connessioni

È possibile visualizzare i registri di VPN connessione del client 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 il tuo VPN endpoint Client.

> **Note**
>
> La colonna Timestamp mostra l'ora in cui il log di connessione è stato pubblicato su 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

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

Per disabilitare la registrazione delle connessioni utilizzando la console

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

Per disattivare la registrazione della connessione 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 utilizzato dai client (utenti) per stabilire una VPN connessione con l'VPNendpoint Client. È necessario scaricare (esportare) questo file e distribuirlo a tutti i client che devono accedere a. VPN In alternativa, se hai abilitato il portale self-service per l'VPNendpoint Client, i client 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'VPNendpoint Client utilizza l'autenticazione reciproca, è necessario aggiungere il certificato client e la chiave privata del client al file di configurazione.ovpn scaricato. Dopo aver aggiunto le informazioni, i client possono importare il file.ovpn nel software Open client. VPN

> **Important**
>
> Se non si aggiungono il certificato del client e le informazioni sulla chiave privata del client al file, i client che si autenticano utilizzando l'autenticazione reciproca non possono connettersi all'endpoint Client. VPN

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

Se l'VPNendpoint Client utilizza l'autenticazione Active Directory e se abiliti l'autenticazione a più fattori (MFA) sulla directory dopo aver distribuito il file di configurazione del client, devi scaricare un nuovo file e ridistribuirlo ai tuoi 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 VPN del client Client utilizzando la console o il AWS CLI.

Per esportare la configurazione del client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint client per il quale scaricare la configurazione del client e scegli Scarica configurazione client.

Per esportare la configurazione del client (AWS CLI)

Usa il comando export-client-vpn-client-configuration e specifica il nome del file di output.

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

Aggiungere il certificato AWS Client VPN client e le informazioni chiave per l'autenticazione reciproca

Se l'VPNendpoint Client utilizza l'autenticazione reciproca, è necessario aggiungere il certificato client e la chiave privata del client al file di configurazione.ovpn 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) Distribuisci il certificato e la chiave del client ai client insieme al file di configurazione dell'VPNendpoint del client. 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. Replace (Sostituisci) `/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 e chiavi client separati per ogni utente che si connetterà all'VPNendpoint Client, ripeti questo passaggio per ogni utente.

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

```
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 ogni route dell'VPNendpoint del client per specificare quali client hanno accesso alla rete di destinazione.

Quando si associa una sottorete da un a un VPC VPN endpoint Client, VPC viene automaticamente aggiunta una route per il dispositivo Client alla tabella di routing dell'VPNendpoint Client. Per abilitare l'accesso a reti aggiuntive, come le reti peered localiVPCs, 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 ClientVPN.

> **Note**
>
> Se state associando più sottoreti all'VPNendpoint Client, assicuratevi di creare una route per ogni sottorete come descritto qui. Risoluzione dei problemi AWS Client VPN: l'accesso a un sistema peeredVPC, ad Amazon S3 o a Internet è intermittente Ogni sottorete associata dovrebbe avere un insieme identico di routing.

Considerazioni sull'utilizzo dello split-tunnel sugli endpoint Client VPN

Quando si utilizza split-tunnel su un VPN endpoint Client, tutte le route presenti nelle tabelle di routing Client vengono aggiunte alla tabella di VPN route client quando viene stabilita la. VPN Se aggiungi una route dopo che VPN è stata stabilita, devi reimpostare la connessione in modo che la nuova route venga inviata al client.

Si consiglia di tenere conto del numero di rotte che il dispositivo client è in grado di gestire prima di modificare la tabella di routing dell'VPNendpoint Client.

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 VPN endpoint Client, 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`.

È possibile aggiungere percorsi a un VPN endpoint Client utilizzando la console e il. AWS CLI

Per creare una route di VPN endpoint Client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client a cui aggiungere il percorso, scegli Tabella delle rotte, quindi scegli Crea percorso.
4. Per Route destination, specifica l'IPv4CIDRintervallo per la rete di destinazione. Per esempio:
    - Per aggiungere un percorso per l'VPNendpoint VPC del Client, inserisci VPC l'IPv4CIDRintervallo.
    - Per aggiungere una route per l'accesso a Internet, immettere `0.0.0.0/0`
    - Per aggiungere un percorso per un peerVPC, inserisci l'intervallo del peer. VPC IPv4 CIDR

- Per aggiungere un percorso per una rete locale, inserisci l'intervallo della connessione da AWS sito a sitoVPN. IPv4 CIDR

5. Per l'ID di sottorete per l'associazione alla rete di destinazione, seleziona la sottorete associata all'endpoint Client. VPN

   In alternativa, se stai aggiungendo un percorso per la rete locale di VPN endpoint Client, seleziona. `local`

6. (Facoltativo) In Descrizione, inserire una breve descrizione del routing.
7. Selezionare Create Route (Crea route).

Per creare una route di VPN endpoint Client ()AWS CLI

Usa il create-client-vpn-routecomando.

Visualizza i AWS Client VPN percorsi degli endpoint

È possibile visualizzare i percorsi per uno specifico VPN endpoint Client utilizzando la console o il. AWS CLI

Per visualizzare i percorsi VPN degli endpoint del client (console)

1. Nel riquadro di navigazione, scegli Client VPN Endpoints.
2. Seleziona l'VPNendpoint Client per il quale visualizzare i percorsi e scegli la tabella Route.

Per visualizzare i percorsi VPN degli endpoint del client ()AWS CLI

Usa il describe-client-vpn-routescomando.

Eliminare una route AWS Client VPN dell'endpoint

Puoi eliminare solo le VPN route Client che hai aggiunto manualmente. Non è possibile eliminare le route che sono state aggiunte automaticamente quando è stata associata una sottorete all'VPNendpoint Client. Per eliminare le route aggiunte automaticamente, è necessario dissociare la sottorete che ne ha avviato la creazione dall'endpoint Client. VPN

È possibile eliminare una route da un VPN endpoint Client utilizzando la console o il. AWS CLI

Per eliminare una route dell'VPNendpoint Client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client da cui eliminare il percorso e scegli la tabella Route.
4. Selezionare il routing da eliminare, scegliere Elimina routing, quindi Elimina routing.

Per eliminare una route dell'VPNendpoint Client ()AWS CLI

Usa il delete-client-vpn-routecomando.

AWS Client VPN reti di destinazione

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

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

Requisiti della rete di VPN destinazione del client

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

- La sottorete deve avere un CIDR blocco 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 CIDR blocco della sottorete non può sovrapporsi all'intervallo client dell'endpoint Client. CIDR VPN
- Se si associano più di una sottorete a un VPN endpoint Client, ogni sottorete deve trovarsi in una zona di disponibilità diversa. È consigliabile associare almeno due sottoreti per garantire la ridondanza delle zone di disponibilità.
- Se hai specificato a VPC quando hai creato l'VPNendpoint Client, la sottorete deve trovarsi nella stessa. VPC Se non hai ancora VPC associato a all'VPNendpoint Client, puoi scegliere qualsiasi sottorete in qualsiasi. VPC

  Tutte le altre associazioni di sottoreti devono appartenere alla stessa. VPC Per associare una sottorete da un'altraVPC, è necessario prima modificare l'VPNendpoint Client e cambiare VPC quello ad esso associato. Per ulteriori informazioni, consulta Modificare un AWS Client VPN endpoint.

Quando associ una sottorete a un VPN endpoint Client, aggiungiamo automaticamente la route locale della sottorete associata VPC in cui viene fornito il provisioning della sottorete associata alla tabella di routing dell'endpoint Client. VPN

> **Note**
>
> Dopo aver associato le reti di destinazione, quando ne aggiungi o rimuovi altre CIDRs da quelle collegateVPC, devi eseguire una delle seguenti operazioni per aggiornare la route locale per la tabella di routing degli endpoint Client: VPN
>
> - Dissocia l'VPNendpoint Client dalla rete di destinazione, quindi associa l'VPNendpoint Client alla rete di destinazione.
> - Aggiungi manualmente la route o rimuovi la route dalla tabella di routing dell'VPNendpoint Client.

Dopo aver associato la prima sottorete all'VPNendpoint Client, lo stato dell'VPNendpoint Client 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 VPN endpoint Client utilizzando la VPC console Amazon o il. AWS CLI Prima di associare una rete di destinazione a un VPN endpoint Client, 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 VPN endpoint Client (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.

3. Seleziona l'VPNendpoint Client a cui associare la rete di destinazione, scegli Associazioni di rete Target, quindi scegli Associa rete di destinazione.
4. Per VPC, scegli l'area VPC in cui si trova la sottorete. Se hai specificato a VPC quando hai creato l'VPNendpoint Client o se hai precedenti associazioni di sottoreti, deve essere la stessa. VPC
5. Per Scegli una 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 associate-client-vpn-target-network.

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

Quando si crea un VPN endpoint Client, è possibile specificare i gruppi di sicurezza da applicare alla rete di destinazione. Quando associ la prima rete di destinazione a un VPN endpoint Client, applichiamo automaticamente il gruppo di sicurezza predefinito VPC in cui si trova la sottorete associata. Per ulteriori informazioni, consulta Gruppi di sicurezza.

È possibile modificare i gruppi di sicurezza per l'endpoint ClientVPN. Le regole del gruppo di sicurezza richieste dipendono dal tipo di VPN accesso che desideri configurare. Per ulteriori informazioni, consulta Scenari ed esempi per il cliente VPN.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client 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 IDs di sicurezza.
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

È possibile visualizzare le destinazioni associate a un VPN endpoint Client utilizzando la console o il AWS CLI.

Per visualizzare le reti target (console)

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint Client appropriato e scegli Associazioni di rete Target.

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 si dissocia una rete di destinazione, tutte le route che sono state aggiunte manualmente alla tabella di VPN routing dell'endpoint Client vengono eliminate, così come la route che è stata creata automaticamente al momento dell'associazione alla rete di destinazione (la route locale del). VPC Se si dissociano tutte le reti di destinazione da un VPN endpoint Client, i client non possono più stabilire una connessione. VPN

Per dissociare una rete di destinazione da un VPN endpoint Client (console)

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

Per dissociare una rete di destinazione da un VPN endpoint Client ()AWS CLI

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

AWS Client VPN durata massima VPN della sessione

AWS Client VPN fornisce diverse opzioni per la durata massima della VPN sessione, che è il tempo massimo consentito per la connessione di un client all'VPNendpoint Client. È possibile configurare una durata massima VPN della sessione più breve per contribuire a soddisfare i requisiti di sicurezza e conformità. Per impostazione predefinita, la durata massima VPN della sessione è di 24 ore. Dopo la scadenza del timeout della sessione, viene stabilita automaticamente una nuova sessione in caso di credenziali utente memorizzate nella cache (Active Directory) o di autenticazione basata su certificati (autenticazione reciproca). Per disconnettersi completamente e non riconnettersi automaticamente, questi utenti devono disconnettersi manualmente. Nel caso dell'autenticazione federata (SAML) non viene stabilita automaticamente una nuova sessione, quindi questi utenti devono autenticarsi nuovamente dopo la scadenza del timeout della sessione per stabilire la connessione. VPN

> **Note**
>
> Quando il valore della durata massima della VPN sessione viene ridotto rispetto al valore corrente, tutte VPN le sessioni attive connesse all'endpoint per un periodo di tempo più lungo della durata appena impostata vengono disconnesse.

Vedi le note di rilascio per il client AWS fornito nel AWS Client VPN Guida per l'utente per i dettagli sulla durata della sessione per le applicazioni desktop client.

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

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

Attività

- Visualizza la durata massima AWS Client VPN attuale VPN della sessione
- Modifica la durata massima AWS Client VPN della sessione

Visualizza la durata massima AWS Client VPN attuale VPN della sessione

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

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN Endpoints.
3. Seleziona l'VPNendpoint del client che desideri visualizzare.
4. Verifica che la scheda Dettagli.
5. Visualizza la durata massima attuale VPN della sessione accanto alle ore di timeout della sessione.

Visualizza la durata massima attuale VPN della sessione per un VPN endpoint Client ()AWS CLI

Usa il describe-client-vpn-endpointscomando.

Modifica la durata massima AWS Client VPN della sessione

Utilizzare i seguenti passaggi per modificare la durata VPN massima VPN della sessione Client esistente.

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

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Client VPN endpoints.
3. Seleziona l'VPNendpoint client che desideri modificare, scegli Azioni, quindi scegli Modifica endpoint client VPN.
4. Per le ore di timeout della sessione, scegli la durata massima della VPN sessione desiderata in ore.
5. Scegli Modifica VPN endpoint client.

Modifica una durata massima VPN della sessione esistente per un VPN endpoint Client ()AWS CLI

Usa il modify-client-vpn-endpointcomando.

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 ulteriori informazioni sui programmi di conformità applicabili AWS Client VPN, consulta AWS Servizi 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 VPC servizio Amazon. Per ulteriori informazioni sulla sicurezza in AmazonVPC, consulta Security in the Amazon VPC User Guide.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi ClientVPN. I seguenti argomenti mostrano come configurare Client VPN per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere VPN le risorse del tuo Client.

Argomenti

Protezione dei dati in AWS Client VPN

Il AWS modello di responsabilità condivisa modello di di si applica alla protezione dei dati in AWS ClienteVPN. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le Cloud AWS. L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta la AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura singoli utenti con AWS IAM Identity Center oppure 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:

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per l'acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di 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 sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente 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 altri Servizi AWS utilizzando la consoleAPI, AWS CLI, oppure AWS SDKs. 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia in transito

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

Riservatezza del traffico Internet

Abilitazione dell'accesso tra reti

È possibile consentire ai client di connettersi alla propria rete VPC e ad altre reti tramite un VPN endpoint Client. Per maggiori informazioni ed esempi, vedi Scenari ed esempi per il cliente VPN.

Limitazione dell'accesso alle reti

Puoi configurare l'VPNendpoint Client per limitare l'accesso a risorse specifiche del 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 Per ulteriori informazioni, consulta Limita l'accesso alla tua rete utilizzando Client VPN.

Autenticazione dei client

L'autenticazione viene implementata al primo punto di ingresso nel AWS Cloud. Viene utilizzato per determinare se i client sono autorizzati a connettersi all'VPNendpoint Client. Se l'autenticazione ha esito positivo, i client si connettono all'VPNendpoint Client e stabiliscono una sessione. VPN Se l'autenticazione fallisce, la connessione viene negata e al client viene impedito di stabilire una sessione. VPN

Il 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 SAML basata) (basata sull'utente)

Gestione delle identità e degli accessi per AWS Client VPN

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle

autorizzazioni) a utilizzare le risorse del client. VPN IAMè un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in ClientVPN.

Utente del servizio: se utilizzi il VPN servizio Client per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più VPN funzionalità del Client per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in ClientVPN, vediRisoluzione dei problemi AWS Client VPN di identità e accesso.

Amministratore del servizio: se sei responsabile delle VPN risorse dei clienti presso la tua azienda, probabilmente hai pieno accesso a ClientVPN. È tuo compito determinare a quali VPN funzionalità e risorse del Client devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM ClientVPN, consultaCome AWS Client VPN funziona con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a ClientVPN. Per visualizzare esempi di politiche VPN basate sull'identità del client che puoi utilizzare inIAM, 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. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console 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 () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

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'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

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 l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

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 AWS 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 informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo 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 IAM amministrare le risorse.

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

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Metodi per assumere un ruolo nella Guida per l'IAMutente.

IAMi ruoli 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 informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo 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 conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in 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 diretto (FAS): quando utilizzi un IAM utente o un ruolo 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. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FASle richieste 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 FAS delle politiche relative alle richieste, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.
- 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 IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. È preferibile archiviare le chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza 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'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole 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 JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM 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 all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute 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. ACLssono 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 informazioniACLs, consulta la panoramica di Access control list (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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM 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 nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche 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 Account AWS di proprietà dell'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. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'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 le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come AWS Client VPN funziona con IAM

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

IAMfunzionalità che puoi usare con AWS Client VPN

IAMcaratteristica	VPNAssistenza clienti
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 politiche)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica generale del funzionamento del Client VPN e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per Client VPN

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. 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 ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Client VPN

Per visualizzare esempi di politiche basate sull'VPNidentità del cliente, vedere. Esempi di policy basate su identità per AWS Client VPN

Politiche basate sulle risorse all'interno di Client VPN

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di 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 azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica 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 IAM amministratore dell'account fidato 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 la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per il cliente VPN

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API 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 VPN azioni del client, vedere Azioni definite dal AWS client VPN nel riferimento di autorizzazione del servizio.

Le azioni politiche in Client VPN utilizzano il seguente prefisso prima dell'azione:

```
ec2
```

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

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

Per visualizzare esempi di politiche VPN basate sull'identità del client, vedere. Esempi di policy basate su identità per AWS Client VPN

Risorse politiche per il cliente VPN

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di VPN risorse Client e relativiARNs, consulta Resources defined by AWS Client VPN nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, consulta Azioni definite dal AWS client VPN.

Per visualizzare esempi di politiche VPN basate sull'identità del client, vedere. Esempi di policy basate su identità per AWS Client VPN

Chiavi relative alle condizioni delle politiche per Client VPN

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano

più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica0R. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

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'IAMutente.

Per visualizzare un elenco delle chiavi di VPN condizione del client, consulta Condition keys for AWS Client VPN nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite dal AWS client VPN.

Per visualizzare esempi di politiche VPN basate sull'identità del cliente, vedere. Esempi di policy basate su identità per AWS Client VPN

ACLsin Client VPN

SupportiACLs: 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon Client VPN

Supporti ABAC (tag nelle politiche): No

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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 suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con Client VPN

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione Servizi AWS relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra 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 sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. 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, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali multiservizio per Client VPN

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo 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. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FASle

richieste 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 FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per il cliente VPN

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità del Client. VPN Modifica i ruoli di servizio solo quando il Client VPN fornisce indicazioni in tal senso.

Ruoli collegati al servizio 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 IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. IAM Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per AWS Client VPN

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le VPN risorse del Client. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di

eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

Per i dettagli sulle azioni e sui tipi di risorse definiti dal ClientVPN, 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

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare VPN le risorse Client 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 gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS 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 le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.

- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

```
{
    "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 seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Client VPN andIAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Client VPN
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle VPN risorse dei miei clienti

Non sono autorizzato a eseguire un'azione in Client VPN

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'`mateojacksonIAMutente` tenta di utilizzare la console per visualizzare i dettagli su una *`my-example-widget`* risorsa fittizia ma non dispone delle autorizzazioni fittizie`ec2:`*`GetWidget`*.

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

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a ClientVPN.

Alcuni Servizi AWS consentono di trasferire 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 IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione 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 assistenza, contatta AWS l'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 VPN risorse dei miei clienti

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 sapere se Client VPN supporta queste funzionalità, consulta. Come AWS Client VPN funziona con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Utilizzo di ruoli collegati ai servizi per AWS Client VPN

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

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

Un ruolo collegato al servizio semplifica la configurazione di Client VPN perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Client VPN definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo Client può assumerne i ruoli. VPN Le

autorizzazioni definite includono la politica di fiducia e la politica di autorizzazione e tale politica di autorizzazione non può essere associata a nessun'altra entità. IAM

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Ciò protegge le VPN risorse del cliente perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Client VPN

Il client VPN utilizza il ruolo collegato al servizio denominato AWSServiceRoleForClientVPN: Consenti VPN al client di creare e gestire risorse relative alle tue connessioni. VPN

Il ruolo AWSServiceRoleForClientVPNcollegato al servizio si affida al seguente servizio per l'assunzione del ruolo:

- `clientvpn.amazonaws.com`

La politica di autorizzazione dei ruoli denominata C lientVPNService RolePolicy consente VPN al Client di completare le seguenti azioni sulle risorse specificate:

- Operazione: `ec2:CreateNetworkInterface` su `Resource: "*"`
- Operazione: `ec2:CreateNetworkInterfacePermission` su `Resource: "*"`
- Operazione: `ec2:DescribeSecurityGroups` su `Resource: "*"`
- Operazione: `ec2:DescribeVpcs` su `Resource: "*"`
- Operazione: `ec2:DescribeSubnets` su `Resource: "*"`
- Operazione: `ec2:DescribeInternetGateways` su `Resource: "*"`
- Operazione: `ec2:ModifyNetworkInterfaceAttribute` su `Resource: "*"`
- Operazione: `ec2:DeleteNetworkInterface` su `Resource: "*"`
- Operazione: `ec2:DescribeAccountAttributes` su `Resource: "*"`
- Operazione: `ds:AuthorizeApplication` su `Resource: "*"`
- Operazione: `ds:DescribeDirectories` su `Resource: "*"`

- Operazione: `ds:GetDirectoryLimits` su `Resource: "*"`
- Operazione: `ds:UnauthorizeApplication` su `Resource: "*"`
- Operazione: `logs:DescribeLogStreams` su `Resource: "*"`
- Operazione: `logs:CreateLogStream` su `Resource: "*"`
- Operazione: `logs:PutLogEvents` su `Resource: "*"`
- Operazione: `logs:DescribeLogGroups` su `Resource: "*"`
- Operazione: `acm:GetCertificate` su `Resource: "*"`
- Operazione: `acm:DescribeCertificate` su `Resource: "*"`
- Operazione: `iam:GetSAMLProvider` su `Resource: "*"`
- Operazione: `lambda:GetFunctionConfiguration` su `Resource: "*"`

È necessario configurare le autorizzazioni per consentire a un'IAMentità (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente. IAM

Creazione di un ruolo collegato al servizio per Client VPN

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

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

Modifica di un ruolo collegato al servizio per Client VPN

Il client VPN non consente di modificare il ruolo collegato al AWSServiceRoleForClientVPN servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, è possibile modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

Eliminazione di un ruolo collegato al servizio per Client VPN

Se non è più necessario utilizzare ClientVPN, si consiglia di eliminare il ruolo collegato al AWSServiceRoleForClientVPNservizio.

È necessario innanzitutto eliminare le relative risorse ClientVPN. Questo ti impedisce di rimuovere accidentalmente l'autorizzazione ad accedere alle risorse.

Utilizza la IAM console IAMCLI, il o il IAM API per eliminare i ruoli collegati al servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Regioni supportate per i ruoli collegati ai servizi client VPN

Il client VPN supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

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

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

Un ruolo collegato al servizio semplifica la configurazione di Client VPN perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Client VPN definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo Client può assumerne i ruoli. VPN Le autorizzazioni definite includono la politica di fiducia e la politica di autorizzazione e tale politica di autorizzazione non può essere associata a nessun'altra entità. IAM

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Ciò protegge le VPN risorse del cliente perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Client VPN

Il client VPN utilizza il ruolo collegato al servizio denominato Service Linked Role AWSServiceRoleForClientVPNConnectionsfor Client connections. VPN

Il ruolo AWSServiceRoleForClientVPNConnections collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `clientvpn-connections.amazonaws.com`

La politica di autorizzazione dei ruoli denominata C lientVPNService ConnectionsRolePolicy consente VPN al Client di completare le seguenti azioni sulle risorse specificate:

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

È necessario configurare le autorizzazioni per consentire a un'IAMentità (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente. IAM

Creazione di un ruolo collegato al servizio per Client VPN

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

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

Modifica di un ruolo collegato al servizio per Client VPN

Il client VPN non consente di modificare il ruolo collegato al AWSServiceRoleForClientVPNConnections servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, è possibile modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

Eliminazione di un ruolo collegato al servizio per Client VPN

Se non è più necessario utilizzare ClientVPN, si consiglia di eliminare il ruolo collegato al AWSServiceRoleForClientVPNConnectionsservizio.

È necessario innanzitutto eliminare le relative risorse ClientVPN. Questo ti impedisce di rimuovere accidentalmente l'autorizzazione ad accedere alle risorse.

Utilizza la IAM console IAMCLI, il o il IAM API per eliminare i ruoli collegati al servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Regioni supportate per i ruoli collegati ai servizi client VPN

Il client VPN supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Resilienza in AWS Client VPN

L'infrastruttura 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

Si associa una rete di destinazione a un VPN endpoint Client per consentire ai client di stabilire VPN sessioni. Le reti di destinazione sono sottoreti del tuo. VPC Ogni sottorete associata all'VPNendpoint Client deve appartenere a una zona di disponibilità diversa. È possibile associare più sottoreti a un VPN endpoint Client per un'elevata disponibilità.

Sicurezza dell'infrastruttura in AWS Client VPN

In quanto 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.

Si utilizzano le API chiamate AWS pubblicate per accedere al client VPN attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.

- Suite di cifratura con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (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 AWS Client VPN regole di autorizzazione.

Gruppi di sicurezza

Utilizza i gruppi di sicurezza per controllare a quali risorse gli utenti possono accedere nel tuoVPC. Per ulteriori informazioni, consulta Gruppi di sicurezza.

Elenchi di revoche di certificati client

Utilizza gli elenchi di revoca dei certificati client per revocare l'accesso a un VPN endpoint Client per certificati client specifici. Ad esempio, quando un utente lascia l'organizzazione. Per ulteriori informazioni, consulta AWS Client VPN elenchi di revoca dei certificati client.

Strumenti di monitoraggio

Utilizza gli strumenti di monitoraggio per tenere traccia della disponibilità e delle prestazioni degli endpoint Client. VPN Per ulteriori informazioni, consulta Monitoraggio AWS Client VPN.

Gestione dell'identità e degli accessi

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

IPv6considerazioni per AWS Client VPN

Attualmente il VPN servizio Client non supporta l'instradamento IPv6 del traffico attraverso il VPN tunnel. Tuttavia, ci sono casi in cui IPv6 il traffico deve essere indirizzato verso il VPN tunnel per evitare IPv6 perdite. IPv6la perdita può verificarsi quando entrambi IPv4 IPv6 sono abilitati e collegati al tunnelVPN, ma VPN non instrada il IPv6 traffico verso il tunnel. In questo caso, quando ti connetti a una destinazione IPv6 abilitata, in realtà ti stai ancora connettendo con IPv6 l'indirizzo fornito dal tuoISP. Questo farà trapelare il tuo vero IPv6 indirizzo. Le istruzioni riportate di seguito spiegano come indirizzare il IPv6 traffico verso il VPN tunnel.

Le seguenti IPv6 direttive relative devono essere aggiunte al file di VPN configurazione del client 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 che l'indirizzo del dispositivo del tunnel locale sia `fd15:53b6:dead::2` e l'IPv6indirizzo dell'VPNendpoint IPv6 remoto sia. `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 VPN connessione.

> **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 VPN connessione.

Verifica

L'organizzazione eseguirà probabilmente i propri test. Una verifica di base consiste nel configurare una VPN connessione tunnel completa, quindi eseguire ping6 su un IPv6 server utilizzando l'indirizzo. IPv6 L'IPv6indirizzo 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 VPN servizio Client. 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 del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di AWS Client VPN e il tuo altro AWS soluzioni. È possibile utilizzare le seguenti funzionalità per monitorare gli VPN endpoint Client, analizzare i modelli di traffico e risolvere i problemi relativi agli endpoint Client. VPN

Amazon CloudWatch

Monitora il tuo AWS le 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 CPU dell'utilizzo 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

Registra le API chiamate e gli eventi correlati effettuati da o per conto di AWS account e consegna i file di log a un bucket Amazon S3 specificato. Puoi identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Tutte le VPN azioni del cliente vengono registrate CloudTrail e documentate in Amazon EC2 API Reference.

CloudWatch Registri Amazon

Consente di monitorare i tentativi di connessione effettuati al AWS Client VPN endpoint. È possibile visualizzare i tentativi di connessione e le reimpostazioni di connessione per le connessioni ClientVPN. Per i tentativi di connessione, è possibile visualizzare i tentativi di connessione riusciti e non riusciti. È possibile specificare il flusso di CloudWatch log dei registri 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

AWS Client VPN pubblica le seguenti metriche su Amazon CloudWatch per gli endpoint dei tuoi clientiVPN. Le metriche vengono pubblicate su Amazon CloudWatch ogni cinque minuti.

Parametro	Descrizione
ActiveConnectionsCount	Il numero di connessioni attive all'VPNendpoint Client. Unità: numero
AuthenticationFailures	Il numero di errori di autenticazione per l'endpoint ClientVPN. Unità: numero
CrlDaysToExpiry	Il numero di giorni che mancano alla scadenza dell'elenco di revoca dei certificati (CRL) configurato sull'endpoint ClientVPN. Unità: giorni
EgressBytes	Il 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	Il numero di download del file di configurazione dell'VPNendpoint del client dal portale self-service. Unità: numero

AWS Client VPN pubblica le seguenti metriche di valutazione della postura per gli endpoint Client. VPN

Parametro	Descrizione
ClientConnectHandlerTimeouts	Il numero di timeout necessari per richiamare il gestore Client Connect per le connessioni all'endpoint Client. VPN Unità: numero
ClientConnectHandlerInvalidResponses	Il numero di risposte non valide restituite dal gestore Client Connect per le connessioni all'endpoint Client. VPN Unità: numero
ClientConnectHandlerOtherExecutionErrors	Il numero di errori imprevisti durante l'esecuzione del gestore di connessione client per le connessioni all'endpoint Client. VPN Unità: numero
ClientConnectHandlerThrottlingErrors	Il numero di errori di limitazione nell'invocazione del gestore Client Connect per le connessioni all'endpoint Client. VPN Unità: numero

Parametro	Descrizione
ClientConnectHandlerDeniedConnections	Il numero di connessioni negate dal gestore di connessione client per le connessioni all'endpo int Client. VPN Unità: numero
ClientConnectHandlerFailedServiceErrors	Il numero di errori sul lato del servizio durante l'esecuzione del gestore di connessione client per le connessioni all'endpoint Client. VPN Unità: numero

Puoi filtrare le metriche per l'VPNendpoint Client per endpoint.

CloudWatch consente di recuperare le statistiche su tali punti dati come 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 VPN degli endpoint dei clienti in Amazon CloudWatch

Visualizza le metriche VPN degli endpoint dei clienti in Amazon CloudWatch

Puoi visualizzare le metriche per il tuo VPN endpoint Client 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 Tutte le metriche, scegli lo spazio dei nomi delle VPN metriche Client.
4. Per visualizzare i parametri, seleziona la dimensione del parametro per endpoint.

Per visualizzare le metriche utilizzando il AWS CLI

Al prompt dei comandi, utilizzate il seguente comando per elencare le metriche disponibili per il Client VPN

```
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 del cliente. 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 per i clienti VPN

Nome	Predefinita	Adattabile
Regole di autorizzazione per endpoint del client VPN	50	Sì
VPNEndpoint client per regione	5	Sì
Connessioni client simultanee per endpoint client VPN	Questo valore dipende dal numero di associazioni sottoreti per l'endpoint. • 1 — 20.000 • 2 – 36.500 • 3 – 66.500 • 4 – 96.500 • 5 – 126.000	Sì
Operazioni simultanee per endpoint VPN Client†	10	No
Voci in un elenco di revoca dei certificati client per gli endpoint Client VPN	20.000	No
Percorsi per endpoint del client VPN	10	Sì

† Le operazioni includono:

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

Quote di utenti e gruppi

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

- 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

Tieni in considerazione quanto segue quando utilizzi gli endpoint ClientVPN:

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

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 open VPN based utilizzato dai client per connettersi a un clientVPN, vedere Risoluzione dei problemi relativi alla VPN connessione del client nella Guida per l'AWS Client VPN utente.

Problemi comuni

- Risoluzione dei problemi AWS Client VPN: impossibile risolvere il nome dell'VPNendpoint DNS del client
- 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 sistema peeredVPC, ad Amazon S3 o a Internet
- Risoluzione dei problemi AWS Client VPN: l'accesso a un sistema peeredVPC, ad Amazon S3 o a Internet è intermittente
- Risoluzione dei problemi AWS Client VPN: il software client restituisce un TLS errore quando si tenta di connettersi al 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 nell'autenticazione federata Client VPN
- 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: instradamento del traffico in modo che LAN non funzioni come previsto
- Risoluzione dei problemi AWS Client VPN: verifica del limite di larghezza di banda per un endpoint client VPN

Risoluzione dei problemi AWS Client VPN: impossibile risolvere il nome dell'VPNendpoint DNS del client

Problema

Non riesco a risolvere il nome dell'VPNendpoint del client. DNS

Causa

Il file di configurazione dell'VPNendpoint Client include un parametro chiamato. `remote-random-hostname` Questo parametro impone al client di aggiungere una stringa casuale al DNS nome per impedire la memorizzazione nella cache. 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'VPNendpoint del client utilizzando l'editor di testo preferito. Individua la riga che specifica il DNS nome dell'VPNendpoint del Client e aggiungi una stringa casuale ad essa in modo che il formato sia *`random_string.displayed_DNS_name`*. Ad esempio:

- DNSNome originale: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- DNSNome 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, viene utilizzata solo una route anche se ho aggiunto entrambe le rotte alla tabella delle route degli VPN endpoint Client.

Causa

È possibile associare più sottoreti a un VPN endpoint Client, ma è possibile 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 selettivamente il traffico tra le sottoreti associate all'endpoint Client. VPN

I client si connettono a un VPN endpoint Client 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

Verifica che l'VPNendpoint Client abbia le stesse voci di percorso 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.

Il client VPN utilizza la corrispondenza dei prefissi più lunga durante la valutazione delle regole di autorizzazione. Per maggiori dettagli, consulta Route priority nella Amazon VPC User Guide.

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.

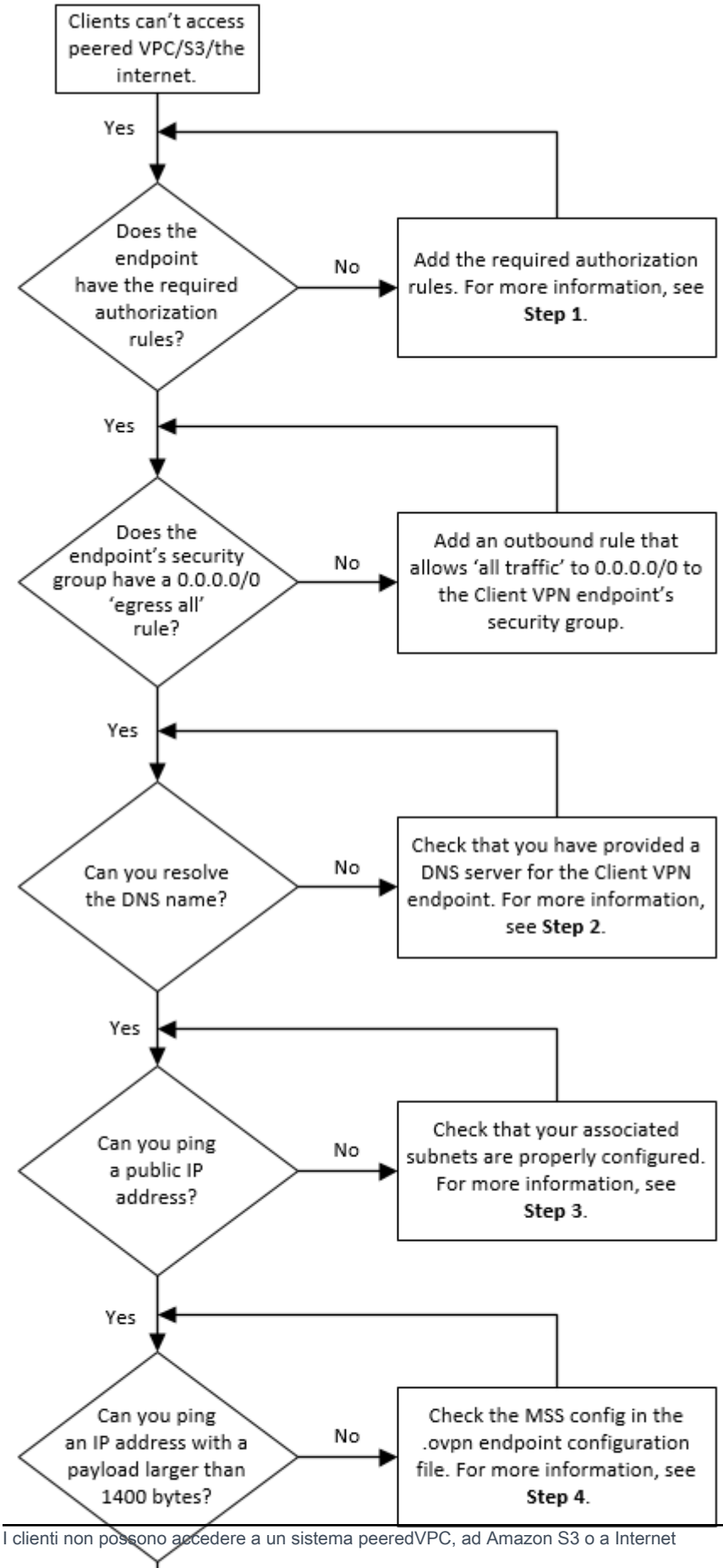
Risoluzione dei problemi AWS Client VPN: i client non possono accedere a un sistema peeredVPC, ad Amazon S3 o a Internet

Problema

Ho configurato correttamente i percorsi VPN degli endpoint Client, ma i miei clienti non possono accedere a un peeredVPC, ad Amazon S3 o a Internet.

Soluzione

Il seguente diagramma di flusso contiene i passaggi per diagnosticare i problemi di connettività InternetVPC, 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 peerVPC, aggiungi una regola di autorizzazione per l'IPv4CIDRintervallo di. VPC

   Per accedere a S3, specifica l'indirizzo IP dell'endpoint Amazon S3.
2. Verifica se sei in grado di risolvere il DNS nome.

   Se non riesci a risolvere il DNS nome, verifica di aver specificato DNS i server per l'VPNendpoint Client. Se gestisci il tuo DNS server, specifica il suo indirizzo IP. Verificate che il DNS server sia accessibile daVPC.

   Se non sei sicuro dell'indirizzo IP da specificare per DNS i server, specifica il VPC DNS resolver all'indirizzo IP .2 nel tuo. 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 ricevi una risposta, assicurati che la tabella di routing per le sottoreti associate abbia una route predefinita destinata a un gateway Internet 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 riesci a raggiungere un peerVPC, verifica che la tabella di routing della sottorete associata contenga una voce di route per il peer. VPC

   Se non riesci a raggiungere Amazon S3, verifica che la tabella di routing della sottorete associata contenga una route per l'endpoint del gateway. VPC
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 riesci a eseguire il ping di un indirizzo IP con un payload superiore a 1400 byte, apri il file di `.ovpn` configurazione dell'VPNendpoint Client utilizzando il tuo editor di testo preferito e aggiungi quanto segue.

```
mssfix 1328
```

Risoluzione dei problemi AWS Client VPN: l'accesso a un sistema peeredVPC, ad Amazon S3 o a Internet è intermittente

Problema

Ho problemi di connettività intermittenti durante la connessione a un sistema peered, ad Amazon VPC S3 o a Internet, ma l'accesso alle sottoreti associate non ne risente. Per risolvere i problemi di connettività devo eseguire la disconnessione e la riconnessione.

Causa

I client si connettono a un endpoint 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

Verifica che l'VPNendpoint Client abbia le stesse voci di percorso 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, supponiamo che l'VPNendpoint Client abbia tre sottoreti associate (subnet A, B e C) e che desideri abilitare l'accesso a Internet per i tuoi clienti. 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 TLS errore quando si tenta di connettersi al client VPN

Problema

In passato ero in grado di connettere VPN correttamente i miei client al Client, ma ora il client VPN basato su Open 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'VPNendpoint Client verifica il certificato client rispetto all'elenco di revoca dei certificati client importato. Se l'elenco delle revoce dei certificati client è scaduto, non è possibile connettersi all'endpoint Client. VPN

Soluzione #1

Controlla la data di scadenza dell'elenco di revoca dei certificati client utilizzando lo strumento Apri. SSL

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

Nell'output vengono visualizzate la data e l'ora di scadenza. Se l'elenco delle revoce dei certificati 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'VPNendpoint Client è scaduto.

Soluzione #2

Controlla lo stato del certificato del tuo server nella AWS Certificate Manager console o utilizzando il. AWS CLI Se il certificato del server è scaduto, crea un nuovo certificato e caricalo su. ACM Per i passaggi dettagliati per generare i certificati e le chiavi del server e del client utilizzando l'utilità Open VPN easy-rsa e importarli in see. ACM Autenticazione reciproca in AWS Client VPN

In alternativa, potrebbe esserci un problema con il software open VPN based utilizzato dal client per connettersi al client. VPN Per ulteriori informazioni sulla risoluzione dei problemi relativi al software open VPN based, consulta Risoluzione dei problemi relativi alla VPN connessione del client nella Guida per l'AWS Client VPN utente.

Risoluzione dei problemi AWS Client VPN: il software client restituisce errori di nome utente e password — Autenticazione Active Directory

Problema

Uso l'autenticazione Active Directory per il mio VPN endpoint Client e prima ero in grado di connettere correttamente i miei client al Client. VPN Ora, tuttavia,i client ricevono errori di nome utente e password non validi.

Possibili cause

Se utilizzi l'autenticazione Active Directory e se hai abilitato l'autenticazione a più fattori (MFA) dopo aver distribuito il file di configurazione del client, il file non contiene le informazioni necessarie per richiedere agli utenti di inserire il proprio 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 MFA configurazione per Active Directory senza utilizzare l'VPNendpoint Client per verificare che funzioni come MFA 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 SAML risposta dell'IdP.

Soluzione

Assicurati che almeno un attributo sia incluso nella SAML risposta dell'IdP. Per ulteriori informazioni, consulta SAMLrisorse di configurazione IdP basate.

Risoluzione dei problemi AWS Client VPN: i client non riescono a connettersi: autenticazione reciproca

Problema

Uso l'autenticazione reciproca per il mio endpoint ClientVPN. I clienti stanno riscontrando errori TLS chiave di negoziazione fallita 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 nell'autenticazione federata Client VPN

Problema

Uso l'autenticazione federata per il mio endpoint Client. VPN Quando i client inseriscono il nome utente e la password nella finestra del browser del provider di identità SAML basato sul provider di identità (IdP), ricevono un errore che indica che le credenziali superano la dimensione massima supportata.

Causa

La SAML risposta restituita dall'IdP supera la dimensione massima supportata. Per ulteriori informazioni, consulta Requisiti e considerazioni per l'autenticazione federata basata 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 TCP porta 35001 per completare l'autenticazione. Per ulteriori informazioni, consulta Requisiti e considerazioni per l'autenticazione federata basata SAML.

Soluzione

Verifica che il dispositivo del client non stia bloccando la TCP porta 35001 o che 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

VPNla connessione 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 VPN server che supporta l'endpoint del clientVPN. Per ulteriori informazioni, consulta Regole e best practice per l'utilizzo AWS Client VPN.

Soluzione

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

Risoluzione dei problemi AWS Client VPN: instradamento del traffico in modo che LAN non funzioni come previsto

Problema

Il tentativo di indirizzare il traffico verso la rete locale (LAN) non funziona come previsto quando gli intervalli di indirizzi LAN IP 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 LAN indirizzi del client non rientra negli intervalli standard sopra indicati, l'VPNendpoint Client invierà automaticamente la VPN direttiva Open «redirect-gateway block-local» al client, forzando tutto il traffico a entrare in. LAN VPN Per ulteriori informazioni, consulta Regole e best practice per l'utilizzo AWS Client VPN.

Soluzione

Se hai bisogno dell'LANaccesso durante VPN le connessioni, ti consigliamo di utilizzare gli intervalli di indirizzi convenzionali sopra elencati per il tuo. LAN

Risoluzione dei problemi AWS Client VPN: verifica del limite di larghezza di banda per un endpoint client VPN

Problema

Devo verificare il limite di larghezza di banda per un endpoint Client. VPN

Causa

La velocità effettiva dipende da diversi fattori, come la capacità della connessione dalla posizione dell'utente e la latenza di rete tra l'applicazione VPN desktop Client sul computer e l'endpoint. VPC Esiste anche un limite di larghezza di banda di 10 Mbps per connessione utente.

Soluzione

Eseguire i seguenti comandi per verificare la larghezza di banda.

```
sudo iperf3 -s -V
```

Sul client:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Cronologia dei documenti per la Client VPN User Guide

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

Modifica	Descrizione	Data
Esempi di regole di autorizzazione	Aggiunta di scenari di esempio per le regole di autorizzazione.	15 settembre 2022
VPNdurata massima della sessione	È possibile configurare una durata massima VPN della sessione 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 VPN desktop Client AWS fornite quando viene stabilita una VPN sessione per soddisfare le esigenze normative e di conformità.	20 gennaio 2022
Handler di connessioni client	È possibile abilitare il gestore di connessione client per l'VPNendpoint Client per eseguire una logica personalizzata che autorizza nuove connessioni.	4 novembre 2020
Portale self-service	Puoi abilitare un portale self-service sull'VPNendpoint Client per i tuoi clienti.	29 ottobre 2020
Accesso C lient-to-client	È possibile consentire ai client che si connettono a un VPN	29 settembre 2020

	endpoint Client di connettersi tra loro.	
SAMLAutenticazione federata basata su 2.0	È possibile autenticare VPN gli utenti Client utilizzando l'autenticazione federata basata su SAML 2.0.	19 maggio 2020
Specifica dei gruppi di sicurezza durante la creazione	È possibile specificare a VPC e gruppi di sicurezza quando si crea l'endpoint. AWS Client VPN	5 marzo 2020
Porte configurabili VPN	È possibile specificare un numero di VPN porta supportato per l' AWS Client VPN endpoint.	16 gennaio 2020
Support per l'autenticazione a più fattori () MFA	L' AWS Client VPN endpoint supporta 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.