Guía del administrador

AWS Client VPN

AWS Client VPN: Guía del administrador

Table of Contents

¿Qué es AWS Client VPN? 1
Características de Client VPN 1
Componentes de Client VPN 2
Uso de Client VPN 4
Precios de Client VPN 4
Reglas y mejores prácticas 5
Funcionamiento de Client VPN 8
Autenticación del cliente 9
Autenticación con Active Directory 10
Autenticación mutua 11
Inicio de sesión único (autenticación federada basada en SAML 2.0) 16
Autorización de cliente 22
Grupos de seguridad 22
Autorización basada en red 23
Autorización de la conexión 23
Requisitos y consideraciones 24
Interfaz de Lambda 25
Uso del controlador de la conexión del cliente para evaluar la posición 27
Habilitación del controlador de la conexión del cliente 27
Función vinculada al servicio 28
Monitoreo de errores de autorización de la conexión 28
Client VPN con un túnel dividido 28
Beneficios del túnel dividido 29
Consideraciones del enrutamiento 29
Habilitación-túnel-dividido 30
Registro de conexión 30
Entradas de registro de conexión 31
Consideraciones de escalado 33
Escenarios y ejemplos 35
Acceso a una VPC 35
Acceso a una VPC interconectada 36
Acceso a una red en las instalaciones 38
Acceder a Internet 40
lient-to-client Acceso C 41

Restringir el acceso a la red 43
Restringir el acceso mediante grupos de seguridad 43
Restringir el acceso en función de grupos de usuarios 45
Explicación introductoria 47
Requisitos previos 48
Paso 1: Generar certificados y claves de cliente y servidor 48
Paso 2: Crear un punto de enlace de Client VPN 48
Paso 3: asociar una red de destino 50
Paso 4: agregar una regla de autorización para la VPC 50
Paso 5: proporcionar acceso a Internet 51
Paso 6: verificar los requisitos del grupo de seguridad 52
Paso 7: descargar el archivo de configuración del punto de conexión de Client VPN 52
Paso 8: conectarse con el punto de conexión de Client VPN 54
Uso de Client VPN 55
Acceso al portal de autoservicio 55
Reglas de autorización 56
Agregar una regla de autorización a un punto de enlace de Client VPN 57
Quitar una regla de autorización de un punto de enlace de Client VPN 58
Visualización de reglas de autorización 58
Ejemplos de escenarios 59
Listas de revocación de certificados del cliente 71
Generación de una lista de revocación de certificados del cliente 72
Importación de una lista de revocación de certificados del cliente 74
Exportación de una lista de revocación de certificados del cliente 75
Conexiones de clientes 75
Visualización de conexiones de clientes 75
Terminación de una conexión de cliente 76
Banner de inicio de sesión de cliente 76
Configurar un banner de inicio de sesión de cliente durante la creación de un punto de conexión de Client VPN 77
Configurar un banner de inicio de sesión de cliente en un punto de conexión de Client VPN 77
Desactivar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente 78
Modificación del texto del banner existente en un punto de conexión de Client VPN 78
Ver el banner de inicio de sesión actualmente configurado 79

Puntos de enlace de Client VPN 80
Creación de un punto de enlace de Client VPN 80
Modificación de un punto de enlace de Client VPN. 84
Consulta de puntos de enlace de Client VPN 87
Eliminación de un punto de enlace de Client VPN 88
Registros de conexión 88
Activar el registro de conexión en un nuevo punto de enlace de Client VPN 89
Habilitar el registro de conexión en un punto de enlace de Client VPN existente 90
Ver registros de conexión. 90
Desactivación del registro de conexiones 91
Exportar y configurar el archivo de configuración del cliente 92
Exportar el archivo de configuración del cliente 92
Agregar el certificado de cliente y la información de la clave (autenticación mutua) 93
Rutas 94
Consideraciones sobre los túneles divididos en los puntos de enlace de Client VPN 95
Creación de una ruta de punto de enlace 95
Visualización de rutas de punto de enlace 96
Eliminación de una ruta de punto de enlace 97
Redes de destino 97
Asociación una red de destino con un punto de enlace de Client VPN 98
Aplicación de un grupo de seguridad a una red de destino 99
Desconectar una red de destino de un punto de enlace de Client VPN 100
Visualización de redes de destino 100
Duración máxima de la sesión VPN 101
Configurar la sesión VPN máxima durante la creación de un punto de conexión de Client VPN 101
Ver la duración máxima de la sesión VPN actual 102
Modificar la duración máxima de la sesión VPN 102
Seguridad 103
Protección de los datos 104
Cifrado en tránsito 105
Privacidad del tráfico entre redes 105
Administración de identidades y accesos 105
Público 106
Autenticación con identidades 107
Administración de acceso mediante políticas 110

Cómo funciona AWS Client VPN con IAM 113
Ejemplos de políticas basadas en identidades 121
Resolución de problemas 123
Uso de roles vinculados a servicios 125
Resiliencia 130
Varias redes de destino para disfrutar de una alta disponibilidad 130
Seguridad de infraestructuras 131
Prácticas recomendadas 131
Consideraciones sobre IPv6 132
Monitoreo de Client VPN 135
Métricas de CloudWatch 135
Ver métricas de CloudWatch en 138
Registros de CloudTrail 139
Información de Client VPN en CloudTrail 139
Descripción de las entradas del archivo de registro de Client VPN 140
Cuotas 142
Cuotas de Client VPN 142
Cuotas de usuarios y grupos 143
Consideraciones generales 143
Solución de problemas 144
No se puede resolver el nombre de DNS del punto de enlace de Client VPN 144
El tráfico no se divide entre subredes 145
Las reglas de autorización para grupos de Active Directory no funcionan de la forma prevista . 146
Los clientes no pueden acceder a una VPC interconectada, a Amazon S3 o a Internet 147
El acceso a una VPC interconectada, a Amazon S3 o a Internet es intermitente 150
El software cliente devuelve un error de TLS 151
El software cliente devuelve errores de nombre de usuario y contraseña (autenticación de Active Directory) 152
El software cliente devuelve errores de nombre de usuario y contraseña (autenticación federada) 152
Los clientes no pueden conectarse (autenticación mutua) 153
El cliente devuelve un error que indica que se ha superado el tamaño máximo de las credenciales (autenticación federada) 153
El cliente no abre el navegador (autenticación federada) 154
El cliente devuelve un error que indica que no hay puertos disponibles (autenticación federada) 154

La conexión VPN se interrumpió debido a una discordancia de IP 155
El enrutamiento del tráfico a la LAN no funciona según lo esperado 155
Comprobación del límite de ancho de banda de un punto de enlace de Client VPN 156
Historial de documentos 157
..... clix

¿Qué es AWS Client VPN?

AWS Client VPN es un servicio de VPN gestionado y basado en el cliente que le permite acceder de forma segura a sus AWS recursos y recursos de la red local. Con Client VPN, puede acceder a los recursos desde cualquier ubicación utilizando un cliente de VPN basado en OpenVPN.

Contenido

- Características de Client VPN
- Componentes de Client VPN
- Uso de Client VPN
- Precios de Client VPN
- Reglas y prácticas recomendadas de AWS Client VPN

Características de Client VPN

Client VPN cuenta con las siguientes características y funcionalidades:

- Conexiones seguras: proporciona una conexión TLS segura desde cualquier ubicación mediante el cliente de OpenVPN.
- Servicio gestionado: es un servicio AWS gestionado, por lo que elimina la carga operativa que supone implementar y gestionar una solución VPN de acceso remoto de terceros.
- Alta disponibilidad y elasticidad: se adapta automáticamente a la cantidad de usuarios que se conectan a sus AWS recursos y a los recursos locales.
- Autenticación: admite la autenticación del cliente a través Active Directory, la autenticación federada y la autenticación basada en certificados.
- Control más preciso: permite implementar controles de seguridad personalizados a través de reglas de acceso basadas en red. Estas reglas se pueden configurar en la granularidad de los grupos de Active Directory. También puede implementar el control de acceso mediante el uso de grupos de seguridad.
- Facilidad de uso: le permite acceder a sus AWS recursos y a los recursos locales mediante un único túnel VPN.

- Facilidad de administración: permite ver los registros de conexión, que contienen información detallada sobre los intentos de conexión del cliente. También puede administrar conexiones de clientes activas y posee la capacidad de terminar las conexiones de clientes activas.
- Integración profunda: se integra con los AWS servicios existentes, incluida AWS Directory Service Amazon VPC.

Componentes de Client VPN

Estos son los conceptos clave de Client VPN:

Punto de enlace de Client VPN

El punto de enlace de Client VPN es el recurso que usted crea y configura para activar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

Red de destino

Una red de destino es la red que se asocia a un punto de enlace de Client VPN. Una subred de una VPC es una red de destino. La asociación de una subred con un punto de enlace de Client VPN le permite establecer las sesiones de VPN. Puede asociar varias subredes con un punto de enlace de Client VPN para disfrutar de una alta disponibilidad. Todas las subredes deben ser de la misma VPC. Cada subred debe pertenecer a una zona de disponibilidad diferente.

Ruta

Cada punto de enlace de Client VPN tiene una tabla de ruta que describe las rutas de la red de destino disponibles. Cada ruta de la tabla de enrutamiento especifica la ruta del tráfico a recursos o redes específicos.

Reglas de autorización

Una regla de autorización restringe los usuarios que pueden obtener acceso a una red. Para una red especificada, se configura el grupo de proveedor de identidades (IdP) o de Active Directory al que se permite el acceso. Solo los usuarios que pertenezcan a este grupo pueden obtener acceso a la red especificada. De forma predeterminada, no hay reglas de autorización, por lo que debe configurarlas para permitir que los usuarios obtengan acceso a los recursos y redes.

Cliente

Usuario final que se conecta al punto de enlace de Client VPN para establecer una sesión de VPN. Los usuarios finales tienen que descargar un cliente OpenVPN y utilizar el archivo de configuración de la VPN de cliente que creó para establecer una sesión de VPN.

Rango de CIDR del cliente

Un rango de direcciones IP desde el que asignar direcciones IP del cliente. A cada conexión con el punto de enlace de Client VPN se le asigna una dirección IP única del intervalo CIDR del cliente. Puede elegir el rango de CIDR del cliente, por ejemplo, `10.2.0.0/16`.

Puertos de Client VPN

AWS Client VPN admite los puertos 443 y 1194 tanto para TCP como para UDP. El valor predeterminado es el puerto 443.

Interfaces de red de Client VPN

Cuando asocia una subred con el punto de enlace de Client VPN, se crean interfaces de red de Client VPN en esa subred. El tráfico que se envía a la VPC desde el punto de enlace de Client VPN se envía a través de una interfaz de red de Client VPN. A continuación, se aplica la traducción de direcciones de red de origen (SNAT), donde la dirección IP de origen del intervalo CIDR del cliente se traduce en la dirección IP de la interfaz de red de Client VPN.

Registro de conexión

Puede activar los registros de conexión en el punto de enlace de Client VPN para que los eventos de conexión queden registrados. Esta información puede resultar útil para ejecutar análisis forenses, analizar cómo se está utilizando el punto de enlace de Client VPN o depurar problemas de conexión.

Portal de autoservicio

Client VPN proporciona un portal de autoservicio como página web para que los usuarios finales descarguen la versión más reciente de AWS VPN Desktop Client y del archivo de configuración del punto de enlace de Client VPN, que contiene la configuración necesaria con el fin de conectarse al punto de enlace. El administrador del punto de enlace de Client VPN puede habilitar o desactivar un portal de autoservicio para el punto de enlace de Client VPN. El portal de autoservicio es un servicio global respaldado por paquetes de servicios en las siguientes regiones: EE. UU. Este (Virginia del Norte), Asia Pacífico (Tokio), Europa (Irlanda) y AWS GovCloud (EE. UU. Oeste).

Uso de Client VPN

Puede utilizar Client VPN de cualquiera de las siguientes formas:

AWS Management Console

La consola proporciona una interfaz de usuario basada en web para Client VPN. Si se ha registrado en una Cuenta de AWS, puede iniciar sesión en la consola de Amazon VPC y seleccionar Client VPN en el panel de navegación.

AWS Command Line Interface (AWS CLI)

AWS CLI Proporciona acceso directo a las API públicas de Client VPN. Es compatible con Windows, macOS y Linux. Para obtener más información sobre cómo empezar a utilizarlas AWS CLI, consulte la Guía del AWS Command Line Interface usuario. Para obtener más información acerca de los comandos de Client VPN, consulte la Referencia de comandos de la AWS CLI.

AWS Tools for Windows PowerShell

AWS proporciona comandos para un amplio conjunto de AWS ofertas para quienes escriben en el PowerShell entorno. Para obtener más información acerca de cómo empezar a trabajar con AWS Tools for Windows PowerShell, consulte la Guía del usuario de AWS Tools for Windows PowerShell. Para obtener más información acerca de los cmdlets de Client VPN, consulte la Referencia de Cmdlet de AWS Tools for Windows PowerShell.

API de consulta

La API de consulta HTTPS de Client VPN le brinda acceso programático a Client VPN y AWS. La API de consulta HTTPS le permite emitir solicitudes HTTPS directamente al servicio. Cuando use la API HTTPS, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulte las acciones de AWS Client VPN.

Precios de Client VPN

Se le cobra por cada asociación de puntos de conexión y cada conexión VPN cada hora. Para más información, consulte Precios de AWS Client VPN.

Se le cobra la transferencia de datos desde Amazon EC2 a Internet. Para obtener más información, consulte la sección Data Transfer (Transferencia de datos) en la página Precios bajo demanda de Amazon EC2.

Si habilita el registro de conexiones para su terminal Client VPN, debe crear un grupo de CloudWatch registros en su cuenta. Se aplican cargos por el uso de grupos de registro. Para obtener más información, consulta CloudWatch los precios de Amazon (en el nivel de pago, selecciona Logs).

Si activa el controlador de la conexión del cliente en el punto de enlace de Client VPN, debe crear e invocar una función Lambda. Se aplicarán cargos por invocar funciones de Lambda. Para más información, consulte Precios de AWS Lambda.

Los puntos finales de Client VPN están asociados a una red de destino, que es una subred de una VPC. Si esta VPC tiene un Internet Gateway, asociamos las direcciones IP elásticas con las interfaces de red elásticas (ENI) de la VPN del cliente. Estas direcciones IP elásticas se cobran como direcciones IPv4 públicas en uso. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página de precios de las VPC.

Reglas y prácticas recomendadas de AWS Client VPN

Las siguientes son las reglas y las mejores prácticas para AWS Client VPN

- Se admite un ancho de banda mínimo de 10 Mbps por conexión de usuario. El ancho de banda máximo por conexión de usuario depende del número de conexiones que se realicen al punto final Client VPN.
- Los intervalos CIDR del cliente no pueden solaparse con el CIDR local de la VPC donde se encuentra la subred asociada ni con ninguna ruta que se haya agregado manualmente a la tabla de enrutamiento del punto de enlace de Client VPN.
- Los rangos de CIDR del cliente deben tener un tamaño de bloque de al menos /22 y no tienen que ser superiores a /12.
- Una parte de las direcciones del intervalo CIDR del cliente se utiliza para permitir el modelo de disponibilidad del punto de enlace de Client VPN y no se puede asignar a los clientes. Por lo tanto, es recomendable que asigne un bloque de CIDR que contenga el doble de direcciones IP de las necesarias para permitir el máximo número de conexiones simultáneas que tenga previsto admitir en el punto de enlace de Client VPN.
- El intervalo CIDR del cliente no se puede cambiar después de crear el punto de enlace de Client VPN.
- Las subredes asociadas a un punto de enlace de Client VPN deben estar en la misma VPC.
- No puede asociar varias subredes de la misma zona de disponibilidad con un punto de enlace de Client VPN.

- Los puntos de enlace de Client VPN no admiten asociaciones de subredes en una VPC con tenencia dedicada.
- Client VPN solo admite el tráfico IPv4. Consulte Consideraciones sobre IPv6 para AWS Client VPN para obtener más detalles sobre IPv6.
- Client VPN no cumple los requisitos del estándar federal de procesamiento de información (FIPS).
- El portal de autoservicio no está disponible para los clientes que utilizan la autenticación mutua.
- No se recomienda conectarse a un punto de conexión de Client VPN mediante direcciones IP. Como Client VPN es un servicio administrado, ocasionalmente verá cambios en las direcciones IP que resuelve el nombre de DNS. Además, verá las interfaces de red Client VPN eliminadas y recreadas en sus CloudTrail registros. Se recomienda conectarse al punto de conexión de Client VPN utilizando el nombre de DNS proporcionado.
- Actualmente, no se admite el reenvío de IP cuando se utiliza la aplicación de AWS Client VPN escritorio. Otros clientes admiten el reenvío de IP.
- Client VPN no admite la replicación en varias regiones en AWS Managed Microsoft AD. El punto final Client VPN debe estar en la misma región que el AWS Managed Microsoft AD recurso.
- Si la autenticación multifactor (MFA) está deshabilitada para Active Directory, las contraseñas de usuario no pueden tener el siguiente formato.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- No puede establecer una conexión VPN desde un ordenador si hay varios usuarios conectados al sistema operativo.
- El servicio Client VPN requiere que la dirección IP a la que está conectado el cliente coincida con la IP en la que se resuelve el nombre DNS del terminal Client VPN. En otras palabras, si configura un registro DNS personalizado para el punto final Client VPN y, a continuación, reenvía el tráfico a la dirección IP real a la que se dirige el nombre DNS del punto final, esta configuración no funcionará con los clientes AWS proporcionados recientemente. Esta regla se agregó para mitigar un ataque IP al servidor como se describe aquí: TunnelCrack.
- El servicio Client VPN requiere que los rangos de direcciones IP de la red de área local (LAN) de los dispositivos cliente estén dentro de los siguientes rangos de direcciones IP privadas estándar: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, o `169.254.0.0/16`. Si se detecta que el rango de direcciones LAN del cliente se encuentra fuera de los rangos anteriores, el punto final de la VPN del cliente enviará automáticamente la directiva de OpenVPN «redirect-gateway block-local» al cliente, lo que obligará a todo el tráfico de la LAN a entrar en la VPN. Por lo tanto, si necesita acceso a una LAN durante las conexiones VPN, se recomienda que utilice los rangos de

direcciones convencionales enumerados anteriormente para su LAN. Esta regla se aplica para mitigar las posibilidades de un ataque a la red local, como se describe aquí: TunnelCrack.

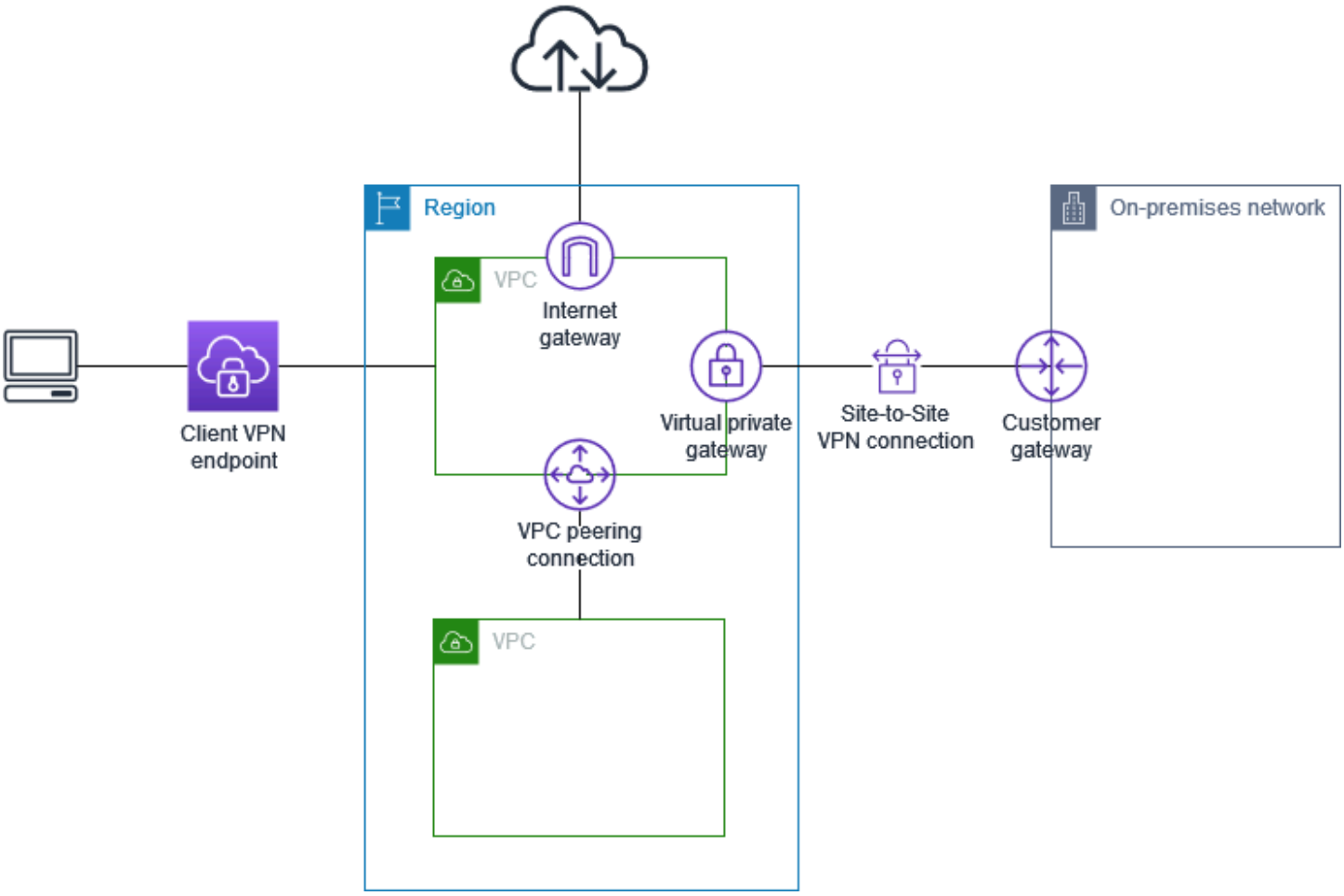
Funcionamiento de AWS Client VPN

Con AWS Client VPN, hay dos tipos de usuarios que pueden interactuar con el punto de enlace de Client VPN: administradores y clientes.

El administrador es responsable de la instalación y configuración del servicio. Esto incluye la creación del punto de enlace de Client VPN, la asociación de la red de destino y la configuración de reglas de autorización y de otras rutas (si es necesario). Una vez que el punto de enlace de Client VPN está instalado y configurado, el administrador descarga el archivo de configuración del punto de enlace de Client VPN y lo distribuye a los clientes que necesitan acceso. El archivo de configuración del punto de enlace de Client VPN contiene el nombre de DNS del punto de enlace de Client VPN y la información de autenticación necesaria para establecer una sesión de VPN. Para obtener más información sobre la configuración del servicio, consulte Introducción a AWS Client VPN.

El cliente es el usuario final. Esta es la persona que se conecta al punto de enlace de Client VPN para establecer una sesión de VPN. El cliente establece la sesión de VPN desde su equipo local o un dispositivo móvil mediante una aplicación cliente de VPN basada en OpenVPN. Después de haber establecido la sesión de VPN, puede obtener acceso de forma segura a los recursos de la VPC en la que se encuentra la subred asociada. También puede obtener acceso a otros recursos de AWS, una red en las instalaciones u otros clientes si se han configurado las reglas de autorización y ruta necesarias. Para obtener más información acerca de la conexión a un punto de enlace de Client VPN para establecer una sesión de VPN, consulte Introducción en la Guía del usuario de AWS Client VPN.

En el gráfico siguiente, se ilustra la arquitectura básica de Client VPN.



Autenticación del cliente

La autenticación del cliente se implementa en el primer punto de entrada a la AWS nube. Se utiliza para determinar si los clientes tienen permiso para conectarse al punto de enlace de Client VPN. Si la autenticación se realiza correctamente, los clientes se conectan al punto de enlace de Client VPN y establecen una sesión de VPN. Si la autenticación falla, se deniega la conexión y el cliente no podrá establecer una sesión de VPN.

Client VPN permite utilizar los siguientes tipos de autenticación de cliente:

- Autenticación con Active Directory (basada en el usuario)
- Autenticación mutua (basada en certificados)
- Inicio de sesión único (autenticación federada basada en SAML) (basada en el usuario)

Puede utilizar solo uno de los métodos mostrados anteriormente o una combinación de autenticación mutua con un método basado en usuarios como el siguiente:

- Autenticación mutua y autenticación federada
- Autenticación mutua y autenticación con Active Directory

> **Important**
>
> Para crear un punto final Client VPN, debe aprovisionar un certificado de servidor AWS Certificate Manager, independientemente del tipo de autenticación que utilice. Para obtener más información acerca de cómo crear y aprovisionar un certificado de servidor, consulte los pasos de Autenticación mutua.

Autenticación con Active Directory

Client VPN proporciona compatibilidad con Active Directory al integrarse con AWS Directory Service. Con la autenticación de Active Directory, los clientes se autentican en grupos de Active Directory existentes. Si AWS Directory Service lo usa, Client VPN puede conectarse a Active Directories existentes aprovisionados en su red local AWS o dentro de ella. Esto le permite utilizar su infraestructura de autenticación del cliente existente. Si utiliza un Active Directory local y no tiene un Microsoft AD AWS administrado existente, debe configurar un conector de Active Directory (AD Connector). Puede utilizar un servidor de Active Directory para autenticar a los usuarios. Para obtener más información acerca de la integración de Active Directory, consulte la Guía de administración de AWS Directory Service.

Client VPN admite la autenticación multifactor (MFA) cuando está habilitada para AWS Managed Microsoft AD o AD Connector. Si la MFA está activada, los clientes tienen que especificar un nombre de usuario, una contraseña y un código de MFA al conectarse a un punto de enlace de Client VPN. Para obtener más información acerca de cómo habilitar la MFA, consulte Habilitar la autenticación multifactor para AWS Managed Microsoft AD y Habilitar la autenticación multifactor para AD Connector en la Guía de administración de AWS Directory Service .

Para obtener información sobre las cuotas y las reglas para configurar usuarios y grupos en Active Directory, consulte Cuotas de usuarios y grupos.

Autenticación mutua

Con la autenticación mutua, Client VPN utiliza certificados para realizar la autenticación entre el cliente y el servidor. Los certificados son un formulario digital de identificación emitido por una entidad de certificación (CA). El servidor utiliza certificados de cliente para autenticar a los clientes cuando intentan conectarse al punto de enlace de Client VPN. Debe crear un certificado y una clave de servidor y al menos un certificado y una clave de cliente.

Debe cargar el certificado del servidor en AWS Certificate Manager (ACM) y especificarlo al crear un punto final Client VPN. Cuando se carga el certificado de servidor en ACM, también se especifica la entidad de certificación (CA). Solo tiene que cargar el certificado de cliente en ACM cuando la entidad de certificación del certificado de cliente es diferente de la entidad de certificación del certificado de servidor. Para obtener más información acerca de ACM, consulte la Guía del usuario de AWS Certificate Manager.

Puede crear una clave y un certificado de cliente diferentes para cada uno de los clientes que se conecte al punto de enlace de Client VPN. De esta forma, puede revocar un certificado de cliente específico si un usuario abandona la organización. En este caso, cuando cree el punto de enlace de Client VPN, puede especificar el ARN del certificado de servidor para el certificado de cliente, siempre que la misma entidad de certificación haya emitido los dos certificados.

> **Note**
>
> Los puntos de enlace de Client VPN solo admiten claves RSA con un tamaño de 1024 bits y 2048 bits. Además, el certificado de cliente debe tener el atributo CN en el campo Subject (Asunto).
>
> Cuando se actualicen los certificados usados con el servicio de Client VPN, ya sea mediante la rotación automática de ACM, importando manualmente un nuevo certificado o actualizaciones de metadatos al centro de identidades de IAM, el servicio de Client VPN actualizará automáticamente el punto de conexión de Client VPN con el certificado más reciente. Este es un proceso automatizado que puede tardar hasta 24 horas.

Linux/macOS

En el procedimiento siguiente, se usa easy-rsa de OpenVPN para generar los certificados y las claves del servidor y el cliente, y después se cargan la clave y el certificado del servidor en ACM. Para obtener más información, consulte Easy-RSA 3 Quickstart README.

Para generar las claves y los certificados del cliente y el servidor, y cargarlos en ACM

1. Clone el repositorio easy-rsa de OpenVPN en su equipo local y navegue a la carpeta `easy-rsa/easyrsa3`.

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

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

2. Inicialice un nuevo entorno de PKI.

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

3. Para crear una nueva entidad de certificación (CA), ejecute este comando y siga las indicaciones.

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

4. Genere el certificado y la clave del servidor.

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

5. Genere el certificado y la clave del cliente.

   Asegúrese de guardar el certificado del cliente y la clave privada del cliente, ya que los necesitará para configurar el cliente.

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

   Tiene la opción de repetir este paso para cada cliente (usuario final) que requiera un certificado y una clave de cliente.

6. Copie el certificado y la clave del servidor y el certificado y la clave del cliente en una carpeta personalizada y, a continuación, vaya a la carpeta personalizada.

   Antes de copiar los certificados y las claves, cree la carpeta personalizada; para ello, ejecute el comando `mkdir`. En el ejemplo siguiente se crea una carpeta personalizada en el directorio principal.

```
$ 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. Cargue las claves y los certificados del cliente y el servidor en ACM. No olvide cargarlos en la misma región en la que quiere crear el punto de enlace de Client VPN. Los siguientes comandos utilizan la AWS CLI para cargar los certificados. Para cargar los certificados a través de la consola de ACM en su lugar, consulte Importar un certificado en la Guía del usuario de AWS Certificate Manager .

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

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

No es necesario cargar el certificado de cliente en ACM. Si el servidor y los certificados del cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado del servidor para el servidor y el cliente cuando cree el punto de enlace de Client VPN. En los pasos anteriores, se ha utilizado la misma CA para crear ambos certificados. Sin embargo, se incluyen los pasos para cargar el certificado de cliente con ánimo de exhaustividad.

Windows

El siguiente procedimiento instala el software Easy-RSA 3.x y lo utiliza para generar los certificados y claves de servidor y cliente.

Para generar las claves y los certificados del cliente y el servidor y cargarlos en ACM

1. Abra la página de versiones de EasyRSA y descargue el archivo ZIP para extraer la versión de Windows.
2. Abra un símbolo del sistema y vaya a la ubicación en la que se extrajo la carpeta `EasyRSA-3.x`.
3. Ejecute el siguiente comando para abrir el shell de EasyRSA 3.

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

4. Inicialice un nuevo entorno de PKI.

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

5. Para crear una nueva entidad de certificación (CA), ejecute este comando y siga las indicaciones.

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

6. Genere el certificado y la clave del servidor.

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

7. Genere el certificado y la clave del cliente.

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

   Tiene la opción de repetir este paso para cada cliente (usuario final) que requiera un certificado y una clave de cliente.

8. Salga del shell de EasyRSA 3.

```
# exit
```

9. Copie el certificado y la clave del servidor y el certificado y la clave del cliente en una carpeta personalizada y, a continuación, vaya a la carpeta personalizada.

   Antes de copiar los certificados y las claves, cree la carpeta personalizada; para ello, ejecute el comando `mkdir`. En el ejemplo siguiente se crea una carpeta personalizada en su unidad 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. Cargue las claves y los certificados del cliente y el servidor en ACM. No olvide cargarlos en la misma región en la que quiere crear el punto de enlace de Client VPN. Los siguientes comandos utilizan el AWS CLI para cargar los certificados. Para cargar los certificados a través de la consola de ACM en su lugar, consulte Importar un certificado en la Guía del usuario de AWS Certificate Manager .

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

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

No es necesario cargar el certificado de cliente en ACM. Si el servidor y los certificados del cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado del servidor para el servidor y el cliente cuando cree el punto de enlace de Client VPN. En los pasos anteriores, se ha utilizado la misma CA para crear ambos certificados. Sin embargo, se incluyen los pasos para cargar el certificado de cliente con ánimo de exhaustividad.

Renovación del certificado de servidor

Puede renovar y volver a importar un certificado de servidor que haya caducado. Dependiendo de la versión de OpenVPN easy-rsa que utilice, el procedimiento variará. Consulte la documentación de renovación y revocación del certificado de Easy-RSA 3 para obtener más información.

Renueve su certificado de servidor

1. Realice una de las siguientes acciones:
   - Easy-RSA versión 3.1.x
     - Ejecute el comando de renovación de certificados.

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA versión 3.2.x

a. Ejecute el comando expire.

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

b. Firme un certificado nuevo.

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

2. Cree una carpeta personalizada, copie los nuevos archivos en ella y, a continuación, navegue hasta la carpeta.

```
$ 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. Importe los archivos nuevos en ACM. Asegúrese de importarlos en la misma región que el punto de conexión de Client VPN.

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

Inicio de sesión único (autenticación federada basada en SAML 2.0)

AWS Client VPN admite la federación de identidades con Security Assertion Markup Language 2.0 (SAML 2.0) para terminales Client VPN. Puede usar proveedores de identidad (IdPs) compatibles con SAML 2.0 para crear identidades de usuario centralizadas. A continuación, puede configurar un punto de enlace de Client VPN para utilizar la autenticación federada basada en SAML y asociarlo al proveedor de identidades. Los usuarios se conectarán entonces al punto de enlace de Client VPN utilizando sus credenciales centralizadas.

Para que el proveedor de identidades basado en SAML funcione con un punto de enlace de Client VPN, debe hacer lo siguiente.

1. Cree una aplicación basada en SAML en el IDP que elija para usarla con una aplicación existente o utilice una AWS Client VPN aplicación existente.

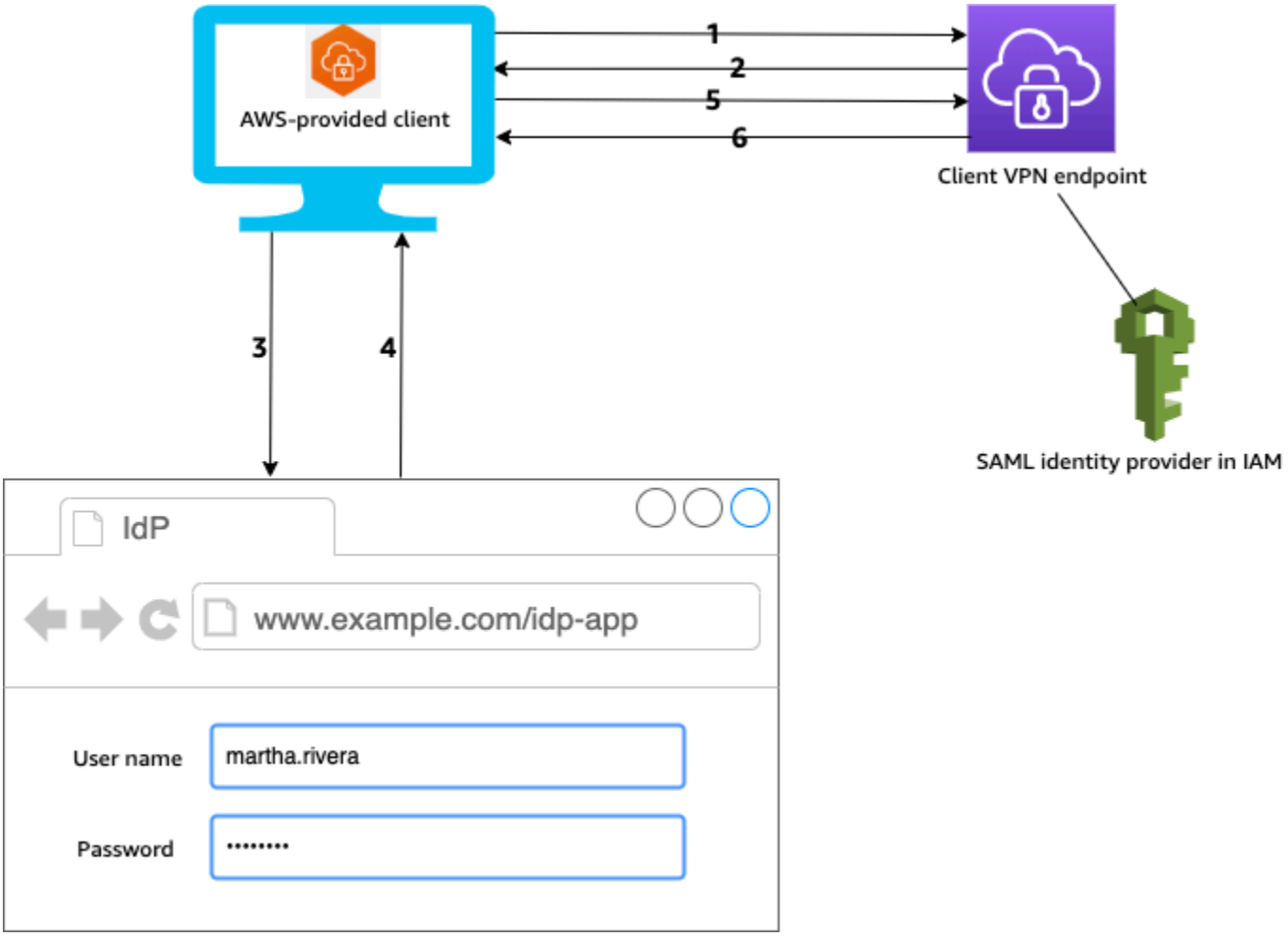
2. Configure el IdP para establecer una relación de confianza con AWS. Para obtener información sobre los recursos, consulte Recursos de configuración de IdP basados en SAML.
3. En su IdP, genere y descargue un documento de metadatos de federación que describa su organización como proveedor de identidades. Este documento XML firmado se utiliza para establecer la relación de confianza entre AWS y el IdP.
4. Cree un proveedor de identidades SAML de IAM en la misma AWS cuenta que el punto final Client VPN. El proveedor de identidades SAML de IAM define la relación entre el IDP y la AWS confianza de su organización mediante el documento de metadatos generado por el IdP. Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM. Si, más adelante, actualiza la configuración de la aplicación en el proveedor de identidades, genere un nuevo documento de metadatos y actualice el proveedor de identidades SAML de IAM.

   > **Note**
   >
   > No es necesario que cree un rol de IAM para utilizar el proveedor de identidades SAML de IAM.

5. Cree un punto de enlace de Client VPN. Especifique la autenticación federada como tipo de autenticación y el proveedor de identidades SAML de IAM que ha creado. Para obtener más información, consulte Creación de un punto de enlace de Client VPN.
6. Exporte el archivo de configuración de cliente y distribúyalo a los usuarios. Indique a los usuarios que descarguen la versión más reciente del cliente proporcionado por AWS y que lo utilicen para cargar el archivo de configuración y conectarse al punto de enlace de Client VPN. Como alternativa, si habilitó el portal de autoservicio para su terminal Client VPN, indique a sus usuarios que vayan al portal de autoservicio para obtener el archivo de configuración y AWS el cliente proporcionado. Para obtener más información, consulte Acceso al portal de autoservicio.

Flujo de trabajo de autenticación

El diagrama siguiente proporciona información general sobre el flujo de trabajo de autenticación de un punto de enlace de Client VPN que utiliza la autenticación federada basada en SAML. Cuando y configure el punto de enlace de Client VPN, tendrá que especificar el proveedor de identidades SAML de IAM.



1. El usuario abre el cliente AWS proporcionado en su dispositivo e inicia una conexión con el punto final Client VPN.
2. El punto de enlace de Client VPN devuelve al cliente una dirección URL del proveedor de identidades y una solicitud de autenticación en función de la información proporcionada en el proveedor de identidades SAML de IAM.
3. El cliente AWS proporcionado abre una nueva ventana del navegador en el dispositivo del usuario. El navegador realiza una solicitud al IdP y muestra una página de inicio de sesión.
4. El usuario escribe sus credenciales en la página de inicio de sesión y el IdP devuelve una aserción SAML firmada al cliente.
5. El cliente AWS proporcionado envía la aserción SAML al punto final de Client VPN.
6. El punto de enlace de Client VPN valida la aserción y permite o deniega el acceso al usuario.

Requisitos y consideraciones de la autenticación federada basada en SAML

A continuación, se indican las consideraciones y los requisitos relativos a la autenticación federada basada en SAML.

- Para obtener información sobre las cuotas y las reglas para configurar usuarios y grupos en un proveedor de identidades basado en SAML, consulte Cuotas de usuarios y grupos.
- La aserción SAML y los documentos de SAML deben estar firmados.
- AWS Client VPN solo admite las condiciones «AudienceRestriction» y «NotBefore y NotOnOrAfter» en las aserciones de SAML.
- El tamaño máximo admitido para las respuestas SAML es de 128 KB.
- AWS Client VPN no proporciona solicitudes de autenticación firmadas.
- No se admite el cierre de sesión único de SAML. Los usuarios pueden cerrar sesión desconectándose del cliente AWS proporcionado o usted puede finalizar las conexiones.
- Los puntos de enlace de Client VPN solo admiten un único proveedor de identidades.
- Multi-Factor Authentication (MFA) se admite si está habilitada en el IdP.
- Los usuarios deben usar el cliente AWS proporcionado para conectarse al punto final Client VPN. Deben usar la versión 1.2.0 o posterior. Para obtener más información, consulte Conectarse mediante el cliente AWS proporcionado.
- Los navegadores siguientes son compatibles con la autenticación de proveedores de identidades: Apple Safari, Google Chrome, Microsoft Edge y Mozilla Firefox.
- El cliente AWS proporcionado reserva el puerto TCP 35001 en los dispositivos de los usuarios para la respuesta SAML.
- Si el documento de metadatos del proveedor de identidades SAML de IAM se actualiza con una dirección URL incorrecta o malintencionada, pueden generarse problemas de autenticación de los usuarios o ataques de suplantación de identidad (phishing). Por lo tanto, se recomienda utilizar AWS CloudTrail para monitorear las actualizaciones que se realizan en el proveedor de identidades SAML de IAM. Para obtener más información, consulte Registro de llamadas a IAM y AWS STS con AWS CloudTrail en la Guía del usuario de IAM.
- AWS Client VPN envía una solicitud AuthN al IDP a través de un enlace de redireccionamiento HTTP. Por lo tanto, el IdP debe ser compatible con los enlaces de redirección HTTP y debe estar presente en el documento de metadatos del IdP.
- Para la aserción SAML, debe utilizar un formato de dirección de correo electrónico para el atributo `NameID`.

Recursos de configuración de IdP basados en SAML

En la siguiente tabla, se enumeran los dispositivos basados en SAML con AWS Client VPN los IdPs que hemos probado su uso y los recursos que pueden ayudarlo a configurar el IdP.

IdP	Recurso
Okta	Autentique AWS Client VPN a los usuarios con SAML
Microsoft Azure Active Directory	Para obtener más información, consulte el tutorial: Integración del inicio de sesión único (SSO) de Azure Active Directory con AWS ClientVPN en el sitio web de documentación de Microsoft.
JumpCloud	Inicio de sesión único (SSO) con AWS Client VPN
AWS IAM Identity Center	Uso del IAM Identity Center con AWS Client VPN fines de autenticación y autorización

Información del proveedor de servicios para crear una aplicación

Para crear una aplicación basada en SAML con un IdP que no aparezca en la tabla anterior, utilice la siguiente información para configurar la información del AWS Client VPN proveedor de servicios.

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

Se debe incluir al menos un atributo en la respuesta SAML del IdP. A continuación, se muestran ejemplos de atributos.

Atributo	Descripción
`FirstName`	El nombre del usuario.
`LastName`	El apellido del usuario.

Atributo	Descripción
`memberOf`	El grupo o los grupos a los que pertenece el usuario.

> **Note**
>
> El atributo `memberOf` es necesario para usar las reglas de autorización basadas en grupos de Active Directory o SAML IdP. Distingue también mayúsculas y minúsculas y se debe configurar exactamente como se especifica. Para obtener más información, consulte Autorización basada en red y Reglas de autorización.

Compatibilidad con el portal de autoservicio

Si activa el portal de autoservicio en el punto de enlace de Client VPN, los usuarios iniciarán sesión en él utilizando las credenciales del proveedor de identidades basado en SAML.

Si el proveedor de identidades admite varias URL de Assertion Consumer Service (ACS), agregue la siguiente URL de ACS a la aplicación.

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

Si utiliza el punto final Client VPN en una GovCloud región, utilice la siguiente URL de ACS en su lugar. Si usa la misma aplicación de IDP para autenticarse tanto en el estándar como en las GovCloud regiones, puede agregar ambas URL.

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

Si el proveedor de identidades no permite utilizar varias URL de ACS, haga lo siguiente:

1. Cree otra aplicación basada en SAML en el proveedor de identidades y especifique la siguiente URL de ACS.

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

2. Genere y descargue un documento de metadatos de federación.

3. Cree un proveedor de identidades SAML de IAM en la misma AWS cuenta que el punto final Client VPN. Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM.

> **Note**
>
> Cree este proveedor de identidades SAML de IAM además del que va a crear para la aplicación principal.

4. Cree el punto de enlace de Client VPN y especifique los dos proveedores de identidades SAML de IAM que ha creado.

Autorización de cliente

Client VPN admite dos tipos de autorización de cliente: los grupos de seguridad y la autorización basada en red (mediante reglas de autorización).

Grupos de seguridad

Cuando cree un punto de enlace de Client VPN, puede especificar los grupos de seguridad de una determinada VPC para aplicarlos al punto de enlace de Client VPN. Al asociar una subred con un punto de enlace de Client VPN, se aplica automáticamente el grupo de seguridad predeterminado de la VPC. Los grupos de seguridad se pueden cambiar después de crear el punto de enlace de Client VPN. Para obtener más información, consulte Aplicación de un grupo de seguridad a una red de destino. Los grupos de seguridad están asociados a interfaces de red de Client VPN.

Puede permitir que los usuarios de Client VPN obtengan acceso a las aplicaciones de una VPC agregando una regla a los grupos de seguridad de las aplicaciones que permita el tráfico desde el grupo de seguridad que se ha aplicado a la asociación.

Para agregar una regla que permita el tráfico desde el grupo de seguridad del punto de enlace de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija el grupo de seguridad asociado a su recurso o aplicación y elija Acciones, Editar reglas de entrada.

4. Seleccione Add rule (Agregar regla).
5. En Type (Tipo), seleccione All traffic (Todo el tráfico). Como opción, puede restringir el acceso a un tipo específico de tráfico, por ejemplo, SSH.

   En Source (Origen), especifique el ID del grupo de seguridad que está asociado a la red de destino (subred) del punto de enlace de Client VPN.
6. Seleccione Save rules (Guardar reglas).

Por el contrario, puede restringir el acceso de los usuarios de Client VPN no especificando el grupo de seguridad que se aplicó a la asociación o quitando la regla que hace referencia al grupo de seguridad del punto de enlace de Client VPN. Las reglas de grupos de seguridad que necesite también podrían depender del tipo de acceso de VPN que desee configurar. Para obtener más información, consulte Escenarios y ejemplos para AWS Client VPN.

Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad de su VPC en la Guía de usuario de Amazon VPC.

Autorización basada en red

La autorización basada en red se implementa mediante reglas de autorización. Por cada red en la que desee permitir el acceso, debe configurar reglas de autorización que limiten los usuarios que tienen acceso. Para una red especificada, debe configurar el grupo de Active Directory o el grupo de IdP basado en SAML que tiene permiso de acceso. Solo los usuarios que pertenecen al grupo especificado pueden obtener acceso a la red especificada. Si no va a utilizar la autenticación federada basada en SAML o Active Directory, o desea permitir el acceso a todos los usuarios, puede especificar una regla que conceda acceso a todos los clientes. Para obtener más información, consulte Reglas de autorización.

Autorización de la conexión

Puede configurar un controlador de la conexión del cliente en el punto de enlace de Client VPN. Este controlador le permite ejecutar una lógica personalizada que autorice las nuevas conexiones en función de los atributos del dispositivo, el usuario y la conexión. El controlador de la conexión del cliente se ejecuta una vez que el servicio de Client VPN ha autenticado el dispositivo y el usuario.

Para configurar un controlador de la conexión del cliente en el punto de enlace de Client VPN, cree una función de AWS Lambda que tome los atributos del dispositivo, el usuario y la conexión como

entrada y devuelva una decisión al servicio Client VPN sobre si se va a permitir o denegar una nueva conexión. Especifique la función Lambda en el punto de enlace de Client VPN. Cuando los dispositivos se conectan al punto de enlace de Client VPN, el servicio Client VPN invoca la función Lambda en su nombre. Solo las conexiones autorizadas por la función Lambda pueden conectarse al punto de enlace de Client VPN.

> **Note**
>
> Actualmente, el único tipo de controlador de conexión del cliente que se admite son las funciones Lambda.

Requisitos y consideraciones

A continuación se explican las consideraciones y los requisitos relacionados con el controlador de la conexión del cliente:

- El nombre de la función Lambda debe comenzar con el prefijo `AWSClientVPN-`.
- Las funciones Lambda calificadas son compatibles.
- La función Lambda debe estar en la misma AWS región y en la misma AWS cuenta que el punto final Client VPN.
- El tiempo de espera de la función Lambda se agota después de 30 segundos. Este valor no se puede modificar.
- La función Lambda se invoca de manera sincrónica. Se invoca después de la autenticación del dispositivo y del usuario, y antes de que se evalúen las reglas de autorización.
- Si la función Lambda se invoca para una nueva conexión y el servicio Client VPN no obtiene una respuesta esperada de la función, el servicio Client VPN deniega la solicitud de conexión. Esto puede ocurrir, por ejemplo, si la función Lambda tiene alguna limitación controlada, se agota su tiempo de espera o se producen otros errores inesperados, o bien si la respuesta de la función no tiene un formato válido.
- Es conveniente que configure la simultaneidad aprovisionada de la función Lambda para que pueda escalarse sin que se produzcan fluctuaciones en la latencia.
- Si actualiza la función Lambda, las conexiones existentes con el punto de enlace de Client VPN no se verán afectadas. Puede terminar las conexiones existentes y pedirle después a sus clientes que establezcan nuevas conexiones. Para obtener más información, consulte Terminación de una conexión de cliente.

- Si los clientes utilizan el cliente AWS proporcionado para conectarse al punto final Client VPN, deben usar la versión 1.2.6 o posterior para Windows y la versión 1.2.4 o posterior para macOS. Para obtener más información, consulte Conexión mediante el cliente proporcionado por AWS.

Interfaz de Lambda

La función Lambda toma atributos del dispositivo, del usuario y de la conexión como entrada del servicio Client VPN. A continuación, debe devolver una decisión al servicio Client VPN acerca de si se va a permitir o denegar la conexión.

Esquema de la solicitud

La función Lambda toma un blob JSON que contiene los siguientes campos como entrada.

```
{
    "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`: ID de la conexión del cliente con el punto de enlace de Client VPN.
- `endpoint-id`: ID del punto de enlace de Client VPN.
- `common-name`: identificador del dispositivo. En el certificado de cliente que va a crear para el dispositivo, el nombre común identifica de forma inequívoca el dispositivo.
- `username`: identificador del usuario, si procede. En la autenticación de Active Directory, es el nombre de usuario. En la autenticación federada basada en SAML, es `NameID`. En la autenticación mutua, este campo está vacío.
- `platform`: plataforma del sistema operativo cliente.
- `platform-version`: versión del sistema operativo. El servicio Client VPN proporciona un valor si la directiva `--push-peer-info` está presente en la configuración del cliente de OpenVPN

cuando los clientes se conectan a un punto de enlace de Client VPN y cuando el cliente ejecuta la plataforma Windows.

- `public-ip`: dirección IP pública del dispositivo de conexión.
- `client-openvpn-version`: versión de OpenVPN que se utiliza en el cliente.
- `aws-client-version`— La versión del AWS cliente.
- `groups`: identificador del grupo, si procede. Para la autenticación de Active Directory, será una lista de grupos de Active Directory. Para la autenticación federada basada en SAML, será una lista de grupos de proveedores de identidades (IdP). En la autenticación mutua, este campo está vacío.
- `schema-version`: versión del esquema. El valor predeterminado es `v3`.

Esquema de respuesta

La función Lambda debe devolver los siguientes campos.

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

- `allow`: obligatorio. Valor booleano (`true` | `false`) que indica si se va a permitir o denegar la nueva conexión.
- `error-msg-on-denied-connection`: obligatorio. Cadena de hasta 255 caracteres que se puede utilizar para proporcionar pasos y directrices a los clientes si la función Lambda deniega la conexión. Si se producen errores durante la ejecución de la función Lambda (por ejemplo, debido a una limitación controlada), se devuelve a los clientes el siguiente mensaje predeterminado.

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

- `posture-compliance-statuses`: obligatorio. Si utiliza la función Lambda para evaluar la posición, es una lista de estados del dispositivo de conexión. Los nombres de estado se definen de acuerdo con las categorías de evaluación de la posición de los dispositivos; por ejemplo, `compliant`, `quarantined`, `unknown`, etc. Un nombre puede tener 255 caracteres como máximo. Puede especificar hasta 10 estados.
- `schema-version`: obligatorio. Versión del esquema. El valor predeterminado es `v3`.

Puede utilizar la misma función Lambda con varios puntos de enlace de Client VPN de la misma región.

Para obtener más información acerca de cómo crear una función de Lambda, consulte Introducción a AWS Lambda en la Guía para desarrolladores de AWS Lambda .

Uso del controlador de la conexión del cliente para evaluar la posición

Puede utilizar el controlador de la conexión del cliente para integrar el punto de enlace de Client VPN con la solución de administración de dispositivos existente y evaluar la conformidad de la posición de los dispositivos de conexión. Para que la función Lambda trabaje como un controlador de autorización de dispositivos, utilice la autenticación mutua con el punto de enlace de Client VPN. Cree un certificado de cliente único y una clave para cada cliente (dispositivo) que se conecte al punto de enlace de Client VPN. La función Lambda puede utilizar el nombre común único del certificado de cliente (que se pasa desde el servicio Client VPN) para identificar el dispositivo y obtener su estado de conformidad de posición de la solución de administración de dispositivos. Puede utilizar la autenticación mutua combinada con la autenticación basada en usuarios.

Si lo desea, también puede realizar una evaluación básica de la posición de la propia función Lambda. Por ejemplo, puede evaluar los campos `platform` y `platform-version` que el servicio Client VPN pasa a la función Lambda.

> **Note**
>
> Si bien el controlador de conexión se puede utilizar para imponer una versión mínima de la AWS Client VPN aplicación, el campo `aws-client-version` del controlador de conexión solo se aplica a la AWS Client VPN aplicación y se rellena a partir de las variables de entorno del dispositivo del usuario.

Habilitación del controlador de la conexión del cliente

Para habilitar el controlador de la conexión del cliente, cree o modifique un punto de enlace de Client VPN y especifique el nombre de recurso de Amazon (ARN) de la función Lambda. Para obtener más información, consulte Creación de un punto de enlace de Client VPN y Modificación de un punto de enlace de Client VPN..

Función vinculada al servicio

AWS Client VPN crea automáticamente un rol vinculado al servicio en tu cuenta llamado. AWSServiceRoleForClientVPNConnections El rol tiene permisos para invocar la función Lambda cuando se realiza una conexión con el punto de enlace de Client VPN. Para obtener más información, consulte Uso de roles vinculados a servicios en Client VPN.

Monitoreo de errores de autorización de la conexión

Puede ver el estado de la autorización de las conexiones con el punto de enlace de Client VPN. Para obtener más información, consulte Visualización de conexiones de clientes.

Cuando se utiliza el controlador de la conexión del cliente para evaluar la posición, también se pueden ver los estados de conformidad de la posición de los dispositivos que se conectan al punto de enlace de Client VPN en los registros de conexión. Para obtener más información, consulte Registro de conexión.

Si un dispositivo no consigue la autorización de conexión, el campo `connection-attempt-failure-reason` de los registros de conexión devuelve uno de los siguientes motivos de error:

- `client-connect-failed`: la función Lambda impidió que se estableciera la conexión.
- `client-connect-handler-timed-out`: se agotó el tiempo de espera de la función Lambda.
- `client-connect-handler-other-execution-error`: la función Lambda encontró un error inesperado.
- `client-connect-handler-throttled`: se aplicaron limitaciones en la función Lambda.
- `client-connect-handler-invalid-response`: la función Lambda devolvió una respuesta que no era válida.
- `client-connect-handler-service-error`: se produjo un error en el lado del servicio durante el intento de conexión.

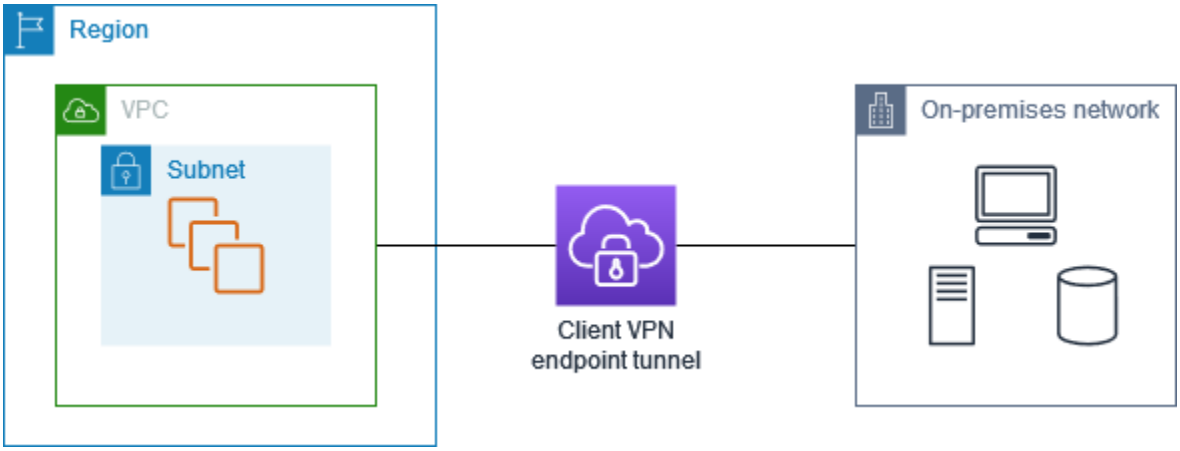
Túnel dividido en los puntos de enlace de AWS Client VPN

De forma predeterminada, cuando tiene un punto de enlace de Client VPN, todo el tráfico de los clientes se direcciona a través del túnel de Client VPN. Cuando activa un túnel dividido en el punto de enlace de Client VPN, las rutas de la tabla de enrutamiento del punto de enlace de Client VPN se insertan en el dispositivo que está conectado al punto de enlace de Client VPN. De esta forma,

el único tráfico que se direcciona a través del túnel de Client VPN es el tráfico dirigido a la red que coincide con una ruta de la tabla de enrutamiento del punto de enlace de Client VPN.

Puede utilizar un punto de enlace de Client VPN con un túnel dividido cuando no quiera que todo el tráfico de los usuarios se direccione a través del punto de enlace de Client VPN.

En el ejemplo siguiente, hay un túnel dividido activado en el punto de enlace de Client VPN. El único tráfico que se direcciona a través del túnel de Client VPN es el que tiene como destino la VPC (`172.31.0.0/16`). El tráfico con destino a los recursos locales no se direcciona a través del túnel de Client VPN.



Beneficios del túnel dividido

El túnel dividido de los puntos de enlace de Client VPN brinda los siguientes beneficios:

- Puede optimizar el enrutamiento del tráfico de los clientes al hacer que solo el tráfico destinado a AWS atraviese el túnel de la VPN.
- Puede reducir el volumen de tráfico saliente de AWS, lo que reduce el costo de transferencia de datos.

Consideraciones del enrutamiento

- Cuando se activa el modo de túnel dividido, todas las rutas de la tabla de enrutamiento del punto de conexión de Client VPN se agregan a la tabla de enrutamiento del cliente cuando se establece la conexión VPN. Esta operación es diferente del comportamiento predeterminado, que sobrescribe la tabla de enrutamiento del cliente con la entrada `0.0.0.0/0` para enrutar todo el tráfico a través de la VPN.

> **Note**
>
> No se recomienda agregar una ruta `0.0.0.0/0` a la tabla de enrutamiento del punto de conexión de Client VPN cuando se utiliza el modo de túnel dividido.

- Cuando el modo de túnel dividido está activado, cualquier modificación en la tabla de enrutamiento del punto de conexión de Client VPN provocará el restablecimiento de todas las conexiones de cliente.

Habilitación-túnel-dividido

Puede activar el túnel dividido en un punto de enlace de Client VPN nuevo o existente. Para obtener más información, consulte los siguientes temas:

- Creación de un punto de enlace de Client VPN
- Modificación de un punto de enlace de Client VPN.

Registro de conexión

El registro de conexión es una característica de AWS Client VPN que le permite capturar registros de conexión del punto de enlace de Client VPN.

Un registro de conexión contiene entradas de registro de conexión. Cada entrada del registro de conexión contiene información sobre un evento de conexión, que es cuando un cliente (usuario final) se conecta, intenta conectarse o se desconecta del punto de enlace de Client VPN. Esta información puede resultar útil para ejecutar análisis forenses, analizar cómo se está utilizando el punto de enlace de Client VPN o depurar problemas de conexión.

El registro de conexión está disponible en todas las regiones donde AWS Client VPN está disponible. Los registros de conexión se publican en un grupo de registros de CloudWatch Logs de la cuenta.

> **Note**
>
> Los intentos fallidos de autenticación mutua no se registran.

Entradas de registro de conexión

Una entrada de registro de conexión es un blob con formato JSON de pares clave-valor. A continuación, se muestra una entrada de registro de conexión de ejemplo.

```
{
    "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 entrada de registro de conexión contiene las siguientes claves:

- `connection-log-type`: tipo de entrada del registro de conexión (`connection-attempt` o `connection-reset`).
- `connection-attempt-status`: estado de la solicitud de conexión (`successful`, `failed`, `waiting-for-assertion` o `NA`).
- `connection-reset-status`: estado de un evento de restablecimiento de conexión (`NA` o `assertion-received`).
- `connection-attempt-failure-reason`: motivo del error de conexión, si procede.
- `connection-id`: ID de la conexión.
- `client-vpn-endpoint-id`: ID del punto de enlace de Client VPN con el que se realizó la conexión.

- `transport-protocol`: protocolo de transporte que se utilizó para la conexión.
- `connection-start-time`: hora de inicio de la conexión.
- `connection-last-update-time`: hora de la última actualización de la conexión. Este valor se actualiza periódicamente en los registros.
- `client-ip`: dirección IP del cliente, que se asigna desde el intervalo CIDR IPv4 del cliente al punto de enlace de Client VPN.
- `common-name`: nombre común del certificado utilizado para la autenticación basada en certificados.
- `device-type`: tipo de dispositivo utilizado por el usuario final para la conexión.
- `device-ip`: dirección IP pública del dispositivo.
- `port`: número de puerto de la conexión.
- `ingress-bytes`: número de bytes de entrada de la conexión. Este valor se actualiza periódicamente en los registros.
- `egress-bytes`: número de bytes de salida de la conexión. Este valor se actualiza periódicamente en los registros.
- `ingress-packets`: número de paquetes de entrada de la conexión. Este valor se actualiza periódicamente en los registros.
- `egress-packets`: número de paquetes de salida de la conexión. Este valor se actualiza periódicamente en los registros.
- `connection-end-time`: hora de finalización de la conexión. El valor es `NA` si la conexión sigue en curso o si el intento de conexión devolvió un error.
- `posture-compliance-statuses`: estados de conformidad de la posición devueltos por el controlador de la conexión del cliente, si procede.
- `username`: el nombre de usuario se registra cuando se utiliza la autenticación basada en el usuario (AD o SAML) para el punto de conexión.
- `connection-duration-seconds`: duración de una conexión en segundos. Igual a la diferencia entre la «hora de inicio de la conexión» y la «hora de finalización de la conexión».

Para obtener más información acerca de cómo activar los registros de conexión, consulte Trabajo con registros de conexión.

Consideraciones de escalado de Client VPN

Cuando cree un punto de enlace de Client VPN, tenga en cuenta el número máximo de conexiones VPN simultáneas que planea admitir. Debe tener en cuenta el número de clientes que admite actualmente y si sel punto de enlace de Client VPN puede satisfacer una demanda adicional si es necesario.

Los siguientes factores afectan al número máximo de conexiones VPN simultáneas que se pueden admitir en un punto de enlace de Client VPN.

Tamaño del rango CIDR del cliente

Al crear un punto de enlace de Client VPN, debe especificar un intervalo CIDR de cliente, que es un bloque CIDR IPv4 entre una máscara de red /12 y /22. A cada conexión VPN con el punto de enlace de Client VPN se le asigna una dirección IP única del intervalo CIDR del cliente. Una parte de las direcciones del intervalo CIDR del cliente se utiliza para admitir el modelo de disponibilidad del punto de enlace de Client VPN y no se puede asignar a los clientes. No puede cambiar el intervalo CIDR del cliente después de crear el punto de enlace de Client VPN.

En general, se recomienda especificar un intervalo CIDR de cliente que contenga el doble del número de direcciones IP (y, por lo tanto, conexiones simultáneas) que va a admitir en el punto de enlace de Client VPN.

Número de subredes asociadas

Cuando asocia una subred con un punto de enlace de Client VPN, permite a los usuarios establecer sesiones VPN en el punto de enlace de Client VPN. Puede asociar varias subredes con un punto de enlace de Client VPN para obtener alta disponibilidad y habilitar capacidad de conexión adicional.

A continuación se muestra el número de conexiones VPN simultáneas admitidas en función del número de asociaciones de subred para el punto de enlace de Client VPN.

Asociaciones de subred	Número de conexiones admitidas
1	7000
2	36 500
3	66 500

Asociaciones de subred	Número de conexiones admitidas
4	96 500
5	126 000

No puede asociar varias subredes de la misma zona de disponibilidad con un punto de enlace de Client VPN. Por lo tanto, el número de asociaciones de subred también depende del número de zonas de disponibilidad disponibles en una región de AWS.

Por ejemplo, si espera admitir 8000 conexiones VPN al punto de enlace de Client VPN, especifique un tamaño mínimo de intervalo CIDR de cliente de `/18` (16 384 direcciones IP) y asocie al menos 2 subredes con el punto de enlace de Client VPN.

Si no está seguro de cuál es el número de conexiones VPN esperadas para el punto de enlace de Client VPN, recomendamos que especifique un bloque `/16` CIDR de tamaño o mayor.

A fin de obtener más información acerca de las reglas y limitaciones para trabajar con rangos CIDR de cliente y redes de destino, consulte Reglas y prácticas recomendadas de AWS Client VPN.

Para obtener más información acerca de las cuotas para el punto de enlace de Client VPN, consulte AWS Cuotas de Client VPN.

Escenarios y ejemplos para AWS Client VPN

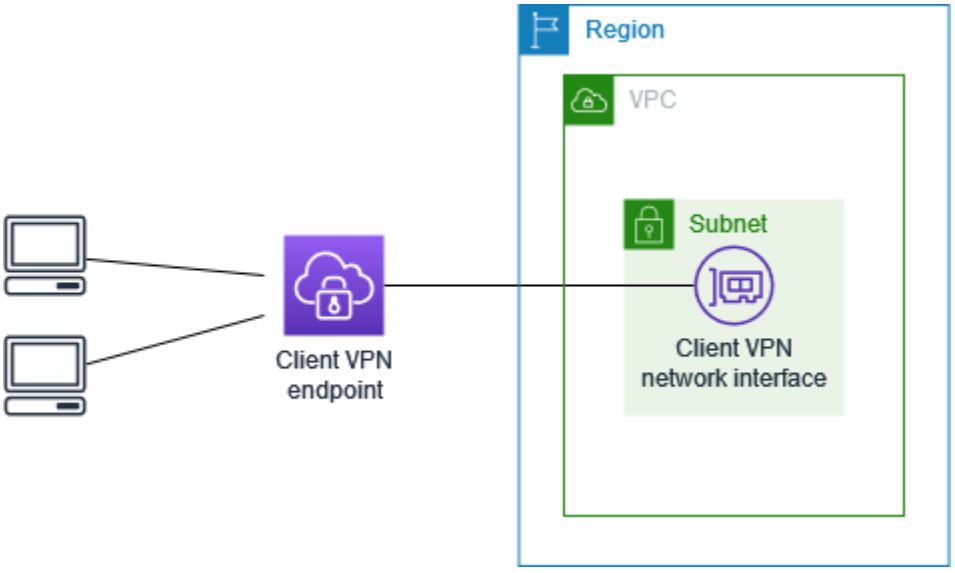
Esta sección contiene ejemplos para crear y configurar el acceso de Client VPN de sus clientes.

Contenido

- Acceso a una VPC mediante AWS Client VPN
- Acceso a una VPC mediante AWS Client VPN
- Acceso a una red en las instalaciones mediante AWS Client VPN
- Acceso a Internet mediante AWS Client VPN
- lient-to-client Acceso a C mediante AWS Client VPN
- Restricción del acceso a su red mediante AWS Client VPN

Acceso a una VPC mediante AWS Client VPN

La configuración de este escenario incluye una VPC de un solo destino. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos solo en una única VPC.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.

- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y prácticas recomendadas de AWS Client VPN.

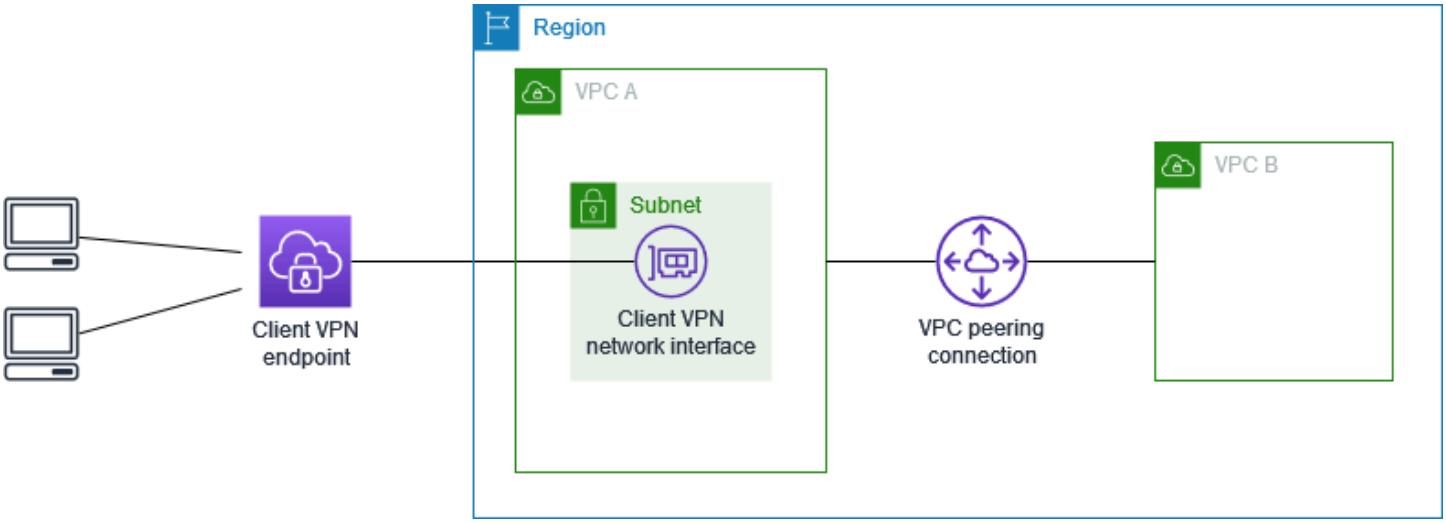
Para implementar esta configuración

1. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Creación de un punto de enlace de Client VPN.
2. Asocie la subred con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociación una red de destino con un punto de enlace de Client VPN y seleccione la subred y la VPC que identificó anteriormente.
3. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se indican en Agregar una regla de autorización a un punto de enlace de Client VPN y, en Destination network (Red de destino), escriba el intervalo CIDR IPv4 de la VPC.
4. Agregue una regla a los grupos de seguridad de sus recursos para permitir el tráfico del grupo de seguridad que se aplicó a la asociación de subred en el paso 2. Para obtener más información, consulte Grupos de seguridad.

Acceso a una VPC mediante AWS Client VPN

La configuración para este escenario incluye una VPC de destino (VPC A) que está interconectada con una VPC adicional (VPC B). Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos internos de una VPC de destino y otras VPC interconectadas con ella (como la VPC B).

> **Note**
>
> El procedimiento para permitir el acceso a una VPC interconectada que se describe a continuación solo es necesario si el punto de enlace de Client VPN se ha configurado para el modo de división de túneles. En modo de túnel completo, el acceso a la VPC interconectada de forma predeterminada está permitido.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y prácticas recomendadas de AWS Client VPN.

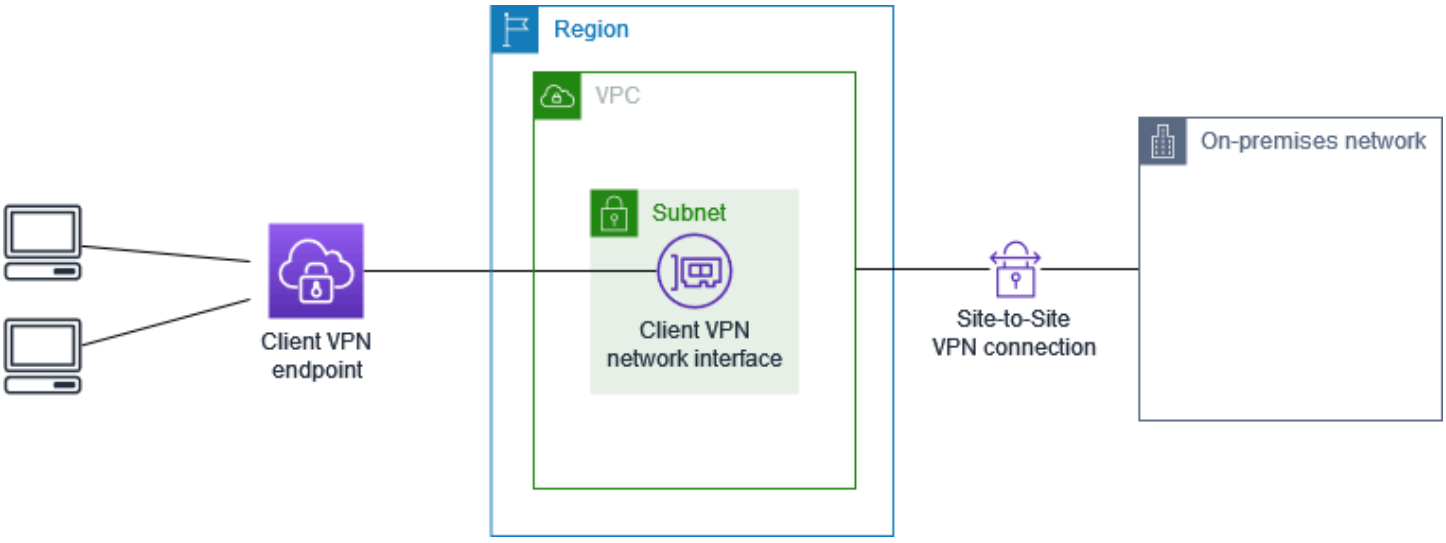
Para implementar esta configuración

1. Establezca la interconexión de VPC entre las VPC. Siga los pasos que se indican en el artículo Creación y aceptación de interconexiones de VPC de la Guía de interconexión de Amazon VPC. Confirme que las instancias de la VPC A puedan comunicarse con las instancias de la VPC B mediante la conexión de emparejamiento.
2. Cree un punto de enlace de Client VPN en la misma región que la VPC de destino. En el diagrama, es VPC A. Realice los pasos descritos en Creación de un punto de enlace de Client VPN.
3. Asocie la subred que identificó con el punto de conexión de Client VPN que ha creado. Para ello, siga los pasos que se indican en Asociación una red de destino con un punto de enlace de Client VPN, seleccione la VPC y la subred. De forma predeterminada, asociamos el grupo de seguridad predeterminado de la VPC con el punto de conexión de Client VPN. Puede asociar un grupo de seguridad diferente siguiendo los pasos que se describen en the section called “Aplicación de un grupo de seguridad a una red de destino”.

4. Agregue una regla de autorización para proporcionar a los clientes acceso a la VPC de destino. Para ello, siga los pasos que se describen en Agregar una regla de autorización a un punto de enlace de Client VPN. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR IPv4 de la VPC.
5. Añada una ruta para dirigir el tráfico hacia la VPC interconectada. En el diagrama, es VPC B. Para ello, siga los pasos que se describen en Creación de una ruta de punto de enlace. Para el Destino de la ruta, ingrese el intervalo CIDR IPv4 de la VPC interconectada. En ID de subred de VPC de destino, seleccione la subred que está asociada al punto de conexión de Client VPN.
6. Añada una regla de autorización para ofrecer a los clientes acceso a la VPC interconectada. Para ello, siga los pasos que se describen en Agregar una regla de autorización a un punto de enlace de Client VPN. En Red de destino, escriba el intervalo CIDR IPv4 de la VPC interconectada.
7. Agregue una regla a los grupos de seguridad para las instancias en la VPC A y VPC B para permitir el tráfico del grupo de seguridad que solicitó el punto de conexión de Client VPN en el paso 3. Para obtener más información, consulte Grupos de seguridad.

Acceso a una red en las instalaciones mediante AWS Client VPN

La configuración de este escenario incluye acceso a una red local únicamente. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos que hay únicamente en una red local.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y prácticas recomendadas de AWS Client VPN.

Para implementar esta configuración

1. Habilite la comunicación entre la VPC y su propia red en las instalaciones a través de una conexión Site-to-Site VPN de AWS. Para ello, siga los pasos descritos en la Introducción de la Guía del usuario de AWS Site-to-Site VPN.

   > **Note**
   >
   > Como opción, puede implementar esta situación mediante una conexión de AWS Direct Connect entre la VPC y la red en las instalaciones. Para obtener más información, consulte la Guía del usuario de AWS Direct Connect.

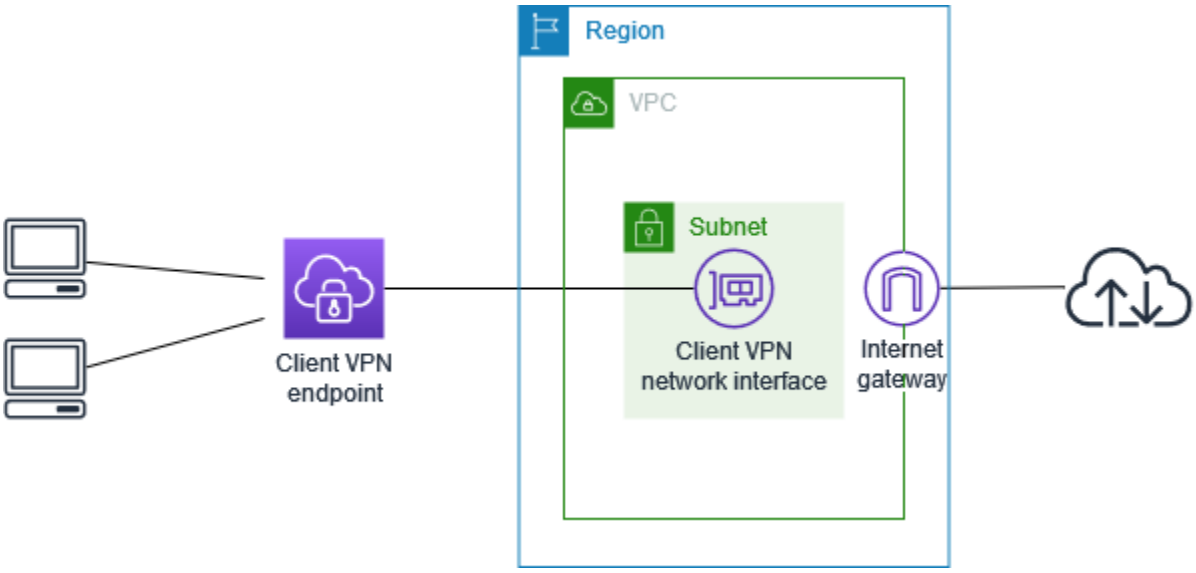
2. Pruebe la conexión de Site-to-Site VPN de AWS que creó en el paso anterior. Para ello, siga los pasos que se indican en la sección Comprobación de la conexión de Site-to-Site VPN de la Guía del usuario de AWS Site-to-Site VPN. Si la conexión de VPN funciona tal y como se esperaba, continúe en el siguiente paso.
3. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Creación de un punto de enlace de Client VPN.
4. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociación una red de destino con un punto de enlace de Client VPN y seleccione la VPC y la subred.
5. Añada una ruta que permita el acceso a la conexión de Site-to-Site VPN de AWS. Para ello, siga los pasos que se indican en Creación de una ruta de punto de enlace; a continuación, en Route destination (Destino de ruta), ingrese el rango IPv4 CIDR de la conexión de Site-to-Site VPN de AWS y, en Target VPC Subnet ID (ID de subred de la VPC de destino), seleccione la subred que asoció al punto de enlace de Client VPN.
6. Añada una regla de autorización para proporcionar a los clientes acceso a la conexión de Site-to-Site VPN de AWS. Para ello, siga los pasos que se indican en Agregar una regla de

autorización a un punto de enlace de Client VPN; en Destination network (Red de destino), ingrese el intervalo CIDR IPv4 de la conexión de Site-to-Site VPN de AWS.

Acceso a Internet mediante AWS Client VPN

La configuración de este escenario incluye una única VPC de destino y acceso a Internet. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos que están en una única VPC de destino y permitir el acceso a Internet.

Si completó el tutorial Introducción a AWS Client VPN, entonces ya ha implementado este escenario.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y prácticas recomendadas de AWS Client VPN.

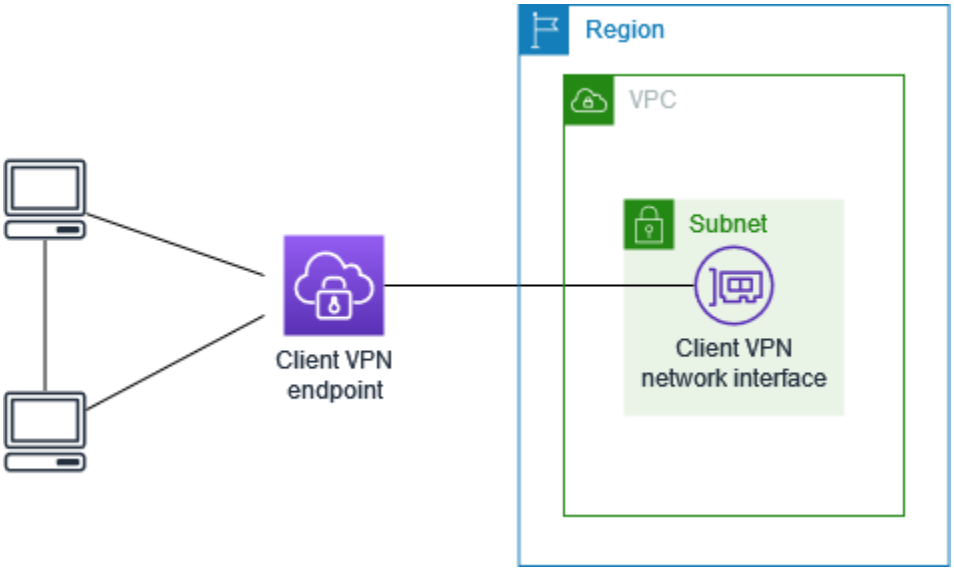
Para implementar esta configuración

1. Asegúrese de que el grupo de seguridad que va a utilizar con el punto de conexión de Client VPN permita el tráfico de Internet de salida. Para ello, agregue reglas de salida que permitan el tráfico hacia 0.0.0.0/0 para el tráfico HTTP y HTTPS.

2. Cree una gateway de Internet y asóciela a su VPC Para obtener más información, consulte Crear y asociar una gateway de Internet en la Guía del usuario de Amazon VPC.
3. Haga que su subred sea pública añadiendo una ruta al gateway de Internet en su tabla de ruteo. En la consola de VPC, elija Subnets (Subredes), seleccione la subred que desea asociar con el punto de enlace de Client VPN, haga clic en Route Table (Tabla de enrutamiento) y elija el ID de la tabla de enrutamiento. Elija Actions (Acciones), seleccione Edit routes (Editar rutas) y luego Add route (Añadir ruta). En Destination (Destino), escriba `0.0.0.0/0` y, en Target (Destino), elija la gateway de Internet del paso anterior.
4. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Creación de un punto de enlace de Client VPN.
5. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociación una red de destino con un punto de enlace de Client VPN y seleccione la VPC y la subred.
6. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se indican en Agregar una regla de autorización a un punto de enlace de Client VPN y, en Destination network to enable (Red de destino que se va a activar), escriba el intervalo CIDR IPv4 de la VPC.
7. Agregue una ruta que permita que el tráfico a Internet. Para ello, siga los pasos que se indican en Creación de una ruta de punto de enlace; a continuación, en Route destination (Destino de ruta), escriba `0.0.0.0/0` y, en Target VPC Subnet ID (ID de subred de la VPC de destino), seleccione la subred que asoció con el punto de enlace de Client VPN.
8. Agregue una regla de autorización para dar a los clientes acceso a Internet. Para ello, siga los pasos que se indican en Agregar una regla de autorización a un punto de enlace de Client VPN y, a continuación, en Destination network (Red de destino), escriba `0.0.0.0/0`.
9. Asegúrese de que los grupos de seguridad de los recursos de la VPC tengan una regla que permita el acceso desde el grupo de seguridad asociado con el punto de conexión de Client VPN. Esto permite a sus clientes acceder a los recursos de su VPC.

lient-to-client Acceso a C mediante AWS Client VPN

La configuración de este escenario permite a los clientes acceder a una sola VPC y enrutar el tráfico entre sí. Esta es la configuración recomendada si los clientes que se conectan al mismo punto de enlace de Client VPN también necesitan comunicarse entre sí. Los clientes pueden comunicarse entre sí utilizando la dirección IP única que se les asigna desde el intervalo CIDR del cliente cuando se conectan al punto de enlace de Client VPN.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y prácticas recomendadas de AWS Client VPN.

> **Note**
>
> Las reglas de autorización basadas en la red que utilizan grupos de Active Directory o grupos de IdP basados en SAML no están soportados en este escenario.

Para implementar esta configuración

1. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Creación de un punto de enlace de Client VPN.
2. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociación una red de destino con un punto de enlace de Client VPN y seleccione la VPC y la subred.

3. Agregue una ruta a la red local en la tabla de enrutamiento. Para ello, siga los pasos que se describen en Creación de una ruta de punto de enlace. En Route destination (Destino de ruta), escriba el intervalo CIDR del cliente y, en Target VPC Subnet ID (ID de subred de VPC de destino), especifique `local`.
4. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se describen en Agregar una regla de autorización a un punto de enlace de Client VPN. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR IPv4 de la VPC.
5. Agregue una regla de autorización para proporcionar a los clientes acceso al intervalo CIDR del cliente. Para ello, siga los pasos que se describen en Agregar una regla de autorización a un punto de enlace de Client VPN. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR del cliente.

Restricción del acceso a su red mediante AWS Client VPN

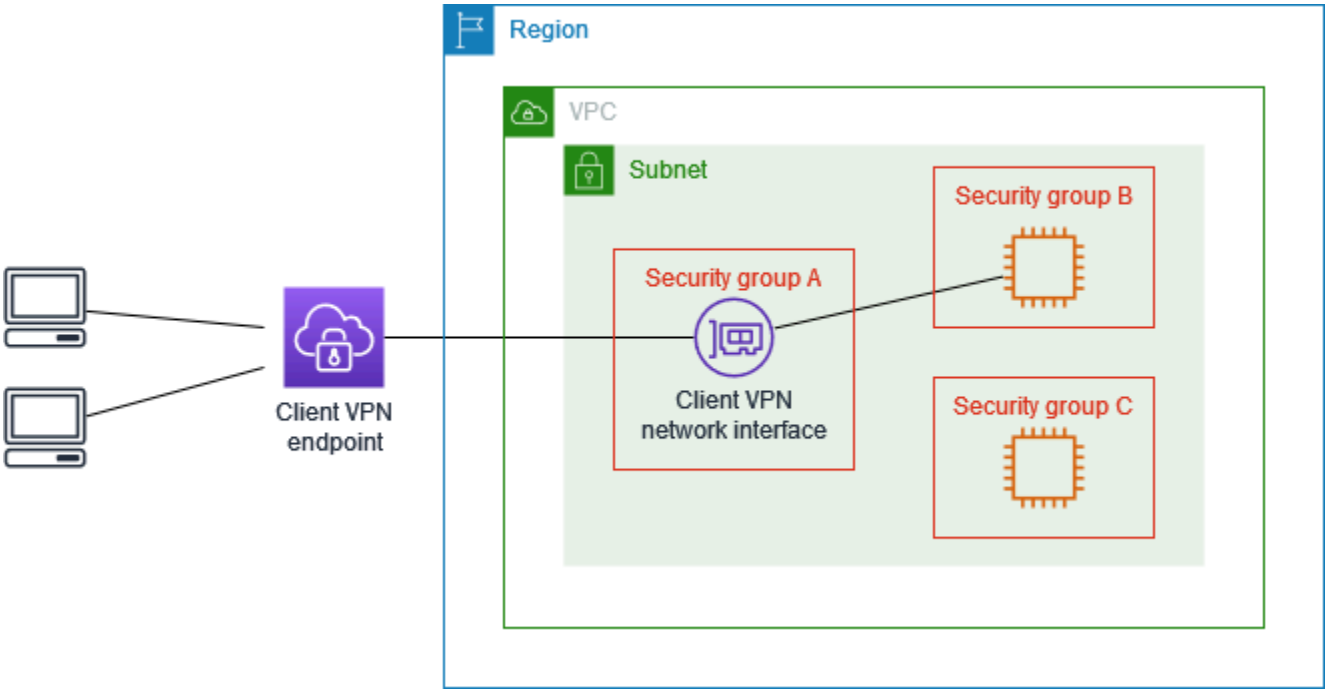
Puede configurar el punto de enlace de Client VPN para restringir el acceso a recursos específicos de la VPC. En la autenticación basada en usuarios, también puede restringir el acceso a partes de la red en función del grupo de usuarios que accede al punto de enlace de Client VPN.

Restringir el acceso mediante grupos de seguridad

Puede conceder o denegar el acceso a recursos específicos de la VPC. Para ello, solo tiene que agregar o quitar reglas del grupo de seguridad que hagan referencia al grupo de seguridad que se aplicó a la asociación de red de destino (el grupo de seguridad de Client VPN). Esta configuración se amplía en el escenario que se describe en Acceso a una VPC mediante AWS Client VPN. Esta configuración se aplica de manera adicional a la regla de autorización configurada en ese escenario.

Para conceder acceso a un recurso específico, identifique el grupo de seguridad asociado a la instancia en la que se está ejecutando el recurso. A continuación, cree una regla que permita el tráfico desde el grupo de seguridad de Client VPN.

En el siguiente diagrama, el grupo de seguridad A es el grupo de seguridad de Client VPN, el grupo de seguridad B está asociado a una instancia de EC2 y el grupo de seguridad C está asociado a una instancia de EC2. Si añade una regla al grupo de seguridad B que permita el acceso desde el grupo de seguridad A, los clientes podrán acceder a la instancia asociada al grupo de seguridad B. Si el grupo de seguridad C no tiene una regla que permita el acceso desde el grupo de seguridad A, los clientes no podrán acceder a la instancia asociada al grupo de seguridad C.



Antes de comenzar, compruebe si el grupo de seguridad de Client VPN está asociado a otros recursos de la VPC. Si agrega o quita reglas que hacen referencia al grupo de seguridad de Client VPN, puede darse el caso de que también conceda o deniegue el acceso a otros recursos asociados. Para evitar esto, utilice un grupo de seguridad creado específicamente para el punto de enlace de Client VPN.

Para crear una regla de un grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija el grupo de seguridad asociado a la instancia en la que se ejecute el recurso.
4. Seleccione Actions (Acciones), Edit inbound rules (Editar reglas de entrada).
5. Elija Add Rule (Agregar regla) y, a continuación, haga lo siguiente:
   - En Type (Tipo), elija All traffic (Todo el tráfico) o un tipo específico de tráfico que desee permitir.
   - En Source (Origen), elija Custom (Personalizado) y, a continuación, escriba o elija el ID del grupo de seguridad de Client VPN.
6. Seleccione Save rules (Guardar reglas).

Para quitar el acceso a un recurso específico, compruebe el grupo de seguridad asociado a la instancia en la que se está ejecutando el recurso. Si hay una regla que permite el tráfico desde el grupo de seguridad de Client VPN, elimínela.

Para comprobar las reglas del grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione Inbound Rules (Reglas de entrada).
4. Revise la lista de reglas. Si hay una regla en la que Source (Origen) es el grupo de seguridad de Client VPN, elija Edit rules (Editar reglas) y, en la regla, haga clic en Delete (Eliminar) (el icono x). Seleccione Guardar reglas.

Restringir el acceso en función de grupos de usuarios

Si el punto de enlace de Client VPN está configurado para utilizar la autenticación basada en usuarios, puede permitir que grupos específicos de usuarios tengan acceso a partes concretas de la red. Para ello, siga los pasos que se describen a continuación:

1. Configure usuarios y grupos en AWS Directory Service o en su IdP. Para obtener más información, consulte los siguientes temas:
   - Autenticación con Active Directory
   - Requisitos y consideraciones de la autenticación federada basada en SAML
2. Cree una regla de autorización para el punto de enlace de Client VPN que permita que un grupo especificado pueda acceder a toda la red o a parte ella. Para obtener más información, consulte Reglas de autorización.

Si el punto de enlace de Client VPN está configurado para utilizar la autenticación mutua, no se pueden configurar grupos de usuarios. Al crear una regla de autorización, debe conceder acceso a todos los usuarios. Para permitir que grupos específicos de usuarios tengan acceso a partes específicas de la red, puede crear varios puntos de enlace de Client VPN. Por ejemplo, para cada grupo de usuarios que tiene acceso a la red, haga lo siguiente:

1. Cree un conjunto de certificados y claves de servidor y cliente para ese grupo de usuarios. Para obtener más información, consulte Autenticación mutua.

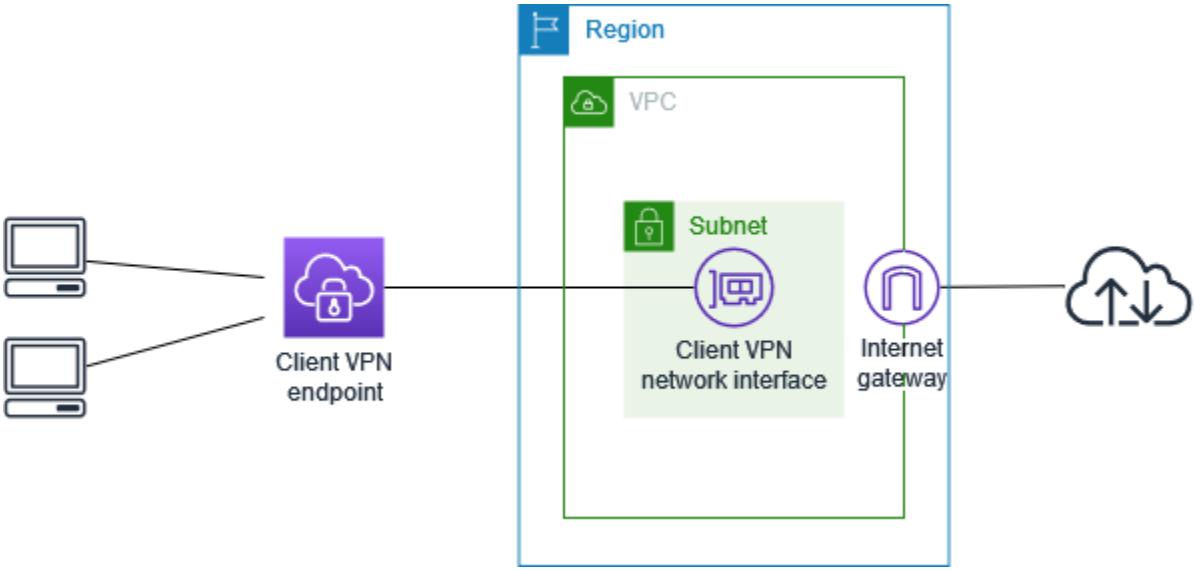
2. Cree un punto de enlace de Client VPN. Para obtener más información, consulte Creación de un punto de enlace de Client VPN.
3. Cree una regla de autorización que conceda acceso a la totalidad o parte de la red. Por ejemplo, si se trata de un punto de enlace de Client VPN que van a utilizar los administradores, puede crear una regla de autorización que conceda acceso a toda la red. Para obtener más información, consulte Agregar una regla de autorización a un punto de enlace de Client VPN.

Introducción a AWS Client VPN

En este tutorial, va a crear un punto de conexión de Client VPN que hace lo siguiente:

- Proporciona a todos los clientes acceso a una única VPC.
- Proporciona a todos los clientes acceso a Internet.
- Utiliza la autenticación mutua.

En el siguiente diagrama, se ilustra la configuración de la VPC y el punto de enlace de Client VPN después de completar este tutorial.



Pasos

- Requisitos previos
- Paso 1: Generar certificados y claves de cliente y servidor
- Paso 2: Crear un punto de enlace de Client VPN
- Paso 3: asociar una red de destino
- Paso 4: agregar una regla de autorización para la VPC
- Paso 5: proporcionar acceso a Internet
- Paso 6: verificar los requisitos del grupo de seguridad
- Paso 7: descargar el archivo de configuración del punto de conexión de Client VPN
- Paso 8: conectarse con el punto de conexión de Client VPN

Requisitos previos

Antes de comenzar este tutorial de introducción, asegúrese de tener lo siguiente:

- Los permisos necesarios para trabajar con puntos de enlace de Client VPN.
- Los permisos necesarios para importar certificados en AWS Certificate Manager.
- Una VPC con al menos una subred y un gateway de Internet. La tabla de rutas asociada a la subred debe tener una ruta al gateway de Internet.

Paso 1: Generar certificados y claves de cliente y servidor

En este tutorial, se utiliza la autenticación mutua. Con la autenticación mutua, Client VPN utiliza certificados para realizar la autenticación entre los clientes y el punto de conexión de Client VPN. Deberá tener un certificado y una clave de servidor y al menos un certificado y una clave de cliente. Como mínimo, será necesario importar el certificado del servidor en AWS Certificate Manager (ACM) y especificarlo cuando cree el punto de conexión de Client VPN. La importación del certificado de cliente en ACM es opcional.

Si aún no dispone de certificados para utilizarlos con este fin, se pueden crear con la utilidad easy-rsa de OpenVPN. Para conocer los pasos detallados para generar los certificados y las claves del servidor y del cliente mediante la utilidad easy-rsa de OpenVPN e importarlos a ACM, consulte Autenticación mutua.

> **Note**
>
> El certificado del servidor se debe aprovisionar o importar en AWS Certificate Manager (ACM) en la misma región de AWS en la que se va a crear el punto de conexión de Client VPN.

Paso 2: Crear un punto de enlace de Client VPN

El punto de enlace de Client VPN es el recurso que usted crea y configura para activar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

Para crear un punto de enlace de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, elija Client VPN Endpoints (Puntos de conexión de Client VPN) y Create Client VPN Endpoint (Crear punto de conexión de Client VPN).
3. (Opcional) Escriba una etiqueta de nombre y una descripción del punto de conexión de Client VPN.
4. En Client IPv4 CIDR (CIDR de IPv4 de cliente), especifique el rango de direcciones IP, en notación CIDR, desde el que se van a asignar las direcciones IP del cliente.

   > **Note**
   >
   > El intervalo de direcciones no puede solaparse al intervalo de direcciones de la red de destino, al intervalo de direcciones de la VPC ni a ninguna de las rutas que se asociarán con el punto de conexión de Client VPN. El intervalo de direcciones del cliente debe tener un tamaño de bloque de CIDR mínimo de /22 y no superior a /12. No puede cambiar el intervalo de direcciones del cliente después de crear el punto de conexión de Client VPN.

5. En Server certificate ARN (ARN del certificado del servidor), seleccione el ARN del certificado del servidor que generó en Paso 1.
6. En Authentication options (Opciones de autenticación), elija Use mutual authentication (Usar autenticación mutua) y, a continuación, en Client certificate ARN (ARN de certificado de cliente), seleccione el ARN del certificado que desea utilizar como certificado de cliente.

   Si los certificados de servidor y de cliente están firmados por la misma entidad de certificación (CA), tiene la opción de especificar el ARN del certificado de servidor para los certificados de cliente y de servidor. En este escenario, cualquier certificado de cliente que se corresponda con el certificado de servidor se puede utilizar para la autenticación.
7. Mantenga los demás valores predeterminados y elija Create Client VPN Endpoint (Crear punto de conexión de Client VPN).

Después de crear el punto de enlace de Client VPN, su estado es `pending-associate`. Los clientes solo pueden establecer una conexión de VPN después de que se haya asociado al menos una red de destino.

Para obtener más información sobre las opciones que puede especificar para un punto de conexión de Client VPN, consulte Creación de un punto de enlace de Client VPN.

Paso 3: asociar una red de destino

Para permitir que los clientes establezcan una sesión de VPN, debe asociar una red de destino con el punto de conexión de Client VPN. Una red de destino es una subred en una VPC.

Para asociar una red de destino con el punto de conexión de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó en el procedimiento anterior y, a continuación, elija Target network associations (Asociaciones de red de destino), Associate target network (Asociar red de destino).
4. En VPC, elija la VPC en la que se encuentra la subred.
5. En Choose a subnet to associate (Elija una subred para asociar), elija la subred que desee asociar con el punto de conexión de Client VPN.
6. Elija Associate target network (Asociar red de destino).
7. Si las reglas de autorización lo permiten, basta con una asociación de subred para que los clientes obtengan acceso a toda la red de una VPC. Puede asociar más subredes para ofrecer una alta disponibilidad en caso de que una de las zonas de disponibilidad deje de funcionar.

Al asociar la primera subred con el punto de enlace de Client VPN, sucede lo siguiente:

- El estado del punto de enlace de Client VPN cambia a `available`. Los clientes ahora pueden establecer una conexión de VPN, pero no pueden acceder a los recursos de la VPC hasta que se añadan las reglas de autorización.
- La ruta local de la VPC se agrega automáticamente a la tabla de enrutamiento del punto de enlace de Client VPN.
- El grupo de seguridad predeterminado de la VPC se aplica automáticamente para el punto de conexión de Client VPN.

Paso 4: agregar una regla de autorización para la VPC

Para que los clientes puedan acceder a la VPC, es necesario que haya una ruta a la VPC en la tabla de enrutamiento del punto de conexión de Client VPN y una regla de autorización. La ruta ya

se agregó automáticamente en el paso anterior. En este tutorial, deseamos conceder a todos los usuarios el acceso a la VPC.

Para agregar una regla de autorización para la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que se agregará la regla de autorización. Elija Authorization rules (Reglas de autorización) y, a continuación, Add authorization rule (Agregar regla de autorización).
4. En Destination network to enable access (Red de destino para habilitar el acceso), ingrese el CIDR de la red para la que desea conceder acceso. Por ejemplo, para permitir el acceso a toda la VPC, especifique el bloque CIDR IPv4 de la VPC.
5. En Grant access to (Conceder acceso a), elija Allow access to all users (Permitir acceso a todos los usuarios).
6. (Opcional) En Description (Descripción), ingrese una breve descripción de la regla de autorización.
7. Seleccione Add authorization rule (Añadir regla de autorización).

Paso 5: proporcionar acceso a Internet

Puede proporcionar acceso a redes adicionales conectadas a la VPC, como servicios de AWS, VPC interconectadas, redes en las instalaciones e Internet. Para cada red adicional, se agrega una ruta a la red en la tabla de enrutamiento del punto de conexión de Client VPN y se configura una regla de autorización para conceder acceso a los clientes.

Para este tutorial, deseamos conceder a todos los usuarios acceso a Internet y también a la VPC. Ya ha configurado el acceso a la VPC, así que este paso es para el acceso a Internet.

Para proporcionar acceso a Internet

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó para este tutorial. Elija Route Table (Tabla de enrutamiento) y, a continuación, Create Route (Crear ruta).

4. En Route destination (Destino de ruta), escriba `0.0.0.0/0`. En Subnet ID for target network association (ID de subred para la asociación de red de destino), especifique el ID de la subred a través de la cual se va a dirigir el tráfico.
5. Elija Create Route (Crear ruta).
6. Elija Authorization rules (Reglas de autorización) y, a continuación, Add authorization rule (Agregar regla de autorización).
7. En Destination network to enable access (Red de destino para permitir el acceso), ingrese `0.0.0.0/0` y elija Allow access to all users (Permitir acceso a todos los usuarios).
8. Seleccione Add authorization rule (Añadir regla de autorización).

Paso 6: verificar los requisitos del grupo de seguridad

En este tutorial, no se especificaron grupos de seguridad durante la creación del punto de conexión de Client VPN en el paso 2. Esto significa que el grupo de seguridad predeterminado para la VPC se aplica automáticamente al punto de conexión de Client VPN cuando se asocia una red de destino. Como resultado, el grupo de seguridad predeterminado para la VPC debería estar ahora asociado con el punto de conexión de Client VPN.

Verifique los siguientes requisitos del grupo de seguridad

- Que el grupo de seguridad asociado a la subred por la que está dirigiendo el tráfico (en este caso, el grupo de seguridad de la VPC predeterminada) permita el tráfico saliente hacia Internet. Para ello, agregue una regla de salida que permita todo el tráfico hacia el destino `0.0.0.0/0`.
- Que los grupos de seguridad de los recursos de su VPC tengan una regla que permita el acceso desde el grupo de seguridad que se aplica al punto de conexión de Client VPN (en este caso, el grupo de seguridad predeterminado de VPC). Esto permite a sus clientes acceder a los recursos de su VPC.

Para obtener más información, consulte Grupos de seguridad.

Paso 7: descargar el archivo de configuración del punto de conexión de Client VPN

El siguiente paso que tiene que realizar es descargar y preparar el archivo de configuración del punto de conexión de Client VPN. El archivo de configuración contiene los detalles del punto de conexión

de Client VPN y la información del certificado necesaria para establecer una conexión de VPN. Este archivo se proporciona a los usuarios finales que necesitan conectarse al punto de conexión de Client VPN. El usuario final utiliza el archivo para configurar su aplicación cliente de VPN.

Para descargar y preparar el archivo de configuración del punto de enlace de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó para este tutorial y elija Download client configuration (Descargar la configuración del cliente).
4. Busque el certificado de cliente y la clave que se generaron en el paso 1. El certificado y la clave del cliente se encuentran en las siguientes ubicaciones del repositorio easy-rsa de OpenVPN clonado:
   - Certificado del client — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Clave de client — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Abra el archivo de configuración del punto de enlace de Client VPN con el editor de texto que prefiera. Agregue las etiquetas `<cert></cert>` y `<key></key>` al archivo. Coloque el contenido del certificado del cliente y el contenido de la clave privada entre las etiquetas correspondientes, del siguiente modo:

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

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

6. Guarde y cierre el archivo de configuración del punto de enlace de Client VPN.
7. Distribuya el archivo de configuración del punto de conexión de Client VPN a sus usuarios finales.

Para obtener más información sobre el archivo de configuración del punto de enlace de Client VPN, consulte Exportar y configurar el archivo de configuración del cliente.

Paso 8: conectarse con el punto de conexión de Client VPN

Puede conectarse al punto de conexión de Client VPN utilizando el cliente proporcionado por AWS u otra aplicación cliente basada en OpenVPN y el archivo de configuración que acaba de crear. Para obtener más información, consulte la Guía del usuario de AWS Client VPN.

Uso de AWS Client VPN

En los siguientes temas se explica cómo trabajar con Client VPN.

Contenido

- Acceso al portal de autoservicio
- Reglas de autorización
- Listas de revocación de certificados del cliente
- Conexiones de clientes
- Banner de inicio de sesión de cliente
- Puntos de enlace de Client VPN
- Trabajo con registros de conexión
- Exportar y configurar el archivo de configuración del cliente
- Rutas
- Redes de destino
- Duración máxima de la sesión VPN

Acceso al portal de autoservicio

Si ha habilitado el portal de autoservicio en el punto de enlace de Client VPN, puede proporcionar a sus clientes una URL del portal de autoservicio. Los clientes pueden acceder al portal en un explorador web y utilizar sus credenciales basadas en usuarios para iniciar sesión. En el portal, los clientes pueden descargar el archivo de configuración del punto de enlace de Client VPN y la versión más reciente del cliente proporcionado por AWS.

Se aplican las siguientes reglas:

- El portal de autoservicio no está disponible para los clientes que utilizan la autenticación mutua.
- El archivo de configuración que está disponible en el portal de autoservicio es el mismo que se exporta a través de la consola de Amazon VPC o la AWS CLI. Si necesita personalizar el archivo de configuración antes de distribuirlo a los clientes, deberá encargarse usted mismo de distribuir el archivo personalizado a los clientes.

- Debe habilitar la opción del portal de autoservicio en el punto de enlace de Client VPN o los clientes no podrán acceder al portal. Si esta opción no está habilitada, puede modificar el punto de enlace de Client VPN para habilitarla.

Una vez que la opción del portal de autoservicio esté habilitada, proporcione a sus clientes una de las siguientes direcciones URL:

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

  Si los clientes acceden al portal mediante esta dirección URL, deben especificar el ID del punto de enlace de Client VPN para poder iniciar sesión.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  En la URL anterior, sustituya *<endpoint-id>* por el ID del punto de enlace de Client VPN; por ejemplo, `cvpn-endpoint-0123456abcd123456`.

También puede ver la URL del portal de autoservicio en la salida del comando describe-client-vpn-endpoints de la AWS CLI. Por otro lado, la URL también está disponible en la pestaña Details (Detalles) de la página VPN Client Endpoints (Puntos de conexión de Client VPN) de la consola de Amazon VPC.

Para obtener más información acerca de cómo configurar el portal de autoservicio para usarlo con la autenticación federada, consulte Compatibilidad con el portal de autoservicio.

Reglas de autorización

Las reglas de autorización actúan como reglas de firewall que conceden acceso a redes. Al agregar reglas de autorización, debe conceder a los clientes específicos acceso a la red especificada. Debe tener una regla de autorización para cada red a la que desea conceder acceso. Puede agregar reglas de autorización a un punto de enlace de Client VPN a través de la consola y la AWS CLI.

> **Note**
>
> Client VPN utiliza la coincidencia de prefijos más larga al evaluar las reglas de autorización. Consulte el tema sobre solución de problemas Las reglas de autorización para grupos de Active Directory no funcionan de la forma prevista y Prioridad de la ruta en la Guía del usuario de Amazon VPC para obtener más información.

Contenido

- Agregar una regla de autorización a un punto de enlace de Client VPN
- Quitar una regla de autorización de un punto de enlace de Client VPN
- Visualización de reglas de autorización
- Escenarios de ejemplo para las reglas de autorización

Agregar una regla de autorización a un punto de enlace de Client VPN

Agregar una regla de autorización a un punto de enlace de Client VPN con AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que va a agregar la regla de autorización y elija Authorization rules (Reglas de autorización) y Add authorization rule (Agregar regla de autorización).
4. En Destination network to enable access (Red de destino para habilitar acceso), ingrese la dirección IP, en notación CIDR, de la red a la que desea que accedan los usuarios (por ejemplo, el bloque de CIDR de la VPC).
5. Especifique qué clientes pueden obtener acceso a la red especificada. En For grant access to (Para conceder acceso a), realice una de las siguientes operaciones::

   - Para conceder acceso a todos los clientes, seleccione Allow access to all users (Permitir acceso a todos los usuarios).
   - Para restringir el acceso a clientes específicos, elija Permitir acceso a los usuarios de un grupo de acceso específico y, a continuación, en ID de grupo de acceso, escriba el ID del grupo al que se va a conceder acceso. Por ejemplo, el identificador de seguridad (SID) de un grupo de Active Directory o bien el ID o el nombre de un grupo definido en un proveedor de identidades (IdP) basado en SAML.
     - (Active Directory) Para obtener el SID, puede utilizar el cmdlet de Microsoft Powershell Get-ADGroup , por ejemplo:

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

También puede abrir la herramienta de usuarios y equipos de Active Directory, consultar las propiedades del grupo, ir a la pestaña del editor de atributos y obtener el valor de `objectSID`. Si es necesario, primero elija View (Ver), Advanced Features (Características avanzadas) para habilitar la pestaña del editor de atributos.

- (Autenticación federada basada en SAML) El nombre o ID de grupo debe coincidir con la información del atributo de grupo que se devuelve en la aserción SAML.

6. En Description (Descripción), escriba una breve descripción de la regla de autorización.
7. Seleccione Add authorization rule (Añadir regla de autorización).

Agregar una regla de autorización a un punto de enlace de Client VPN (AWS CLI)

Utilice el comando authorize-client-vpn-ingress.

Quitar una regla de autorización de un punto de enlace de Client VPN

Al eliminar una regla de autorización, se elimina el acceso a la red especificada.

Puede eliminar reglas de autorización de un punto de enlace de Client VPN a través de la consola y la AWS CLI.

Para eliminar una regla de autorización de un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN en el que se agregó la regla de autorización y elija Authorization rules (Reglas de autorización).
4. Seleccione la regla de autorización a eliminar, elija Remove authorization rule (Eliminar regla de autorización) y elija Remove authorization rule (Eliminar regla de autorización).

Para quitar una regla de autorización de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando revoke-client-vpn-ingress.

Visualización de reglas de autorización

Puede consultar las reglas de autorización de un punto de enlace de Client VPN específico a través de la consola y AWS CLI.

Para ver las reglas de autorización (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN cuyas reglas de autorización desee ver y elija Authorization rules (Reglas de autorización).

Para ver las reglas de autorización (AWS CLI)

Utilice el comando describe-client-vpn-authorization-rules.

Escenarios de ejemplo para las reglas de autorización

En esta sección se describe cómo funcionan las reglas de autorización para AWS Client VPN. Incluye puntos clave para entender las reglas de autorización, una arquitectura de ejemplo y la explicación de escenarios de ejemplo que se asignan a la arquitectura de ejemplo.

Contenido

- Puntos clave para entender las reglas de autorización
- Ejemplo de arquitectura para escenarios de reglas de autorización
- Escenario 1: acceso a un único destino
- Escenario 2: uso de cualquier CIDR de destino (0.0.0.0/0)
- Escenario 3: coincidencia de prefijo IP más largo
- Escenario 4: CIDR superpuesto (mismo grupo)
- Escenario 5: regla adicional 0.0.0.0/0
- Escenario 6: agregar regla para 192.168.0.0/24
- Escenario 7: acceso para todos los grupos de usuarios

Puntos clave para entender las reglas de autorización

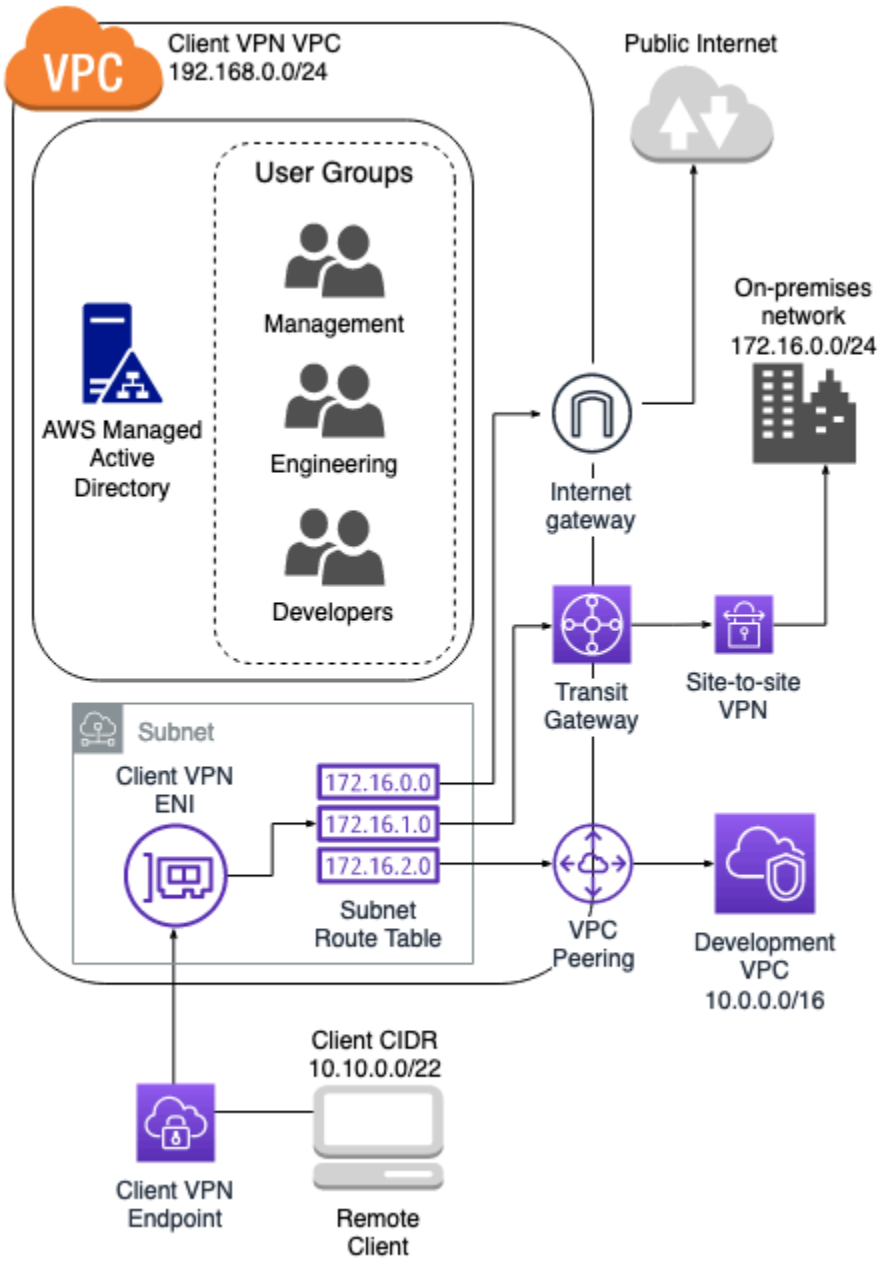
En los siguientes puntos se explican algunos de los comportamientos de las reglas de autorización:

- Para permitir el acceso a una red de destino, debe agregarse explícitamente una regla de autorización. El comportamiento predeterminado es denegar el acceso.
- No puede agregar una regla de autorización para restringir el acceso a una red de destino.

- El CIDR `0.0.0.0/0` se gestiona como un caso especial. Se procesa en último lugar, independientemente del orden en que se crearon las reglas de autorización.
- El CIDR `0.0.0.0/0` puede considerarse como "cualquier destino" o "cualquier destino no definido por otras reglas de autorización".
- La coincidencia del prefijo más largo es la regla que tiene prioridad.

Ejemplo de arquitectura para escenarios de reglas de autorización

En el siguiente diagrama se muestra la arquitectura de ejemplo que se utiliza para los escenarios de ejemplo que se encuentran en esta sección.



Escenario 1: acceso a un único destino

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingenierí	S-xxxxx14	False	172.16.0.0/24

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
a a la red en las instalaciones			
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administración a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder solo a `10.0.0.0/16`.
- El grupo de administradores puede acceder solo a `192.168.0.0/24`.
- El punto de conexión de Client VPN descarta el resto del tráfico.

> **Note**
>
> En este escenario, ningún grupo de usuarios tiene acceso al Internet público.

Escenario 2: uso de cualquier CIDR de destino (0.0.0.0/0)

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
	S-xxxxx14	False	172.16.0.0/24

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones			
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder solo a `10.0.0.0/16`.
- El grupo de administradores puede acceder al Internet público y a `192.168.0.0/24`, pero no puede acceder a `172.16.0.0/24` ni `10.0.0/16`.

> **Note**
>
> En este escenario, como no hay reglas que hagan referencia a `192.168.0.0/24`, el acceso a esa red también lo proporciona la regla `0.0.0.0/0`.
> Una regla que contenga `0.0.0.0/0` siempre se evalúa en último lugar, independientemente del orden en que se crearon las reglas. Por ello, hay que tener en cuenta que las reglas evaluadas antes que `0.0.0.0/0` desempeñan un rol en la determinación de las redes a las que `0.0.0.0/0` concede acceso.

Escenario 3: coincidencia de prefijo IP más largo

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.0.44/32

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la VPC de desarrollo, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la VPC de desarrollo.

> **Note**
>
> Aquí se ve cómo una regla con un prefijo IP más largo tiene prioridad sobre una regla con un prefijo IP más corto. Si desea que el grupo de desarrollo tenga acceso a `10.0.2.119/32`, es necesario agregar una regla adicional que conceda acceso a `10.0.2.119/32` al equipo de desarrollo.

Escenario 4: CIDR superpuesto (mismo grupo)

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.0.44/32

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a una subred más pequeña en las instalaciones	S-xxxxx14	False	17216,0,1288/25

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería tiene acceso a `172.16.0.0/24`, incluida la subred más específica `172.16.0.128/25`.

Escenario 5: regla adicional 0.0.0.0/0

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.0.44/32
Proporcionar acceso al grupo de ingeniería a una subred más pequeña en las instalaciones	S-xxxxx14	False	17216.0.128/25
Proporcionar acceso al grupo de ingeniería a cualquier destino	S-xxxxx14	False	0.0.0.0/0

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `192.168.0.0/24` y `172.16.0.0/24`, incluida la subred más específica `172.16.0.128/25`.

> **Note**
>
> Observe que tanto el grupo de ingenieros como el de administradores ahora pueden acceder a `192.168.0.0/24`. Esto se debe a que ambos grupos tienen acceso a `0.0.0.0/0` (cualquier destino) y no hay otras reglas que hagan referencia a `192.168.0.0/24`.

Escenario 6: agregar regla para 192.168.0.0/24

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.0.44/32
	S-xxxxx14	False	17216.0.128/25

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingenierí a a una subred en la red en las instalaci ones			
Proporcionar acceso al grupo de ingeniería a cualquier destino	S-xxxxx14	False	0.0.0.0/0
Proporcionar acceso al grupo de administr ación a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `172.16.0.0/24` y `172.16.0.128/25`.

> **Note**
>
> Observe cómo al agregar la regla para que el grupo de administradores acceda a `192.168.0.0/24`, el grupo de desarrollo deja de tener acceso a esa red de destino.

Escenario 7: acceso para todos los grupos de usuarios

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.0.44/32
Proporcionar acceso al grupo de ingeniería a una subred en la red en las instalaciones	S-xxxxx14	False	17216.0.128/25
	S-xxxxx14	False	0.0.0.0/0

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a todas las redes			
Proporcionar acceso al grupo de administración a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24
Proporcionar acceso a todos los grupos	N/A	True	0.0.0.0/0

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `172.16.0.0/24` y `172.16.0.128/25`.
- Cualquier otro grupo de usuarios, por ejemplo, el "grupo de administradores", puede acceder al Internet público, pero no a otras redes de destino definidas en las demás reglas.

Listas de revocación de certificados del cliente

Puede utilizar listas de revocación de certificados de cliente para revocar el acceso a un punto de enlace de Client VPN en una serie de certificados de cliente específicos.

> **Note**
>
> Para obtener más información sobre cómo generar los certificados y las claves del cliente y el servidor, consulte Autenticación mutua

Para obtener más información sobre la cantidad de entradas que puede agregar a la lista de revocación de certificados del cliente, consulte Cuotas de Client VPN.

Contenido

- Generación de una lista de revocación de certificados del cliente
- Importación de una lista de revocación de certificados del cliente
- Exportación de una lista de revocación de certificados del cliente

Generación de una lista de revocación de certificados del cliente

Linux/macOS

En el procedimiento siguiente, genera una lista de revocación de certificados del cliente mediante la utilidad de línea de comandos easy-rsa de OpenVPN.

Para generar una lista de revocación de certificados del cliente mediante easy-rsa de OpenVPN

1. Inicie sesión en el servidor que aloja la instalación easyrsa que se usó para generar el certificado.
2. Vaya a la carpeta `easy-rsa/easyrsa3` de su repositorio local.

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

3. Revocar el certificado de cliente y generar la lista de revocación de cliente.

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

Escriba `yes` cuando se le solicite.

Windows

El siguiente procedimiento utiliza el software OpenVPN para generar una lista de revocación de clientes. Se supone que ha seguido los pasos para utilizar el software OpenVPN para generar los certificados y claves de cliente y servidor.

Para generar una lista de revocación de certificados de cliente utilizando EasyRSA versión 3.x.x

1. Abra un símbolo del sistema y navegue hasta el directorio EasyRSA-3.x.x, que dependerá de dónde esté instalado en el sistema.

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

2. Ejecute el archivo “EasyRSA-Start.bat” para iniciar el shell de EasyRSA.

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

3. Revoque el certificado del cliente en el shell de EasyRSA.

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

4. Escriba “sí” cuando se le solicite.
5. Genere la lista de revocación de clientes.

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

6. La lista de revocación de clientes se creará en la siguiente ubicación:

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

Para generar una lista de revocación de certificados de cliente utilizando versiones anteriores de EasyRSA

1. Abra un símbolo del sistema y vaya al directorio de OpenVPN.

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

2. Ejecute el archivo `vars.bat`.

```
C:\> vars
```

3. Revocar el certificado de cliente y generar la lista de revocación de cliente.

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

Importación de una lista de revocación de certificados del cliente

Debe tener un archivo de lista de revocación de certificados de cliente para importarlo. Para obtener más información sobre cómo generar una lista de revocación de certificados del cliente, consulte Generación de una lista de revocación de certificados del cliente.

Puede importar una lista de revocación de certificados del cliente mediante la consola y la AWS CLI.

Para importar una lista de revocación de certificados del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN para el que va a importar la lista de revocación de certificados del cliente.
4. Elija Actions (Acciones) y seleccione Import Client Certificate CRL (Importar CRL de certificados de cliente).
5. En Certificate Revocation List (Lista de revocación de certificados), ingrese el archivo de la lista de revocación de certificados del cliente y seleccione Import client certificate CRL (Importar CRL de certificados de cliente).

Para importar una lista de revocación de certificados del cliente (AWS CLI)

Utilice el 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
```

Exportación de una lista de revocación de certificados del cliente

Puede exportar listas de revocación de certificados del cliente mediante la consola y la AWS CLI.

Para exportar una lista de revocación de certificados del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN para el que va a exportar la lista de revocación de certificados del cliente.
4. Elija Actions (Acciones), seleccione Export Client Certificate CRL (Exportar CRL de certificados de cliente) y elija Export Client Certificate CRL (Exportar CRL de certificados de cliente).

Para exportar una lista de revocación de certificados del cliente (AWS CLI)

Utilice el comando export-client-vpn-client-certificate-revocation-list.

Conexiones de clientes

Las conexiones son sesiones de VPN que han establecido los clientes. Una conexión se establece cuando un cliente se conecta correctamente a un punto de enlace de Client VPN.

Contenido

- Visualización de conexiones de clientes
- Terminación de una conexión de cliente

Visualización de conexiones de clientes

Puede ver las conexiones de clientes mediante la consola y la AWS CLI. La información de conexión incluye la dirección IP asignada desde el rango de CIDR del cliente.

Para ver las conexiones de clientes (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN cuyas conexiones de clientes desee ver.

4. Elija la pestaña Connections (Conexiones). En la pestaña Connections (Conexiones) se incluyen todas las conexiones de clientes activas y terminadas.

Para ver las conexiones de clientes (AWS CLI)

Utilice el comando describe-client-vpn-connections.

Terminación de una conexión de cliente

Cuando termine una conexión de cliente, la sesión de VPN finaliza.

Puede terminar las conexiones de clientes mediante la consola y la AWS CLI.

Para terminar una conexión de cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN al que está conectado el cliente y elija Connections (Conexiones).
4. Seleccione la conexión que va a terminar, seleccione Terminate Connection (Terminar conexión) y elija Terminate Connection (Terminar conexión).

Para terminar una conexión de cliente (AWS CLI)

Utilice el comando terminate-client-vpn-connections.

Banner de inicio de sesión de cliente

AWS Client VPN ofrece la opción de mostrar un banner de texto en AWS proporciona aplicaciones de escritorio de Client VPN cuando se establece una sesión VPN. Puede definir el contenido del banner de texto para satisfacer sus necesidades normativas y de conformidad. Se pueden utilizar un máximo de 1400 caracteres codificados en UTF-8.

> **Note**
>
> Cuando se ha habilitado un banner de inicio de sesión de cliente, solo se mostrará en las sesiones VPN recién creadas. Las sesiones VPN existentes no se interrumpen, aunque el banner se mostrará cuando se restablezca una sesión existente.

Consulte Notas de la versión del cliente proporcionado por AWS en la Guía del usuario de AWS Client VPN para obtener más detalles sobre las aplicaciones de escritorio del cliente.

Contenido

- Configurar un banner de inicio de sesión de cliente durante la creación de un punto de conexión de Client VPN
- Configurar un banner de inicio de sesión de cliente en un punto de conexión de Client VPN
- Desactivar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente
- Modificación del texto del banner existente en un punto de conexión de Client VPN
- Ver el banner de inicio de sesión actualmente configurado

Configurar un banner de inicio de sesión de cliente durante la creación de un punto de conexión de Client VPN

Para obtener pasos detallados para habilitar un banner de inicio de sesión de cliente durante la creación de un punto de conexión de Client VPN, consulte Creación de un punto de enlace de Client VPN.

Configurar un banner de inicio de sesión de cliente en un punto de conexión de Client VPN

Siga los siguientes pasos para configurar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente.

Habilitar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Active Enable client login banner (Habilitar banner de inicio de sesión de cliente).
6. En Client login banner text (Texto de banner de inicio de sesión de cliente), ingrese el texto que se mostrará en un banner de clientes proporcionados en AWS cuando se establece una

sesión VPN. Utilice sólo caracteres codificados en UTF-8, con un máximo de 1400 caracteres permitidos.

7. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Habilitar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Desactivar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente

Siga estos pasos para desactivar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente.

Desactivar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Desactive Enable client login banner (Habilitar banner de inicio de sesión de cliente).
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Desactivar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Modificación del texto del banner existente en un punto de conexión de Client VPN

Siga los siguientes pasos para modificar el texto existente en el banner de inicio de sesión de cliente.

Modificación del texto del banner existente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).
4. En Enable client login banner?(¿Habilitar banner de inicio de sesión de cliente?), verifique que se ha activado.
5. En Client login banner text (Texto de banner de inicio de sesión de cliente), reemplace el texto existente por el nuevo texto que desea que se muestre en un banner de clientes proporcionados en AWS cuando se establece una sesión VPN. Utilice sólo caracteres codificados en UTF-8, con un máximo de 1400 caracteres.
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Modificación de un banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Ver el banner de inicio de sesión actualmente configurado

Siga estos pasos para ver un banner de inicio de sesión configurado actualmente.

Ver el banner de inicio de sesión actual para un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea ver.
4. Verifique que la pestaña Details (Detalles) esté seleccionada.
5. Vea el texto del banner de inicio de sesión configurado actualmente junto a Client login banner text (Texto del banner de inicio de sesión de cliente).

Ver un banner de inicio de sesión configurado actualmente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

Puntos de enlace de Client VPN

Todas las sesiones de VPN del cliente terminan en el punto de enlace de Client VPN. Puede configurar el punto de enlace de Client VPN para que administre y controle todas las sesiones de VPN del cliente.

Contenido

- Creación de un punto de enlace de Client VPN
- Modificación de un punto de enlace de Client VPN.
- Consulta de puntos de enlace de Client VPN
- Eliminación de un punto de enlace de Client VPN

Creación de un punto de enlace de Client VPN

Cree un punto de enlace de Client VPN para que sus clientes puedan establecer una sesión de VPN.

La conexión de Client VPN debe crearse en la misma cuenta de AWS en la que está aprovisionada la red de destino.

Requisitos previos

Antes de comenzar, asegúrese de hacer lo siguiente:

- Revise las reglas y las limitaciones en Reglas y prácticas recomendadas de AWS Client VPN.
- Genere el certificado de servidor y, si es necesario, el certificado de cliente. Para obtener más información, consulte Autenticación del cliente.

Para crear un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN) y Create Client VPN Endpoint (Crear punto de enlace de Client VPN).
3. (Opcional) Escriba una etiqueta de nombre y una descripción del punto de conexión de Client VPN.
4. En Client IPv4 CIDR (CIDR de IPv4 de cliente), especifique el rango de direcciones IP, en notación CIDR, desde el que se van a asignar las direcciones IP del cliente. Por ejemplo, `10.0.0.0/22`.

> **Note**
>
> El intervalo de direcciones no puede solaparse al intervalo de direcciones de la red de destino, al intervalo de direcciones de la VPC ni a ninguna de las rutas que se asociarán con el punto de conexión de Client VPN. El intervalo de direcciones del cliente debe tener un tamaño de bloque de CIDR mínimo de /22 y no superior a /12. No puede cambiar el intervalo de direcciones del cliente después de crear el punto de conexión de Client VPN.

5. En Server certificate ARN (ARN del certificado del servidor), especifique el ARN del certificado TLS que va a utilizar el servidor. Los clientes utilizan el certificado de servidor para autenticar el punto de enlace de Client VPN al que están conectados.

> **Note**
>
> El certificado de servidor debe estar presente en AWS Certificate Manager (ACM) en la región en la que está creando el punto de enlace de Client VPN. El certificado se puede aprovisionar con ACM o importarse a ACM.

6. Especifique el método de autenticación que se va a utilizar para autenticar los clientes al establecer una conexión de VPN. Debe seleccionar un método de autenticación.

   - Para usar la autenticación basada en usuarios, seleccione Utilizar la autenticación basada en usuarios y, a continuación, elija una de las opciones siguientes:
     - Autenticación con Active Directory: elija esta opción para la autenticación con Active Directory. Para ID de directorio, especifique el ID de Active Directory que se va a utilizar.
     - Autenticación federada: elija esta opción para la autenticación federada basada en SAML.

       Para ARN del proveedor SAML, especifique el ARN del proveedor de identidades SAML de IAM.

       (Opcional) En Self-service SAML provider ARN (ARN del proveedor SAML de autoservicio), especifique el ARN del proveedor de identidades SAML de IAM que creó para poder utilizar el portal de autoservicio, si procede.
   - Para utilizar la autenticación mutua de certificados, seleccione Use mutual authentication (Usar autenticación mutua) y luego, en Client certificate ARN (ARN de certificado de cliente),

especifique el ARN del certificado de cliente aprovisionado en AWS Certificate Manager (ACM).

> **Note**
>
> Si los certificados de servidor y cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado de servidor para el servidor y el cliente. Si el certificado de cliente fue emitido por una entidad de certificación distinta, debe especificarse el ARN del certificado de cliente.

7. (Opcional) Para el registro de conexiones, especifique si desea registrar los datos sobre las conexiones de los clientes mediante Amazon CloudWatch Logs. Active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente). En el nombre del grupo de CloudWatch registros, introduzca el nombre del grupo de registros que se va a utilizar. En el caso del nombre del flujo de registro de CloudWatch registros, introduzca el nombre del flujo de registro que desee utilizar o deje esta opción en blanco para que podamos crear un flujo de registro para usted.
8. (Opcional) En Client Connect Handler (Controlador de conexión de cliente), active Enable client connect handler (Habilitar controlador de conexión de cliente) para ejecutar código personalizado que permita o deniegue una nueva conexión con el punto de conexión de Client VPN. En Client Connect Handler ARN (ARN del controlador de la conexión del cliente), especifique el nombre de recurso de Amazon (ARN) de la función Lambda que contiene la lógica que va a permitir o a denegar las conexiones.
9. (Opcional) Especifique qué servidores DNS se van a utilizar para la resolución de DNS. Para utilizar servidores DNS personalizados, en DNS Server 1 IP address (Dirección IP de servidor de DNS 1) yDNS Server 2 IP address (Dirección IP de servidor de DNS 2), especifique las direcciones IP de los servidores DNS que se van a utilizar. Para utilizar un servidor DNS de la VPC, en DNS Server 1 IP address (Dirección IP del servidor DNS 1) o DNS Server 2 IP address (Dirección IP del servidor DNS 2), especifique las direcciones IP y agregue la dirección IP del servidor DNS de la VPC.

> **Note**
>
> Asegúrese de que los clientes pueden acceder a los servidores DNS.

10. (Opcional) De forma predeterminada, el punto de conexión de Client VPN utiliza el protocolo de transporte UDP. Para utilizar el protocolo de transporte TCP en su lugar, en Transport Protocol (Protocolo de transporte), seleccione TCP.

    > **Note**
    >
    > Normalmente UDP tiene mejor rendimiento que TCP. El protocolo de transporte no se puede cambiar una vez creado el punto de enlace de Client VPN.

11. (Opcional) Para que el punto de conexión sea un punto de conexión de Client VPN de túnel dividido, active Enable split-tunnel (Habilitar túnel dividido). De forma predeterminada, el túnel dividido en un punto de conexión de Client VPN está desactivado.
12. (Opcional) En VPC ID (ID de VPC), elija la VPC que desea asociar con el punto de enlace de Client VPN. En Security Group IDs (ID de grupo de seguridad), elija uno o varios grupos de seguridad de la VPC para aplicarlos al punto de enlace de Client VPN.
13. (Opcional) En VPN port (Puerto de VPN), elija el número de puerto de VPN. El valor predeterminado es 443.
14. (Opcional) Si desea generar una URL del portal de autoservicio para los clientes, active Enable self-service portal (Habilitar portal de autoservicio).
15. (Opcional) Para Session timeout hours (Tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas de las opciones disponibles o deje el valor predeterminado de 24 horas.
16. (Opcional) Especifique si desea habilitar el texto del banner de inicio de sesión de cliente. Active Enable client login banner (Habilitar banner de inicio de sesión de cliente). En Client Login Banner Text (Texto de banner de inicio de sesión de cliente), ingrese el texto que se mostrará en un banner en los clientes proporcionados por AWS cuando se establezca una sesión de VPN. Solo caracteres con codificación UTF-8. Máximo de 1400 caracteres.
17. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

Cuando haya creado el punto de enlace de Client VPN, haga lo siguiente para completar la configuración y permitir que los clientes se conecten:

- El estado inicial del punto de enlace de Client VPN es `pending-associate`. Los clientes solo pueden conectarse al punto de enlace de Client VPN después de asociar la primera red de destino.
- Cree una regla de autorización para especificar qué clientes tienen acceso a la red.

- Descargue y prepare el archivo de configuración del punto de enlace de Client VPN para distribuirlo a sus clientes.
- Indique a sus clientes que utilicen el cliente proporcionado por AWS u otra aplicación cliente basada en OpenVPN para conectarse al punto de enlace de Client VPN. Para obtener más información, consulte la AWS Client VPNGuía del usuario de .

Para crear un punto de enlace de Client VPN (AWS CLI)

Utilice el comando create-client-vpn-endpoint.

Modificación de un punto de enlace de Client VPN.

Después de crear una conexión de Client VPN, se puede modificar cualquiera de los siguientes ajustes:

- La descripción
- El certificado de servidor
- Las opciones de registro de la conexión de cliente
- La opción del controlador de la conexión del cliente
- Los servidores DNS
- La opción de túnel dividido
- Rutas (cuando se utiliza la opción de túnel dividido)
- Lista de revocación de certificados (CRL)
- Reglas de autorización
- Las asociaciones de grupos de seguridad y VPC
- El número de puerto de VPN
- La opción del portal de autoservicio
- El máximo de duración de la sesión VPN
- Habilitar o desactivar el texto del banner de inicio de sesión de cliente
- Texto del banner de inicio de sesión de cliente

> **Note**
>
> Las modificaciones de los puntos de conexión de Client VPN, incluidos los cambios en la lista de revocación de certificados (CRL), surtirán efecto hasta cuatro horas después de que el servicio Client VPN acepte una solicitud.
> No puede modificar el intervalo CIDR IPv4 del cliente, las opciones de autenticación, el certificado de cliente ni el protocolo de transporte después de crear el punto de conexión de Client VPN.

Cuando modifica cualquiera de los siguientes parámetros en un punto de enlace de Client VPN, la conexión se restablece:

- El certificado de servidor
- Los servidores DNS
- La opción de túnel dividido (activar o desactivar el soporte)
- Rutas (cuando se utiliza la opción de túnel dividido)
- Lista de revocación de certificados (CRL)
- Reglas de autorización
- El número de puerto de VPN

Los puntos de enlace de Client VPN se pueden modificar a través de la consola o la AWS CLI.

Para modificar un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea modificar, elija Actions (Acciones) y haga clic en Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. En Description (Descripción), escriba una breve descripción del punto de enlace de Client VPN.
5. En Server certificate ARN (ARN del certificado del servidor), especifique el ARN del certificado TLS que va a utilizar el servidor. Los clientes utilizan el certificado de servidor para autenticar el punto de enlace de Client VPN al que están conectados.

> **Note**
>
> El certificado de servidor debe estar presente en AWS Certificate Manager (ACM) en la región en la que está creando el punto de enlace de Client VPN. El certificado se puede aprovisionar con ACM o importarse a ACM.

6. Especifique si desea registrar los datos sobre las conexiones de los clientes mediante Amazon CloudWatch Logs. En Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente), realice una de las siguientes acciones:

   - Para activar el registro de la conexión del cliente, active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente). En el nombre del grupo de CloudWatch registros, seleccione el nombre del grupo de registros que se va a usar. En el nombre del flujo de registro de CloudWatch registros, seleccione el nombre del flujo de registro que desee utilizar o deje esta opción en blanco para que podamos crear un flujo de registro para usted.
   - Para desactivar el registro de la conexión del cliente, desactive Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).

7. En Client connect handler (Controlador de conexión de cliente), para activar el controlador de conexión de cliente, active Enable client connect handler (Habilitar controlador de conexión de cliente). En Client Connect Handler ARN (ARN del controlador de la conexión del cliente), especifique el nombre de recurso de Amazon (ARN) de la función Lambda que contiene la lógica que va a permitir o a denegar las conexiones.

8. Active o desactive Enable DNS servers (Habilitar servidores DNS). Para utilizar servidores DNS personalizados, en DNS Server 1 IP address (Dirección IP de servidor de DNS 1) yDNS Server 2 IP address (Dirección IP de servidor de DNS 2), especifique las direcciones IP de los servidores DNS que se van a utilizar. Para utilizar un servidor DNS de la VPC, en DNS Server 1 IP address (Dirección IP del servidor DNS 1) o DNS Server 2 IP address (Dirección IP del servidor DNS 2), especifique las direcciones IP y agregue la dirección IP del servidor DNS de la VPC.

   > **Note**
   >
   > Asegúrese de que los clientes pueden acceder a los servidores DNS.

9. Active o desactive Enable split-tunnel (Habilitar túnel dividido). De forma predeterminada, el túnel dividido en un punto de conexión de VPN está desactivado.

10. En VPC ID (ID de VPC), elija la VPC que desea asociar con el punto de conexión de Client VPN. En Security Group IDs (ID de grupo de seguridad), elija uno o varios grupos de seguridad de la VPC para aplicarlos al punto de enlace de Client VPN.
11. En VPN port (Puerto de VPN), elija el número de puerto de VPN. El valor predeterminado es 443.
12. Si desea generar una URL del portal de autoservicio para los clientes, active Enable self-service portal (Habilitar portal de autoservicio).
13. En Session timeout hours (Horas de tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas de las opciones disponibles o deje el valor predeterminado de 24 horas.
14. Active o desactive Enable client login banner (Habilitar banner de inicio de sesión de cliente). Si desea usar el banner de inicio de sesión de cliente, ingrese el texto que se mostrará en un banner en los clientes proporcionados por AWS cuando se establezca una sesión VPN. Solo caracteres con codificación UTF-8. Máximo de 1400 caracteres.
15. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Modificación de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Consulta de puntos de enlace de Client VPN

Puede consultar información sobre los puntos de enlace de Client VPN a través de la consola o la AWS CLI.

Para ver los puntos de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN que desea ver.
4. Use las pestañas Details (Detalles), Target network associations (Asociaciones de red de destino), Security groups (Grupos de seguridad), Authorization rules (Reglas de autorización), Route table (Tabla de enrutamiento), Connections (Conexiones) y Tags (Etiquetas) para ver la información sobre los puntos de conexión de Client VPN existentes.

   También puede usar filtros para mejorar la búsqueda.

Para ver los puntos de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

Eliminación de un punto de enlace de Client VPN

Tendrá que desconectar todas las redes de destino para poder eliminar un punto de conexión de Client VPN. Cuando se elimina un punto de enlace de Client VPN, su estado cambia a `deleting` y los clientes ya no pueden conectarse a él.

Los puntos de enlace de Client VPN pueden eliminarse a través de la consola o la AWS CLI.

Para eliminar un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea eliminar. Elija Actions (Acciones), Delete Client VPN endpoint (Eliminar punto de conexión de Client VPN).
4. Ingrese delete en la ventana de confirmación y elija Delete (Eliminar).

Eliminación de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando delete-client-vpn-endpoint.

Trabajo con registros de conexión

Puede habilitar el registro de conexión de un punto de enlace de Client VPN nuevo o existente y comenzar a capturar registros de conexión.

Antes de comenzar, debe tener un grupo de registro de CloudWatch Logs en su cuenta. Para obtener más información, consulte Uso de grupos de registros y flujos de registro en la Guía del usuario de Amazon CloudWatch Logs. Se aplican cargos por usar los registros de CloudWatch Logs. Para obtener más información, consulte los precios de Amazon CloudWatch.

Cuando habilita el registro de conexión, puede especificar el nombre de una secuencia de registros en el grupo de registros. Si no especifica ninguna secuencia de registros, el servicio Client VPN creará una automáticamente.

Activar el registro de conexión en un nuevo punto de enlace de Client VPN

Puede activar el registro de conexión al crear un nuevo punto de enlace de Client VPN a través de la consola o la línea de comandos.

Para habilitar el registro de conexión de un nuevo punto de enlace de Client VPN a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de conexión de Client VPN) y Create Client VPN endpoint (Crear punto de conexión de Client VPN).
3. Complete las opciones hasta que llegue a la sección Registro de conexión. Para obtener más información sobre las opciones, consulte Creación de un punto de enlace de Client VPN.
4. En Connection logging (Registro de conexiones), active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. En CloudWatch Logs log group name (Nombre del grupo de registros de CloudWatch Logs), elija el nombre del grupo de registros de CloudWatch Logs.
6. (Opcional) En CloudWatch Logs log stream name (Nombre de la secuencia de registros de CloudWatch Logs), elija el nombre de la secuencia de registros de CloudWatch Logs.
7. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

Para habilitar el registro de conexión en un nuevo punto de enlace de Client VPN a través de la AWS CLI

Utilice el comando create-client-vpn-endpoint y especifique el parámetro `--connection-log-options`. Puede especificar la información de los registros de conexión en formato JSON, como se muestra en el siguiente ejemplo.

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

Habilitar el registro de conexión en un punto de enlace de Client VPN existente

Puede habilitar el registro de conexión en un punto de enlace de Client VPN existente a través de la consola o la línea de comandos.

Para habilitar el registro de conexión en un punto de enlace de Client VPN existente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar el punto de conexión de Client VPN).
4. En Connection logging (Registro de conexiones), active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. En CloudWatch Logs log group name (Nombre del grupo de registros de CloudWatch Logs), elija el nombre del grupo de registros de CloudWatch Logs.
6. (Opcional) En CloudWatch Logs log stream name (Nombre de la secuencia de registros de CloudWatch Logs), elija el nombre de la secuencia de registros de CloudWatch Logs.
7. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Para habilitar el registro de conexión en un punto de enlace de Client VPN a través de la AWS CLI

Utilice el comando modify-client-vpn-endpoint y especifique el parámetro `--connection-log-options`. Puede especificar la información de los registros de conexión en formato JSON, como se muestra en el siguiente ejemplo.

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

Ver registros de conexión.

Puede ver los registros de conexión a través de la consola de CloudWatch Logs.

Para ver los registros de conexión mediante la consola

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Grupos de registros y seleccione el grupo de registros que contiene los registros de conexión.
3. Seleccione la secuencia de registros del punto de enlace de Client VPN.

> **Note**
>
> En la columna Timestamp (Marca temporal), se muestra la hora a la que el registro de conexión se publicó en CloudWatch Logs, no la hora de la conexión.

Para obtener más información sobre la búsqueda de datos de registro, consulte Búsqueda de datos de registro mediante patrones de filtro en la Guía del usuario de Amazon CloudWatch Logs.

Desactivación del registro de conexiones

Puede desactivar los registros de conexiones de un punto de conexión de Client VPN a través de la consola o la línea de comandos. Cuando desactiva el registro de conexiones, no se eliminan los registros de CloudWatch Logs existentes.

Para desactivar el registro de conexiones mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar el punto de conexión de Client VPN).
4. En Connection logging (Registro de conexiones), desactive Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Para desactivar el registro de conexiones mediante la AWS CLI

Utilice el comando modify-client-vpn-endpoint y especifique el parámetro `--connection-log-options`. Asegúrese de que `Enabled` está establecido en `false`.

Exportar y configurar el archivo de configuración del cliente

El archivo de configuración del punto de enlace de Client VPN es el archivo que usan los clientes (usuarios) para establecer una conexión de VPN con el punto de enlace de Client VPN. Debe descargar (exportar) este archivo y distribuirlo a todos los clientes que necesitan acceder a la VPN. Si ha habilitado el portal de autoservicio para el punto de enlace de Client VPN, los clientes también pueden iniciar sesión en el portal y descargar el archivo de configuración ellos mismos. Para obtener más información, consulte Acceso al portal de autoservicio.

Si el punto de enlace de Client VPN utiliza la autenticación mutua, debe agregar el certificado y la clave privada del cliente al archivo de configuración .ovpn que descargue. Después de agregar la información, los clientes pueden importar el archivo .ovpn al software de cliente OpenVPN.

> **Important**
>
> Si no agrega el certificado de cliente y la información de la clave privada del cliente al archivo, los clientes que utilicen la autenticación mutua no podrán conectarse al punto de enlace de Client VPN.

De forma predeterminada, la opción «remote-random-hostname» de la configuración del cliente de OpenVPN habilita el DNS comodín. Dado que el DNS comodín está habilitado, el cliente no almacena en caché la dirección IP del punto de enlace, por lo que no podrá hacer ping al nombre de DNS del punto de enlace.

Si el punto de enlace de Client VPN utiliza la autenticación de Active Directory y habilita la autenticación multifactor (MFA) en el directorio después de distribuir el archivo de configuración del cliente, deberá descargar un archivo nuevo y volver a distribuirlo entre sus clientes. Los clientes no pueden usar el archivo de configuración anterior para conectarse al punto de enlace de Client VPN.

Exportar el archivo de configuración del cliente

Puede exportar la configuración del cliente mediante la consola o la AWS CLI.

Para exportar la configuración del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).

3. Seleccione el punto de enlace de Client VPN cuyo archivo de configuración desea descargar y elija Download Client Configuration (Descargar configuración del cliente).

Para exportar la configuración del cliente (AWS CLI)

Utilice el comando export-client-vpn-client-configuration y especifique el nombre del archivo de salida.

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

Agregar el certificado de cliente y la información de la clave (autenticación mutua)

Si el punto de enlace de Client VPN utiliza la autenticación mutua, debe agregar el certificado y la clave privada del cliente al archivo de configuración .ovpn que descargue.

No se puede modificar el certificado de cliente cuando utiliza la autenticación mutua.

Para agregar el certificado de cliente y la información de la clave (autenticación mutua)

Puede utilizar una de las siguientes opciones.

(Opción 1) Distribuya la clave y el certificado de cliente entre los clientes junto con el archivo de configuración del punto de enlace de Client VPN. En este caso, especifique la ruta de acceso al certificado y la clave en el archivo de configuración. Abra el archivo de configuración utilizando el editor que prefiera y agregue lo siguiente al final del archivo. Reemplace */ruta/* por la ubicación del certificado y la clave del cliente (la ubicación es relativa al cliente que se conecta al punto de enlace).

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

(Opción 2) Añada el contenido del certificado de cliente entre las etiquetas <cert></cert> y el contenido de la clave privada entre las etiquetas <key></key> al archivo de configuración. Si elige esta opción, distribuirá únicamente el archivo de configuración entre sus clientes.

Si ha generado certificados y claves de cliente diferentes para cada uno de los usuarios que se van a conectar al punto de enlace de Client VPN, repita este paso con todos los usuarios.

A continuación, se muestra un ejemplo del formato de un archivo de configuración de Client VPN que incluye la clave y el certificado de cliente.

```
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
```

Rutas

Cada punto de enlace de Client VPN tiene una tabla de ruta que describe las rutas de la red de destino disponibles. Cada ruta de la tabla de ruteo determina la ubicación a la que se dirige el tráfico de red. Debe configurar reglas de autorización en cada ruta del punto de enlace de Client VPN para especificar qué clientes tienen acceso a la red de destino.

Cuando asocia una subred de una VPC con un punto de enlace de Client VPN, se agrega automáticamente una ruta de la VPC a la tabla de enrutamiento del punto de enlace de Client VPN. Para activar el acceso en otras redes, como las VPC interconectadas, las redes de las instalaciones, la red local (para permitir que los clientes se comuniquen entre sí) o Internet, debe agregar manualmente una ruta a la tabla de enrutamiento del punto de enlace de Client VPN.

> **Note**
>
> Si va a asociar varias subredes al punto de enlace de Client VPN, debe asegurarse de crear una ruta para cada subred tal como se describe aquí: El acceso a una VPC interconectada, a Amazon S3 o a Internet es intermitente. Cada subred asociada debe tener un conjunto de rutas idéntico.

Contenido

- Consideraciones sobre los túneles divididos en los puntos de enlace de Client VPN
- Creación de una ruta de punto de enlace
- Visualización de rutas de punto de enlace
- Eliminación de una ruta de punto de enlace

Consideraciones sobre los túneles divididos en los puntos de enlace de Client VPN

Cuando se utiliza un túnel dividido en un punto de enlace de Client VPN, todas las rutas que están en las tablas de enrutamiento de Client VPN se agregan a la tabla de enrutamiento del cliente al establecer la VPN. Si agrega una ruta después de establecer la VPN, tendrá que restablecer la conexión para que la nueva ruta se envíe al cliente.

Es conveniente que tenga en cuenta el número de rutas que el dispositivo cliente puede controlar antes de modificar la tabla de enrutamiento del punto de enlace de Client VPN.

Creación de una ruta de punto de enlace

Al crear una ruta, debe especificar cómo se debe dirigir el tráfico de la red de destino.

Para permitir que los clientes obtengan acceso a Internet, añada una ruta `0.0.0.0/0` de destino.

Puede agregar rutas a un punto de enlace de Client VPN a través de la consola y la AWS CLI.

Para crear la ruta de un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).

3. Seleccione el punto de conexión de Client VPN al que desee agregar la ruta y elija Route table (Table de enrutamiento) y Create Route (Crear ruta).
4. En Route destination (Destino de ruta), especifique el rango de CIDR de IPv4 para la red de destino. Por ejemplo:

   - Para agregar una ruta para la VPC del punto de conexión de Client VPN, ingrese el intervalo CIDR IPv4 de la VPC.
   - Para agregar una ruta para acceder a Internet, escriba `0.0.0.0/0`.
   - Para agregar una ruta para una VPC interconectada, escriba el rango de CIDR de IPv4 de la VPC interconectada.
   - Para agregar la ruta de una red en las instalaciones, ingrese el rango CIDR IPv4 de la conexión de AWS Site-to-Site VPN.
5. En Subnet ID for target network association (ID de subred para la asociación de red de destino), seleccione la subred que está asociada al punto de conexión de Client VPN.

   Si va a agregar una ruta para la red local del punto de conexión de Client VPN, también puede seleccionar `local`.
6. (Opcional) En Description (Descripción), ingrese una breve descripción de la ruta.
7. Elija Create route (Crear ruta).

Para crear una ruta de punto de enlace de Client VPN (AWS CLI)

Utilice el comando create-client-vpn-route.

Visualización de rutas de punto de enlace

Puede ver las rutas de un punto de enlace de Client VPN específico a través de la consola o la AWS CLI.

Para ver las rutas de un punto de enlace de Client VPN (consola)

1. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
2. Seleccione el punto de conexión de Client VPN cuyas rutas desee ver y elija Route Table (Tabla de enrutamiento).

Para ver las rutas de un punto de enlace de Client VPN (AWS CLI)

Ejecute el comando describe-client-vpn-routes.

Eliminación de una ruta de punto de enlace

Solo puede eliminar las rutas que haya añadido manualmente. No se pueden eliminar las rutas que se hayan agregado automáticamente al asociar una subred con el punto de enlace de Client VPN. Para eliminar las rutas que se han agregado automáticamente, debe desconectar la subred que inició la creación de estas rutas del punto de enlace de Client VPN.

Puede eliminar una ruta de un punto de enlace de Client VPN a través de la consola o la AWS CLI.

Para eliminar una ruta de punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN del que desea eliminar la ruta y elija Route table (Tabla de enrutamiento).
4. Seleccione la ruta que va a eliminar, elija Delete route (Eliminar ruta) y seleccione Delete route (Eliminar ruta).

Para eliminar la ruta de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando delete-client-vpn-route.

Redes de destino

Una red de destino es una subred en una VPC. Un punto de enlace de Client VPN debe tener al menos una red de destino que permita que los clientes se conecten a ella y establezcan una conexión de VPN.

Para obtener más información sobre los tipos de acceso que puede configurar (por ejemplo, permitir que sus clientes accedan a Internet), consulte Escenarios y ejemplos para AWS Client VPN.

Contenido

- Asociación una red de destino con un punto de enlace de Client VPN
- Aplicación de un grupo de seguridad a una red de destino
- Desconectar una red de destino de un punto de enlace de Client VPN
- Visualización de redes de destino

Asociación una red de destino con un punto de enlace de Client VPN

Puede asociar una o varias redes de destino (subredes) a un punto de enlace de Client VPN.

Se aplican las siguientes reglas:

- La subred debe tener un bloque de CIDR con al menos una máscara de bits de /27, por ejemplo 10.0.0.0/27. La subred debe tener también al menos 20 direcciones IP disponibles en todo momento.
- El bloque de CIDR de la subred no se puede solapar con el intervalo CIDR del cliente del punto de enlace de Client VPN.
- Si asocia varias subredes con un punto de enlace de Client VPN, cada subred tendrá que estar en una zona de disponibilidad diferente. Le recomendamos que asocie al menos dos subredes para proporcionar redundancia a la zona de disponibilidad.
- Si al crear el punto de enlace de Client VPN especificó una subred, dicha subred tendrá que estar en la misma VPC. Si aún no ha asociado ninguna VPC con el punto de enlace de Client VPN, puede elegir cualquier subred de cualquier VPC.

  Todas las asociaciones de subred adicionales tienen que ser de la misma VPC. Para asociar una subred de una VPC diferente, primero tiene que modificar el punto de enlace de Client VPN y cambiar la VPC que tiene asociada. Para obtener más información, consulte Modificación de un punto de enlace de Client VPN..

Al asociar una subred con un punto de enlace de Client VPN, la ruta local de la VPC en la que está aprovisionada la subred asociada se agrega automáticamente a la tabla de enrutamiento del punto de enlace de Client VPN.

> **Note**
>
> Una vez asociadas las redes de destino, cuando agregue o quite CIDR adicionales a la VPC conectada, debe realizar una de las siguientes operaciones para actualizar la ruta local para la tabla de enrutamiento del punto de enlace de Client VPN:
>
> - Desasocie el punto de enlace de Client VPN de la red de destino y, a continuación, asocie el punto de enlace de Client VPN a la red de destino.
> - Agregar manualmente o eliminar la ruta de la tabla de enrutamiento del punto de enlace de Client VPN.

Después de asociar la primera subred con el punto de enlace de Client VPN, el estado del punto de enlace de Client VPN cambia de `pending-associate` a `available` y los clientes pueden establecer una conexión de VPN.

Para asociar una red de destino a un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN con el que desee asociar la red de destino, elija Target network associations (Asociaciones de red de destino) y, a continuación, elija Associate target network (Asociar red de destino).
4. En VPC, elija la VPC en la que se encuentra la subred. Si al crear el punto de enlace de Client VPN especificó una VPC o si tiene asociaciones de subredes anteriores, debe ser la misma VPC.
5. En Choose a subnet to associate (Elija una subred para asociar), elija la subred que desee asociar con el punto de conexión de Client VPN.
6. Elija Associate target network (Asociar red de destino).

Asociación una red de destino con un punto de enlace de Client VPN (AWS CLI)

Utilice el comando associate-client-vpn-target-network.

Aplicación de un grupo de seguridad a una red de destino

Cuando cree un punto de enlace de Client VPN, puede especificar los grupos de seguridad que se aplicarán a la red de destino. Al asociar la primera red de destino con un punto de enlace de Client VPN, se aplica automáticamente el grupo de seguridad predeterminado de la VPC en la que se encuentra la subred asociada. Para obtener más información, consulte Grupos de seguridad.

Puede cambiar los grupos de seguridad del punto de enlace de Client VPN. Las reglas de los grupos de seguridad que necesite también pueden depender del tipo de acceso de VPN que desee configurar. Para obtener más información, consulte Escenarios y ejemplos para AWS Client VPN.

Para aplicar un grupo de seguridad a una red de destino (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).

3. Seleccione el punto de enlace de Client VPN al que se aplican los grupos de seguridad.
4. Elija Security Groups (Grupos de seguridad) y, luego, elija Apply Security Groups (Aplicar grupos de seguridad).
5. Seleccione los grupos de seguridad adecuados en Security group IDs (ID de grupos de seguridad).
6. Elija Apply Security Groups (Aplicar grupos de seguridad).

Para aplicar un grupo de seguridad a una red de destino (AWS CLI)

Utilice el comando apply-security-groups-to-client-vpn-target-network.

Desconectar una red de destino de un punto de enlace de Client VPN

Cuando desasocie una red de destino, se eliminará cualquier ruta que se haya agregado manualmente a la tabla de enrutamiento del punto de conexión de la VPN de cliente, así como la ruta que se creó automáticamente cuando se realizó la asociación de la red de destino (la ruta local de la VPC). Si desconecta todas las redes de destino de un punto de enlace de Client VPN, los clientes ya no podrán establecer una conexión de VPN.

Para desconectar una red de destino de un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que está asociada la red de destino y elija Target network associations (Asociaciones de red de destino).
4. Seleccione la red de destino que desea desasociar, elija Disassociate (Desasociar) y, a continuación, elija Disassociate target network (Desasociar red de destino).

Desconectar una red de destino de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando disassociate-client-vpn-target-network.

Visualización de redes de destino

Puede ver los destinos asociados con un determinado punto de enlace de Client VPN a través de la consola o la AWS CLI.

Para ver las redes de destino (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN adecuado y elija Target network associations (Asociaciones de la red de destino).

Para ver las redes de destino mediante la AWS CLI

Utilice el comando describe-client-vpn-target-networks.

Duración máxima de la sesión VPN

AWS Client VPN proporciona varias opciones para la duración máxima de la sesión VPN. Puede configurar una sesión VPN de duración máxima menor para cumplir con los requisitos de seguridad y conformidad. De forma predeterminada, la duración máxima de la sesión VPN es de 24 horas.

> **Note**
>
> Cuando se reduce el valor máximo de duración de la sesión VPN, se desconectarán las sesiones VPN activas anteriores al nuevo valor de tiempo de espera.

Consulte Notas de la versión del cliente proporcionado por AWS en la Guía del usuario de AWS Client VPN para obtener más detalles sobre las aplicaciones de escritorio del cliente.

Contenido

- Configurar la sesión VPN máxima durante la creación de un punto de conexión de Client VPN
- Ver la duración máxima de la sesión VPN actual
- Modificar la duración máxima de la sesión VPN

Configurar la sesión VPN máxima durante la creación de un punto de conexión de Client VPN

Para obtener detalles sobre los pasos para configurar la sesión VPN máxima durante la creación de un punto de conexión de Client VPN, consulte Creación de un punto de enlace de Client VPN.

Ver la duración máxima de la sesión VPN actual

Siga estos pasos para ver la duración de la sesión de VPN máxima actual.

Ver la duración de la sesión de Client VPN (consola) de un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea ver.
4. Verifique que la pestaña Details (Detalles) esté seleccionada.
5. Consulte la duración máxima de la sesión VPN actual junto al Tiempo de espera de la sesión.

Ver la duración máxima de la sesión de Client VPN para un punto de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

Modificar la duración máxima de la sesión VPN

Siga los pasos siguientes para modificar la duración máxima de una sesión VPN existente.

Modificar la duración máxima de una sesión VPN existente para un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN endpoints (Puntos de conexión de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. Para el Session timeout hours (Tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas.
5. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Modificar la duración máxima de una sesión VPN existente para un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Seguridad en AWS Client VPN

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener información sobre los programas de conformidad que se aplican a AWS Client VPN, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

AWS Client VPN forma parte del servicio Amazon VPC. Para obtener más información sobre la seguridad en Amazon VPC, consulte Seguridad en la Guía del usuario de Amazon VPC.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida al utilizar Client VPN. En los siguientes temas, aprenderá a configurar Client VPN para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios de AWS que le ayudarán a monitorear y proteger los recursos de Client VPN.

Contenido

- Protección de datos en AWS Client VPN
- Administración de identidad y acceso para AWS Client VPN
- Resiliencia en AWS Client VPN
- Seguridad de la infraestructura en AWS Client VPN
- Prácticas recomendadas de seguridad para AWS Client VPN
- Consideraciones sobre IPv6 para AWS Client VPN

Protección de datos en AWS Client VPN

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de en AWS Client VPN. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Es responsable de mantener el control sobre su contenido que se encuentra alojado en esta infraestructura. También es responsable de la configuración de seguridad y las tareas de administración de los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog AWSShared Responsibility Model and GDPR en el Blog de seguridad de AWS.

A los fines de la protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe solamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilizar la autenticación multifactor (MFA) en cada cuenta.
- Utilizar SSL/TLS para comunicarse con los recursos de AWS. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configurar la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilizar las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión habilitado para FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Recomendamos firmemente nunca ingresar información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando se trabaja con Client VPN u otros Servicios de AWS con la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en tránsito

AWS Client VPN proporciona conexiones seguras desde cualquier ubicación mediante seguridad de la capa de transporte (TLS) 1.2 o una versión posterior.

Privacidad del tráfico entre redes

Activación del acceso entre redes

Puede permitir que los clientes se conecten a la VPC y a otras redes a través de un punto de enlace de Client VPN. Para obtener más información y ejemplos, consulte Escenarios y ejemplos para AWS Client VPN.

Restringir el acceso a las redes

Puede configurar el punto de enlace de Client VPN para restringir el acceso a recursos específicos de la VPC. En la autenticación basada en usuarios, también puede restringir el acceso a partes de la red en función del grupo de usuarios que accede al punto de enlace de Client VPN. Para obtener más información, consulte Restricción del acceso a su red mediante AWS Client VPN.

Autenticación de clientes

La autenticación es lo primero que se implementa en la nube de AWS. Se utiliza para determinar si los clientes tienen permiso para conectarse al punto de enlace de Client VPN. Si la autenticación se realiza correctamente, los clientes se conectan al punto de enlace de Client VPN y establecen una sesión de VPN. Si la autenticación falla, se deniega la conexión y el cliente no podrá establecer una sesión de VPN.

Client VPN permite utilizar los siguientes tipos de autenticación de cliente:

- Autenticación con Active Directory (basada en el usuario)
- Autenticación mutua (basada en certificados)
- Inicio de sesión único (autenticación federada basada en SAML) (basada en el usuario)

Administración de identidad y acceso para AWS Client VPN

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Client VPN. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona AWS Client VPN con IAM
- Ejemplos de políticas basadas en identidad para Client VPN AWS
- Solución de problemas de identidad y acceso a AWS Client VPN
- Uso de roles vinculados a servicios en Client VPN

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Client VPN.

Usuario de servicio: si utiliza el servicio de Client VPN para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Client VPN para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Client VPN, consulte Solución de problemas de identidad y acceso a AWS Client VPN.

Administrador de servicio: si está a cargo de los recursos de Client VPN en su empresa, probablemente tenga acceso completo a Client VPN. Su trabajo consiste en determinar a qué características y recursos de Client VPN deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Client VPN, consulte Cómo funciona AWS Client VPN con IAM.

Administrador de IAM: si es administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Client VPN. Para consultar ejemplos de políticas

basadas en la identidad de Client VPN que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad para Client VPN AWS.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las

tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios

tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una

solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus

cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS Client VPN con IAM

Antes de utilizar IAM para administrar el acceso a Client VPN, conozca qué características de IAM se pueden utilizar con Client VPN.

Funciones de IAM que puede utilizar con AWS Client VPN

Característica de IAM	Compatibilidad con Client VPN
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí

Característica de IAM	Compatibilidad con Client VPN
ACL	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Client VPN y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Client VPN

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Client VPN

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en identidad para Client VPN AWS.

Políticas basadas en recursos dentro de Client VPN

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas para Client VPN

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Client VPN, consulte Acciones definidas por AWS Client VPN en la Referencia de autorización del servicio.

Las acciones de políticas en Client VPN utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en identidad para Client VPN AWS.

Recursos de políticas para Client VPN

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Client VPN y sus ARN, consulte Recursos definidos por AWS Client VPN en la Referencia de autorización del servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Client VPN.

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en identidad para Client VPN AWS.

Claves de condición de política para Client VPN

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Client VPN, consulte Claves de condición de AWS Client VPN en la Referencia de autorización del servicio. Para saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones definidas por AWS Client VPN.

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en identidad para Client VPN AWS.

Las ACL en Client VPN

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Client VPN

Admite ABAC (etiquetas en las políticas)	No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Client VPN

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios para Client VPN

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción

en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Client VPN

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Client VPN. Edite los roles de servicio solo cuando Client VPN proporcione orientación para hacerlo.

Uso de roles vinculados a servicios en Client VPN

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Client VPN AWS

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Client VPN. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Client VPN, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de AWS Client VPN en la Referencia de autorización del servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Client VPN de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

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

Solución de problemas de identidad y acceso a AWS Client VPN

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Client VPN e IAM.

Temas

- No tengo autorización para realizar una acción en Client VPN
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Client VPN

No tengo autorización para realizar una acción en Client VPN

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `ec2:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `ec2:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deberán actualizarse a fin de permitirle pasar un rol a Client VPN.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Client VPN. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Client VPN

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Client VPN admite estas características, consulte Cómo funciona AWS Client VPN con IAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos a través de Cuentas de AWS los suyos, consulte Proporcionar acceso a un usuario de IAM en otro de su Cuenta de AWS propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles vinculados a servicios en Client VPN

AWS Client VPN utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Client VPN. Los roles vinculados a servicios están predefinidos por Client VPN e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Temas

- Uso de roles para Client VPN
- Uso de roles para la autorización de conexiones

Uso de roles para Client VPN

AWS Client VPN utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Client VPN. Los roles vinculados a servicios están predefinidos por Client VPN e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Client VPN porque ya no tendrá que agregar manualmente los permisos necesarios. Client VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Client VPN puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar una función vinculada a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Client VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service-linked roles (Roles vinculados a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios en Client VPN

Client VPN utiliza el rol vinculado a servicios denominado AWSServiceRoleForClientVPN: permite a Client VPN crear y gestionar recursos relacionados con las conexiones de Client VPN.

El rol vinculado al servicio AWSServiceRoleForClientVPN confía en el siguiente servicio para que asuma el rol:

- `clientvpn.amazonaws.com`

La política de permisos llamada ClientVPNServiceRolePolicy permite a Client VPN realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:CreateNetworkInterface` en `Resource: "*"`
- Acción: `ec2:CreateNetworkInterfacePermission` en `Resource: "*"`
- Acción: `ec2:DescribeSecurityGroups` en `Resource: "*"`

- Acción: `ec2:DescribeVpcs` en `Resource: "*"`
- Acción: `ec2:DescribeSubnets` en `Resource: "*"`
- Acción: `ec2:DescribeInternetGateways` en `Resource: "*"`
- Acción: `ec2:ModifyNetworkInterfaceAttribute` en `Resource: "*"`
- Acción: `ec2:DeleteNetworkInterface` en `Resource: "*"`
- Acción: `ec2:DescribeAccountAttributes` en `Resource: "*"`
- Acción: `ds:AuthorizeApplication` en `Resource: "*"`
- Acción: `ds:DescribeDirectories` en `Resource: "*"`
- Acción: `ds:GetDirectoryLimits` en `Resource: "*"`
- Acción: `ds:UnauthorizeApplication` en `Resource: "*"`
- Acción: `logs:DescribeLogStreams` en `Resource: "*"`
- Acción: `logs:CreateLogStream` en `Resource: "*"`
- Acción: `logs:PutLogEvents` en `Resource: "*"`
- Acción: `logs:DescribeLogGroups` en `Resource: "*"`
- Acción: `acm:GetCertificate` en `Resource: "*"`
- Acción: `acm:DescribeCertificate` en `Resource: "*"`
- Acción: `iam:GetSAMLProvider` en `Resource: "*"`
- Acción: `lambda:GetFunctionConfiguration` en `Resource: "*"`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Client VPN

No necesita crear manualmente un rol vinculado a servicios. Cuando se crea el primer punto de conexión de Client VPN en la cuenta con la AWS Management Console, la AWS CLI y la API de AWS, Client VPN crea el rol vinculado a servicios para usted.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando se crea el primer punto de conexión de Client VPN en la cuenta, Client VPN crea el rol vinculado a servicios para usted de nuevo.

Edición de roles vinculados a servicios en Client VPN

Client VPN no permite editar el rol AWSServiceRoleForClientVPN vinculado a servicios. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de roles vinculados a servicios en Client VPN

Si ya no tiene que utilizar Client VPN, le recomendamos que elimine el rol vinculado a servicios AWSServiceRoleForClientVPN.

Primero debe eliminar los recursos de Client VPN relacionados. Esto garantiza que no pueda eliminar accidentalmente el permiso para obtener acceso a los recursos.

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de Client VPN

Client VPN admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de enlace y regiones de AWS.

Uso de roles para la autorización de conexiones

AWS Client VPN utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Client VPN. Los roles vinculados a servicios están predefinidos por Client VPN e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Client VPN porque ya no tendrá que agregar manualmente los permisos necesarios. Client VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Client VPN puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar una función vinculada a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Client VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service-linked roles (Roles vinculados a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios en Client VPN

Client VPN utiliza el rol vinculado a servicios denominado AWSServiceRoleForClientVPNConnections: rol vinculado a servicios para conexiones de Client VPN.

El rol AWSServiceRoleForClientVPNConnections vinculado a servicios confía en que los siguientes servicios asuman el rol:

- `clientvpn-connections.amazonaws.com`

La política de permisos llamada ClientVPNServiceConnectionsRolePolicy permite a Client VPN realizar las siguientes acciones en los recursos especificados:

- Acción: `lambda:InvokeFunction` en `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Client VPN

No necesita crear manualmente un rol vinculado a servicios. Cuando se crea el primer punto de conexión de Client VPN en la cuenta con la AWS Management Console, la AWS CLI y la API de AWS, Client VPN crea el rol vinculado a servicios para usted.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando se crea el primer punto de conexión de Client VPN en la cuenta, Client VPN crea el rol vinculado a servicios para usted de nuevo.

Edición de roles vinculados a servicios en Client VPN

Client VPN no permite editar el rol AWSServiceRoleForClientVPNConnections vinculado a servicios. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol

mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de roles vinculados a servicios en Client VPN

Si ya no tiene que utilizar Client VPN, le recomendamos que elimine el rol vinculado a servicios AWSServiceRoleForClientVPNConnections.

Primero debe eliminar los recursos de Client VPN relacionados. Esto garantiza que no pueda eliminar accidentalmente el permiso para obtener acceso a los recursos.

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de Client VPN

Client VPN admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de enlace y regiones de AWS.

Resiliencia en AWS Client VPN

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, AWS Client VPN ofrece características que lo ayudan en sus necesidades de resiliencia y copia de seguridad de los datos.

Varias redes de destino para disfrutar de una alta disponibilidad

Puede asociar una red de destino con un punto de enlace de Client VPN para permitir que los clientes establezcan sesiones de VPN. Las redes de destino son subredes de la VPC. Cada una

de las subredes que asocie con el punto de enlace de Client VPN debe pertenecer a una zona de disponibilidad diferente. Puede asociar varias subredes con un punto de enlace de Client VPN para disfrutar de una alta disponibilidad.

Seguridad de la infraestructura en AWS Client VPN

Como se trata de un servicio administrado, AWS Client VPN está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Se utilizan las llamadas a la API publicadas por AWS para acceder a la Client VPN a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prácticas recomendadas de seguridad para AWS Client VPN

AWS Client VPN proporciona un número de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Reglas de autorización

Utilice reglas de autorización para restringir los usuarios que pueden acceder a la red. Para obtener más información, consulte Reglas de autorización.

Grupos de seguridad

Utilice grupos de seguridad para controlar a qué recursos de la VPC pueden acceder los usuarios. Para obtener más información, consulte Grupos de seguridad.

Listas de revocación de certificados del cliente

Puede utilizar listas de revocación de certificados de cliente para revocar el acceso a un punto de enlace de Client VPN en certificados de cliente específicos. Por ejemplo, cuando un usuario abandona la organización. Para obtener más información, consulte Listas de revocación de certificados del cliente.

Herramientas de monitoreo

Utilice herramientas de supervisión para realizar un seguimiento de la disponibilidad y el rendimiento de los puntos de enlace de Client VPN. Para obtener más información, consulte Monitorización de AWS Client VPN.

Administración de identidades y accesos

Administre el acceso a los recursos y las API de Client VPN utilizando políticas de IAM con los usuarios y roles de IAM. Para obtener más información, consulte Administración de identidad y acceso para AWS Client VPN.

Consideraciones sobre IPv6 para AWS Client VPN

Actualmente, el servicio Client VPN no admite el enrutamiento del tráfico IPv6 a través del túnel VPN. Sin embargo, hay casos en los que el tráfico IPv6 debe enrutarse al túnel VPN para evitar fugas de IPv6. La fuga de IPv6 puede ocurrir cuando IPv4 e IPv6 están habilitados y conectados a la VPN, pero la VPN no enruta el tráfico IPv6 a su túnel. En este caso, cuando se conecta a un destino habilitado para IPv6, todavía se está conectando con su dirección IPv6 proporcionada por su ISP. Esto filtrará su dirección IPv6 real. Las siguientes instrucciones explican cómo enrutar el tráfico IPv6 al túnel VPN.

Las siguientes directivas relacionadas con IPv6 deben agregarse al archivo de configuración de Client VPN para evitar fugas de IPv6:

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

Por ejemplo:

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

En este ejemplo, `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` configurará la dirección IPv6 del dispositivo de túnel local como `fd15:53b6:dead::2` y la dirección IPv6 del punto de enlace VPN remoto como `fd15:53b6:dead::1`.

El siguiente comando, `route-ipv6 2000::/4` enrutará las direcciones IPv6 de `2000:0000:0000:0000:0000:0000:0000:0000` a `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` en la conexión de VPN.

> **Note**
>
> Para el enrutamiento de dispositivos “TAP” en Windows, por ejemplo, el segundo parámetro de `ifconfig-ipv6` se usará como destino de ruta para `--route-ipv6`.

Las organizaciones deben configurar los dos parámetros de `ifconfig-ipv6` ellos mismos, y pueden usar direcciones en `100::/64` (de `0100:0000:0000:0000:0000:0000:0000:0000` a `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) o `fc00::/7` (de `fc00:0000:0000:0000:0000:0000:0000:0000` a `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` es un bloque de direcciones de descarte únicamente, y `fc00::/7` es local y único.

Otro ejemplo.

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

En este ejemplo, la configuración enrutará todo el tráfico IPv6 asignado actualmente a la conexión de VPN.

Verification (Verificación)

Es probable que su organización tenga sus propias pruebas. Una verificación básica consiste en configurar una conexión de VPN de túnel completa y, a continuación, ejecutar ping6 en un servidor

IPv6 utilizando la dirección IPv6. La dirección IPv6 del servidor debe estar en el rango especificado por el comando `route-ipv6`. Esta prueba de ping debería fallar. Sin embargo, esto puede cambiar si la compatibilidad con IPv6 se agrega al servicio de Client VPN en el futuro. Si el ping se realiza correctamente y puede acceder a sitios públicos cuando está conectado en modo túnel completo, es posible que tenga que hacer pruebas para solucionar el problema. También puede probar usando algunas herramientas disponibles públicamente como ipleak.org.

Monitorización de AWS Client VPN

La supervisión tiene un papel importante en el mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Client VPN, así como de las demás soluciones de AWS. Puede utilizar las siguientes características para monitorear los puntos de enlace de Client VPN, analizar sus patrones de tráfico y solucionar sus problemas.

Amazon CloudWatch

Monitoriza los recursos de AWS y las aplicaciones que se ejecutan en AWS en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede hacer que CloudWatch haga un seguimiento del uso de la CPU u otras métricas de las instancias de Amazon EC2 y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

AWS CloudTrail

Captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Amazon CloudWatch Logs

Permite monitorizar los intentos de conexión realizados al punto de enlace de AWS Client VPN. Puede ver los intentos de conexión y los restablecimientos de conexiones de Client VPN. Para los intentos de conexión, puede ver tanto los correctos como los fallidos. Puede especificar la secuencia de registros de CloudWatch Logs que va a registrar los detalles de la conexión. Para obtener más información, consulte Registro de conexión y la Guía del usuario de Amazon CloudWatch Logs.

Métricas de CloudWatch para AWS Client VPN

AWS Client VPN publica las siguientes métricas en Amazon CloudWatch para los puntos de conexión de Client VPN. Las métricas se publican en Amazon CloudWatch cada cinco minutos.

Métrica	Descripción
ActiveConnectionsCount	Número de conexiones activas en el punto de enlace de Client VPN. Unidades: recuento
AuthenticationFailures	Número de errores de autenticación del punto de enlace de Client VPN. Unidades: recuento
CrlDaysToExpiry	Número de días hasta que expire la lista de revocación de certificados (CRL) configurada en el punto de enlace de Client VPN. Unidades: días
EgressBytes	Número de bytes enviados desde el punto de enlace de Client VPN. Unidades: bytes
EgressPackets	Número de paquetes enviados desde el punto de enlace de Client VPN. Unidades: recuento
IngressBytes	Número de bytes recibidos por el punto de enlace de Client VPN. Unidades: bytes
IngressPackets	Número de paquetes recibidos por el punto de enlace de Client VPN. Unidades: recuento
SelfServicePortalClientConfigurationDownloads	Número de descargas del archivo de configuración del punto de enlace de Client VPN realizadas en el portal de autoservicio.

Métrica	Descripción
	Unidad: recuento

AWS Client VPN publica las siguientes métricas de evaluación de la posición para los puntos de conexión de Client VPN.

Métrica	Descripción
ClientConnectHandlerTimeouts	Número de tiempos de espera en la invocación del controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerInvalidResponses	Número de respuestas no válidas que devuelve el controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerOtherExecutionErrors	Número de errores inesperados en la ejecución del controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerThrottlingErrors	Número de errores de limitación en la invocación del controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento

Métrica	Descripción
ClientConnectHandlerDeniedConnections	Número de conexiones que deniega el controlador de conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerFailedServiceErrors	Número de errores del lado del servicio en el que se ejecuta el controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento

Puede filtrar las métricas de cada punto de enlace de Client VPN.

CloudWatch permite recuperar las estadísticas sobre estos puntos de datos como un conjunto ordenado de datos de serie temporal denominado métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Ver métricas de CloudWatch en

Puede ver las métricas de su punto de conexión de Client VPN de la manera siguiente.

Para ver las métricas a través de la consola de CloudWatch

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (Métricas).

3. En All metrics (Todas las métricas), elija el espacio de nombres de métricas ClientVPN.
4. Para ver las métricas, seleccione la dimensión de métricas by endpoint (por punto de conexión).

Para ver métricas mediante la AWS CLI

En el símbolo del sistema, use el siguiente comando para enumerar las métricas que están disponibles para Client VPN.

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

Registros de CloudTrail para AWS Client VPN

AWS Client VPN está integrado en AWS CloudTrail, un servicio que registra las acciones que lleva a cabo un usuario, un rol o un servicio de AWS en Client VPN. CloudTrail captura como eventos todas las llamadas a las API de Client VPN. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Client VPN, así como las llamadas de código realizadas a las operaciones de API de Client VPN. Si crea un registro de seguimiento, puede activar la entrega continua de eventos de CloudTrail en un bucket de Amazon S3, incluidos los eventos de Client VPN. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Utilice la información que CloudTrail recopila para determinar la solicitud que se envió a Client VPN, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo la realizó y otros detalles.

Para obtener más información acerca de CloudTrail, consulte la AWS CloudTrailGuía del usuario de .

Información de Client VPN en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Client VPN, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS y se agrega a Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Client VPN, cree una traza. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS.

El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Consulte Servicios e integraciones compatibles con CloudTrail.
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Para obtener más información, consulte Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas.

Todas las acciones de Client VPN se registran en CloudTrail y están documentadas en la Referencia de las API de Amazon EC2. Por ejemplo, las llamadas a las acciones `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` y `AuthorizeClientVpnIngress` generan entradas en los archivos de log de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas del archivo de registro de Client VPN

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Para obtener más información, consulte Logging Amazon EC2, Amazon EBS, and Amazon VPC API calls with AWS CloudTrail en la Referencia de las API de Amazon EC2.

AWS Cuotas de Client VPN

Su AWS cuenta tiene las siguientes cuotas, anteriormente denominadas límites, relacionadas con los puntos de conexión de Client VPN. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para solicitar un aumento de una cuota ajustable, elija Yes (Sí) en la columna Adjustable (Ajustable). Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Cuotas de Client VPN

Nombre	Valor predeterminado	Ajustable
Reglas de autorización por punto de enlace de Client VPN	50	Sí
Puntos de enlace de Client VPN por región	5	Sí
Conexiones de cliente simultáneas por punto de enlace de Client VPN	Este valor depende de la cantidad de asociaciones de subred por punto de enlace. • 1 — 20 000 • 2 - 36 500 • 3 - 66 500 • 4 - 96 500 • 5 - 126 000	Sí
Operaciones simultáneas por punto de enlace de Client VPN †	10	No
Entradas en una lista de revocación de certificados del cliente para puntos de enlace de Client VPN	20 000	No

Nombre	Valor predeterminado	Ajustable
Rutas por punto de enlace de Client VPN	10	Sí

Entre las operaciones † se incluyen:

- Asociar o desasociar subredes
- Crear o eliminar rutas
- Crear o eliminar reglas de entrada y salida
- Crear o eliminar grupos de seguridad

Cuotas de usuarios y grupos

Al configurar usuarios y grupos para Active Directory o un IdP basado en SAML, se aplican las cuotas siguientes:

- Los usuarios pueden pertenecer a un máximo de 200 grupos. Se ignora cualquier grupo después de superar el límite de 200 indicado.
- La longitud máxima del ID de grupo es de 255 caracteres.
- La longitud máxima del ID de nombre es de 255 caracteres. Se trunca cualquier carácter después de superar el límite de 255 indicado.

Consideraciones generales

Tenga en cuenta lo siguiente cuando utilice los puntos de enlace de Client VPN:

- Si usa Active Directory para autenticar al usuario, el punto final Client VPN debe pertenecer a la misma cuenta que el AWS Directory Service recurso utilizado para la autenticación de Active Directory.
- Si utilizas la autenticación federada basada en SAML para autenticar a un usuario, el punto final Client VPN debe pertenecer a la misma cuenta que el proveedor de identidades SAML de IAM que hayas creado para definir la relación entre el IDP y la confianza.AWS El proveedor de identidad SAML de IAM se puede compartir en varios puntos de conexión Client VPN de la misma cuenta. AWS

Solución de problemas de AWS Client VPN

El siguiente tema le puede ayudar a solucionar los problemas que podrían presentarse con un punto de enlace de Client VPN.

Para obtener más información acerca de cómo solucionar los problemas del software basado en OpenVPN que utilizan los clientes para conectarse a Client VPN, consulte Solución de problemas de conexión de Client VPN en la Guía del usuario de AWS Client VPN .

Problemas comunes

- No se puede resolver el nombre de DNS del punto de enlace de Client VPN
- El tráfico no se divide entre subredes
- Las reglas de autorización para grupos de Active Directory no funcionan de la forma prevista
- Los clientes no pueden acceder a una VPC interconectada, a Amazon S3 o a Internet
- El acceso a una VPC interconectada, a Amazon S3 o a Internet es intermitente
- El software cliente devuelve un error de TLS
- El software cliente devuelve errores de nombre de usuario y contraseña (autenticación de Active Directory)
- El software cliente devuelve errores de nombre de usuario y contraseña (autenticación federada)
- Los clientes no pueden conectarse (autenticación mutua)
- El cliente devuelve un error que indica que se ha superado el tamaño máximo de las credenciales (autenticación federada)
- El cliente no abre el navegador (autenticación federada)
- El cliente devuelve un error que indica que no hay puertos disponibles (autenticación federada)
- La conexión VPN se interrumpió debido a una discordancia de IP
- El enrutamiento del tráfico a la LAN no funciona según lo esperado
- Comprobación del límite de ancho de banda de un punto de enlace de Client VPN

No se puede resolver el nombre de DNS del punto de enlace de Client VPN

Problema

No puedo resolver el nombre de DNS del punto de enlace de Client VPN.

Causa

El archivo de configuración del punto de enlace de Client VPN contiene un parámetro llamado `remote-random-hostname`. Este parámetro obliga al cliente a prefijar una cadena aleatoria al nombre de DNS para evitar el almacenamiento en caché del DNS. Algunos clientes no reconocen este parámetro y, por lo tanto, no prefijan la cadena aleatoria requerida al nombre de DNS.

Solución

Abra el archivo de configuración del punto de enlace de Client VPN con el editor de texto que prefiera. Busque la línea que especifica el nombre de DNS del punto de enlace de Client VPN y asígnele como prefijo una cadena aleatoria de manera que el formato sea *`cadena_aleatoria.nombre_DNS_mostrado`*. Por ejemplo:

- Nombre de DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nombre de DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

El tráfico no se divide entre subredes

Problema

Estoy tratando de dividir el tráfico de red entre dos subredes. El tráfico privado debe direccionarse a través de una subred privada, mientras que el tráfico de Internet debe direccionarse a través de una subred pública. Sin embargo, solo se utiliza una ruta, aunque he agregado las dos a la tabla de enrutamiento del punto de enlace de Client VPN.

Causa

Puede asociar varias subredes a un punto de enlace de Client VPN, pero solo puede asociar una subred por zona de disponibilidad. La finalidad de la asociación de varias subredes es proporcionar a los clientes alta disponibilidad y redundancia de zonas de disponibilidad. Sin embargo, la VPN de cliente no permite dividir el tráfico de forma selectiva entre las subredes asociadas con el punto de enlace de la VPN del cliente.

Los clientes se conectan a un punto de enlace de VPN de cliente basado en el algoritmo rotativo de DNS. Esto significa que su tráfico se puede direccionar a través de cualquiera de las subredes

asociadas cuando establecen una conexión. Por lo tanto, pueden experimentar problemas de conectividad si acaban en una subred asociada que no tiene las entradas de rutas necesarias.

Por ejemplo, supongamos que configura las siguientes asociaciones y rutas de subred:

- Asociaciones de subred
  - Asociación 1: Subred A (us-east-1a)
  - Asociación 2: Subred B (us-east-1b)
- Rutas
  - Ruta 1:10.0.0.0/16 direccionada a la Subred A
  - Ruta 2:172.31.0.0/16 direccionada a la Subred B

En este ejemplo, los clientes que acaban en la Subred A cuando se conectan no pueden acceder a la Ruta 2, mientras que los clientes que acaban en la Subred B cuando se conectan no pueden acceder a la Ruta 1.

Solución

Compruebe que el punto de enlace de VPN de cliente tiene las mismas entradas de ruta con destinos para cada red asociada. Esto garantiza que los clientes tengan acceso a todas las rutas independientemente de la subred a través de la cual se direcciona su tráfico.

Las reglas de autorización para grupos de Active Directory no funcionan de la forma prevista

Problema

He configurado reglas de autorización para mis grupos de Active Directory, pero no funcionan como esperaba. He agregado una regla de autorización para `0.0.0.0/0` para autorizar el tráfico para todas las redes, pero el tráfico sigue fallando para los CIDR con destinos específicos.

Causa

Las reglas de autorización se indexan en los CIDR de red. Las reglas de autorización deben conceder acceso a los grupos de Active Directory a CIDR de red específicos. Las reglas de autorización para `0.0.0.0/0` se tratan como un caso especial y, por lo tanto, se evalúan en último lugar, independientemente del orden en que se creen las reglas de autorización.

Por ejemplo, supongamos que crea cinco reglas de autorización en el siguiente orden:

- Regla 1: Acceso del grupo 1 a `10.1.0.0/16`
- Regla 2: acceso del grupo 1 a `0.0.0.0/0`
- Regla 3: acceso del grupo 2 a `0.0.0.0/0`
- Regla 4: acceso del grupo 3 a `0.0.0.0/0`
- Regla 5: acceso del grupo 2 a `172.131.0.0/16`

En este ejemplo, la regla 2, la regla 3 y la regla 4 se evalúan en último lugar. El Grupo 1 solo tiene acceso a `10.1.0.0/16` y el Grupo 2 solo tiene acceso a `172.131.0.0/16`. El Grupo 3 no tiene acceso a `10.1.0.0/16` ni `172.131.0.0/16`, pero tiene acceso a todas las demás redes. Si quita las reglas 1 y 5, los tres grupos tienen acceso a todas las redes.

Client VPN utiliza la coincidencia de prefijos más larga al evaluar las reglas de autorización. Consulte Prioridad de la ruta en la Guía del usuario de Amazon VPC para obtener más información.

Solución

Compruebe que las reglas de autorización que crea conceden explícitamente a los grupos de Active Directory acceso a CIDR de red específicos. Si agrega una regla de autorización para `0.0.0.0/0`, tenga en cuenta que se evaluará en último lugar y que las reglas de autorización anteriores podrían limitar las redes a las que concede acceso.

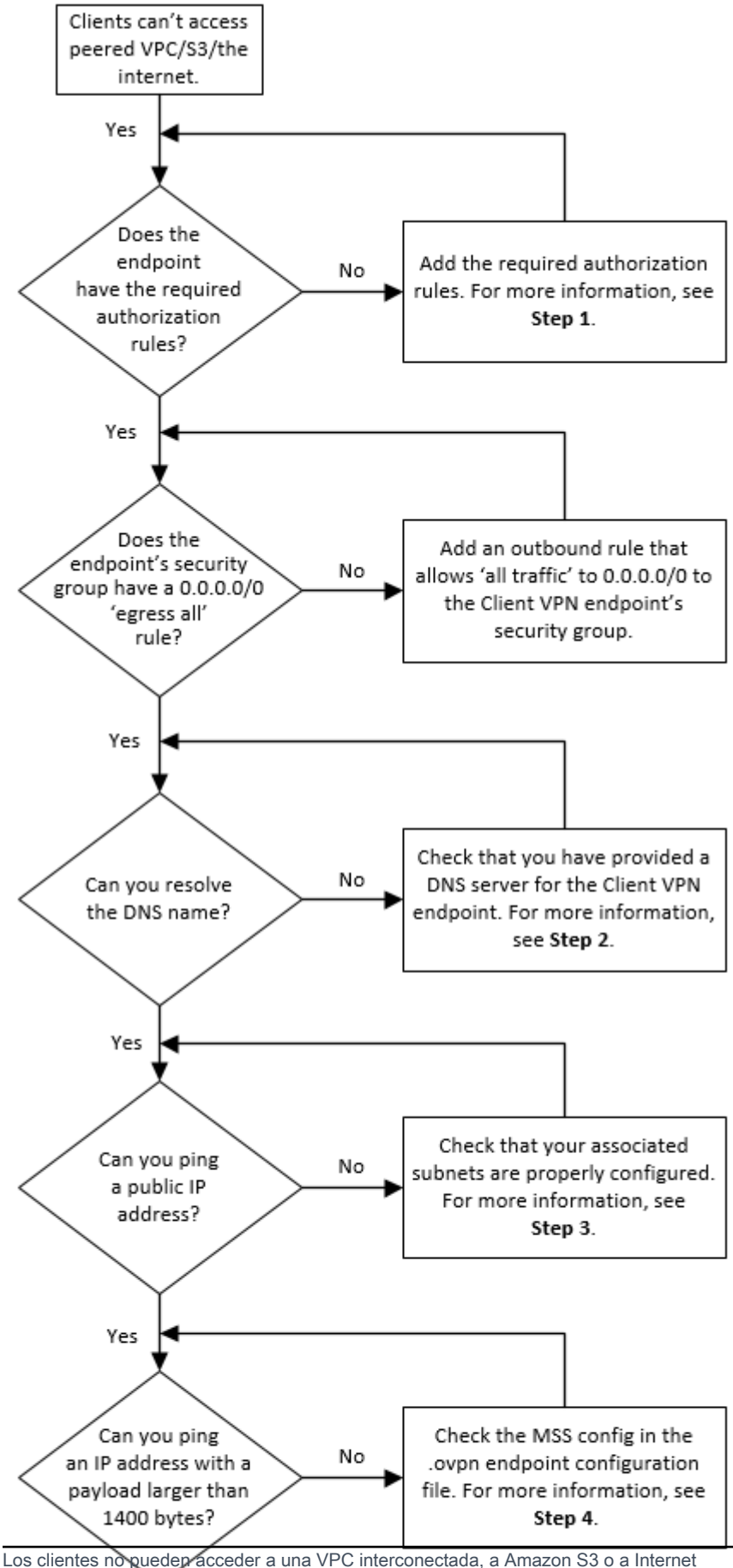
Los clientes no pueden acceder a una VPC interconectada, a Amazon S3 o a Internet

Problema

He configurado correctamente las rutas del punto de enlace de Client VPN, pero mis clientes no pueden acceder a una VPC interconectada, a Amazon S3 ni a Internet.

Solución

El siguiente diagrama de flujo contiene los pasos para diagnosticar problemas de conectividad de Internet, de las VPC interconectadas y de 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. Para obtener acceso a Internet, agregue una regla de autorización para `0.0.0.0/0`.

   Para obtener acceso a una VPC interconectada, agregue una regla de autorización para el rango de CIDR IPv4 de la VPC.

   Para obtener acceso a S3, especifique la dirección IP del punto de enlace de Amazon S3.
2. Compruebe si puede resolver el nombre de DNS.

   Si no puede resolver el nombre de DNS, compruebe que ha especificado los servidores DNS del punto de enlace de Client VPN. Si administra su propio servidor DNS, especifique su dirección IP. Compruebe que el servidor DNS sea accesible desde la VPC.

   Si no está seguro de qué dirección IP especificar para los servidores DNS, especifique el solucionador de DNS de VPC en la dirección IP .2 de la VPC.
3. Para el acceso a Internet, compruebe si puede hacer ping a una dirección IP pública o a un sitio web público, por ejemplo, `amazon.com`. Si no obtiene respuesta, asegúrese de que la tabla de enrutamiento de las subredes asociadas tiene una ruta predeterminada que está dirigida a una gateway de Internet o a una gateway NAT. Si la ruta está en su lugar, compruebe que la subred asociada no tenga reglas de listas de control de acceso de red que bloqueen el tráfico entrante y saliente.

   Si no puede conectarse a una VPC interconectada, compruebe que la tabla de enrutamiento de la subred asociada tenga una entrada de ruta para la VPC interconectada.

   Si no puede conectarse a Amazon S3, compruebe que la tabla de enrutamiento de la subred asociada tiene una entrada de ruta para el punto de enlace de la VPC de la gateway.
4. Compruebe si puede hacer ping a una dirección IP pública con una carga superior a 1400 bytes. Utilice uno de los siguientes comandos:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

Si no puede hacer ping a una dirección IP con una carga superior a 1400 bytes, abra el archivo de configuración `.ovpn` del punto de enlace de Client VPN utilizando el editor de texto que prefiera y agregue lo siguiente.

```
mssfix 1328
```

El acceso a una VPC interconectada, a Amazon S3 o a Internet es intermitente

Problema

Tengo problemas de conectividad intermitentes cuando me conecto a una VPC interconectada, a Amazon S3 o a Internet, pero el problema no ocurre cuando me conecto a las subredes asociadas. Tengo que desconectarme y volver a conectarme para resolver los problemas de conectividad.

Causa

Los clientes se conectan a un punto de enlace de VPN de cliente basado en el algoritmo rotativo de DNS. Esto significa que su tráfico se puede direccionar a través de cualquiera de las subredes asociadas cuando establecen una conexión. Por lo tanto, pueden experimentar problemas de conectividad si acaban en una subred asociada que no tiene las entradas de rutas necesarias.

Solución

Compruebe que el punto de enlace de VPN de cliente tiene las mismas entradas de ruta con destinos para cada red asociada. Esto garantiza que los clientes tengan acceso a todas las rutas independientemente de la subred asociada a través de la cual se direcciona su tráfico.

Por ejemplo, supongamos que su punto de enlace de VPN de cliente tiene tres subredes asociadas (Subred A, B y C) y desea habilitar el acceso a Internet para sus clientes. Para ello, debe agregar tres rutas de `0.0.0.0/0` que se dirijan a cada subred asociada:

- Ruta 1: `0.0.0.0/0` para la Subred A
- Ruta 2: `0.0.0.0/0` para la Subred B
- Ruta 3: `0.0.0.0/0` para la Subred C

El software cliente devuelve un error de TLS

Problema

Antes podía conectar mis clientes a Client VPN sin ningún problema, pero ahora el cliente basado en OpenVPN devuelve uno de los siguientes errores cuando intenta conectarse:

```
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.
```

Causa posible n.º 1

Si utiliza la autenticación mutua y ha importado una lista de revocación de certificados de cliente, es posible que la lista de revocación de certificados de cliente haya caducado. Durante la fase de autenticación, el punto de enlace de Client VPN comprueba el certificado de cliente en la lista de revocación de certificados de cliente que ha importado. Si esta lista ha caducado, no puede conectarse al punto de enlace de Client VPN.

Solución n.º 1

Compruebe la fecha de caducidad de su lista de revocación de certificados de cliente con la herramienta OpenSSL.

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

La salida muestra la fecha y la hora de caducidad. Si la lista de revocación de certificados de cliente ha caducado, debe crear una nueva e importarla al punto de enlace de Client VPN. Para obtener más información, consulte Listas de revocación de certificados del cliente.

Causa posible n.º 2

El certificado de servidor que se utiliza para el punto de conexión de Client VPN ha caducado.

Solución n.º 2

Compruebe el estado del certificado de servidor en la AWS Certificate Manager consola o mediante la AWS CLI. Si el certificado del servidor ha caducado, cree uno nuevo y cárguelo en ACM. Para

conocer los pasos detallados para generar los certificados y las claves del servidor y del cliente mediante la utilidad easy-rsa de OpenVPN e importarlos a ACM, consulte Autenticación mutua.

También es posible que haya un problema con el software basado en OpenVPN que el cliente está utilizando para conectarse a Client VPN. Para obtener más información acerca de cómo solucionar los problemas del software basado en OpenVPN, consulte Solución de problemas de la conexión de Client VPN en la AWS Client VPN Guía del usuario.

El software cliente devuelve errores de nombre de usuario y contraseña (autenticación de Active Directory)

Problema

Utilizo la autenticación de Active Directory con el punto de enlace de Client VPN y antes podía conectar los clientes a Client VPN correctamente. Pero ahora los clientes están recibiendo errores de nombre de usuario y contraseña no válidos.

Causas posibles

Si utiliza la autenticación de Active Directory y ha habilitado la autenticación multifactor (MFA) después de distribuir el archivo de configuración del cliente, el archivo no contiene la información necesaria para solicitar a los usuarios que introduzcan su código MFA. A los usuarios se les pide que introduzcan únicamente su nombre de usuario y contraseña, por lo que la autenticación falla.

Solución

Descargue un nuevo archivo de configuración de cliente y distribúyalo entre sus clientes. Compruebe que el archivo contenga la siguiente línea.

```
static-challenge "Enter MFA code " 1
```

Para obtener más información, consulte Exportar y configurar el archivo de configuración del cliente. Pruebe la configuración de MFA de Active Directory sin utilizar el punto de enlace de Client VPN para comprobar que MFA funciona de la forma prevista.

El software cliente devuelve errores de nombre de usuario y contraseña (autenticación federada)

Problema

Al intentar iniciar sesión con un nombre de usuario y una contraseña con autenticación federada, aparece el error «Las credenciales recibidas son incorrectas». Póngase en contacto con su administrador de TI».

Causa

Este error puede deberse a que no se incluye al menos un atributo en la respuesta SAML del IdP.

Solución

Asegúrese de incluir al menos un atributo en la respuesta SAML del IdP. Para obtener más información, consulte Recursos de configuración de IdP basados en SAML.

Los clientes no pueden conectarse (autenticación mutua)

Problema

Utilizo la autenticación mutua con el punto de enlace de Client VPN. Los clientes están recibiendo errores de negociación de claves TLS y errores de tiempo de espera.

Causas posibles

El archivo de configuración proporcionado a los clientes no contiene el certificado del cliente y la clave privada del cliente, o el certificado y la clave son incorrectos.

Solución

Asegúrese de que el archivo de configuración contiene el certificado de cliente y la clave correctos. Si es necesario, corrija el archivo de configuración y vuelva a distribuirlo entre sus clientes. Para obtener más información, consulte Exportar y configurar el archivo de configuración del cliente.

El cliente devuelve un error que indica que se ha superado el tamaño máximo de las credenciales (autenticación federada)

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes escriben el nombre de usuario y la contraseña en la ventana del navegador del proveedor de identidades (IdP) basado en SAML, reciben un error que indica que las credenciales superan el tamaño máximo admitido.

Causa

La respuesta SAML que devuelve el IdP supera el tamaño máximo admitido. Para obtener más información, consulte Requisitos y consideraciones de la autenticación federada basada en SAML.

Solución

Pruebe a reducir el número de grupos a los que pertenece el usuario en el IdP e intente conectarse de nuevo.

El cliente no abre el navegador (autenticación federada)

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes intentan conectarse al punto de enlace, el software del cliente no abre una ventana del navegador y, en su lugar, se muestra una ventana emergente para el nombre de usuario y la contraseña.

Causa

El archivo de configuración proporcionado a los clientes no contiene la marca `auth-federate`.

Solución

Exporte el archivo de configuración más reciente, impórtelo al cliente AWS proporcionado e intente conectarse de nuevo.

El cliente devuelve un error que indica que no hay puertos disponibles (autenticación federada)

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes intentan conectarse al punto de enlace, el software de cliente devuelve el siguiente error:

```
The authentication flow could not be initiated. There are no available ports.
```

Causa

El cliente AWS proporcionado requiere el uso del puerto TCP 35001 para completar la autenticación. Para obtener más información, consulte Requisitos y consideraciones de la autenticación federada basada en SAML.

Solución

Compruebe que el dispositivo del cliente no está bloqueando el puerto TCP 35001 ni lo está utilizando para otro proceso.

La conexión VPN se interrumpió debido a una discordancia de IP

Problema

La conexión VPN ha finalizado y el software del cliente devuelve el siguiente error: `"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

El cliente AWS proporcionado requiere que la dirección IP a la que está conectado coincida con la IP del servidor VPN que respalda el punto final Client VPN. Para obtener más información, consulte Reglas y prácticas recomendadas de AWS Client VPN.

Solución

Compruebe que no haya ningún proxy DNS entre el cliente AWS proporcionado y el punto final Client VPN.

El enrutamiento del tráfico a la LAN no funciona según lo esperado

Problema

El intento de enrutar el tráfico a la red de área local (LAN) no funciona según lo esperado cuando los rangos de direcciones IP de la LAN no se encuentran dentro de los siguientes rangos de direcciones IP privadas estándar: `10.0.0.0/8` `172.16.0.0/12`,`192.168.0.0/16`, o`169.254.0.0/16`.

Causa

Si se detecta que el rango de direcciones LAN del cliente se encuentra fuera de los rangos estándar anteriores, el punto final de Client VPN enviará automáticamente la directiva de OpenVPN «redirect-

gateway block-local» al cliente, obligando a todo el tráfico de la LAN a entrar en la VPN. Para obtener más información, consulte Reglas y prácticas recomendadas de AWS Client VPN.

Solución

Si necesita acceso a una LAN durante las conexiones a la VPN, se recomienda que utilice los rangos de direcciones convencionales enumerados anteriormente para su LAN.

Comprobación del límite de ancho de banda de un punto de enlace de Client VPN

Problema

Tengo que comprobar el límite de ancho de banda de un punto de enlace de Client VPN.

Causa

El rendimiento depende de varios factores, como la capacidad de la conexión desde su ubicación y la latencia de red entre la aplicación de escritorio de Client VPN del equipo y el punto de enlace de la VPC. También hay un límite de ancho de banda de 10 Mbps por conexión de usuario.

Solución

Ejecute los siguientes comandos para verificar el ancho de banda.

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

En el cliente:

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

Historial de revisión de la Guía del usuario de Client VPN

En la siguiente tabla, se describen las actualizaciones de la Guía del administrador de Client VPN de AWS.

Cambio	Descripción	Fecha
Ejemplos de reglas de autorización	Adición de escenarios de ejemplo para las reglas de autorización.	15 de septiembre de 2022
Duración máxima de la sesión VPN	Puede configurar una sesión VPN de duración máxima menor para cumplir con los requisitos de seguridad y conformidad.	20 de enero de 2022
Banner de inicio de sesión de cliente	Puede habilitar un banner de texto en las aplicaciones de escritorio de Client VPN proporcionadas por AWS cuando se establece una sesión de VPN para cumplir con las necesidades normativas y de conformidad.	20 de enero de 2022
Controlador de la conexión del cliente	Puede activar el controlador de la conexión del cliente en el punto de enlace de Client VPN para ejecutar una lógica personalizada que autorice nuevas conexiones.	4 de noviembre de 2020
Portal de autoservicio	Puede activar un portal de autoservicio en el punto de enlace de Client VPN para sus clientes.	29 de octubre de 2020

Acceso entre clientes	Puede permitir que los clientes utilicen un punto de enlace de Client VPN para conectarse entre sí.	29 de septiembre de 2020
Autenticación federada basada en SAML 2.0	Puede autenticar a los usuarios de Client VPN utilizando la autentica ción federada basada en SAML 2.0.	19 de mayo de 2020
Especificar grupos de seguridad durante la creación	Puede especificar una VPC y grupos de seguridad al crear el punto de conexión de Client VPN de AWS.	5 de marzo de 2020
Puertos VPN configurables	Puede especificar un número de puerto de VPN compatibl e con el punto de conexión de Client VPN de AWS.	16 de enero de 2020
Compatibilidad con Multi-Fac tor Authentication (MFA)	Su punto de conexión de Client VPN de AWS es compatible con MFA si está habilitado para su Active Directory.	30 de septiembre de 2019
Compatibilidad con la división de túneles	Puede habilitar un túnel dividido en el punto de conexión de Client VPN de AWS.	24 de julio de 2019
Versión inicial	Esta versión presenta AWS Client VPN.	18 de diciembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.