Guía del usuario

AWS Client VPN

AWS Client VPN: Guía del usuario

Table of Contents

¿Qué es AWS Client VPN?

AWS Client VPN es un servicio de VPN administrado basado en el cliente que le permite acceder con seguridad a los recursos de AWS y de la red en las instalaciones.

En esta guía, encontrará los pasos necesarios para establecer una conexión de VPN con un punto de enlace de Client VPN utilizando una aplicación cliente del dispositivo.

Componentes

Estos son los componentes clave que se utilizan con AWS Client VPN.

- Punto de enlace de Client VPN: el administrador de Client VPN crea y configura un punto de enlace de Client VPN en AWS. Su administrador controla a qué redes y recursos puede obtener acceso al establecer una conexión de VPN.
- Aplicación cliente de VPN: es la aplicación de software que va a utilizar para conectarse al punto de enlace de Client VPN y establecer una conexión de VPN segura.
- Archivo de configuración del punto de enlace de Client VPN: es el archivo de configuración que tiene que proporcionarle el administrador de Client VPN. Este archivo contiene información sobre del punto de enlace de Client VPN y los certificados necesarios para establecer una conexión de VPN. Cargue este archivo en la aplicación cliente de VPN que haya elegido.

Recursos adicionales

Si es el administrador de Client VPN, consulte la Guía del administrador de AWS Client VPN para obtener más información acerca de cómo crear y configurar un punto de enlace de Client VPN.

Introducción a Client VPN

Para poder establecer una sesión de VPN, el administrador de Client VPN debe crear y configurar un punto de enlace de Client VPN. Su administrador controla a qué redes y recursos puede obtener acceso al establecer una sesión de VPN. Puede utilizar una aplicación cliente de VPN para conectarse a un punto de enlace de Client VPN y establecer una conexión de VPN segura.

Si es un administrador que necesita crear un punto de enlace de Client VPN, consulte la Guía del administrador de AWS Client VPN.

Temas

Prerequisites

Para establecer una conexión de VPN, debe disponer de lo siguiente:

- Acceso a Internet
- Un dispositivo compatible
- En el caso de los puntos de enlace de Client VPN que utilizan la autenticación federada basada en SAML (inicio de sesión único), uno de los navegadores siguientes:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Paso 1: Obtener una aplicación cliente de VPN

Puede conectarse a un punto de enlace de Client VPN y establecer una conexión de VPN mediante el cliente proporcionado por AWS u otra aplicación cliente basada en OpenVPN.

El cliente proporcionado por AWS es compatible con Windows, macOS, Ubuntu 18.04 LTS y Ubuntu 20.04 LTS. Puede descargar el cliente en AWS Client VPN download.

También puede descargar e instalar una aplicación cliente de OpenVPN en el dispositivo desde el que vaya a establecer la conexión de VPN.

Paso 2: Obtener el archivo de configuración del punto de enlace de Client VPN

El administrador debe proporcionarle el archivo de configuración del punto de enlace de Client VPN. Este archivo de configuración contiene información sobre el punto de enlace de Client VPN y los certificados que son necesarios para establecer una conexión de VPN.

Como alternativa, si el administrador de Client VPN ha configurado un portal de autoservicio para el punto de enlace de Client VPN, puede descargar usted mismo la versión más reciente del cliente proporcionado por AWS y del archivo de configuración del punto de enlace de Client VPN. Para obtener más información, consulte Uso del portal de autoservicio.

Paso 3: Conectarse a la VPN

Importe el archivo de configuración del punto de enlace de Client VPN al cliente proporcionado por AWS o a la aplicación cliente de OpenVPN y conéctese a la VPN. Para informarse de los pasos para conectarse a una VPN, consulte los siguientes temas:

- Conexión mediante un cliente proporcionado por AWS
- Conexión mediante un cliente de OpenVPN

En los puntos de enlace de Client VPN que usan la autenticación de Active Directory, se le pedirá que escriba el nombre de usuario y la contraseña. Si se ha habilitado la Multi-Factor Authentication (MFA) para el directorio, también se le pedirá que escriba el código MFA.

En el caso de los puntos de enlace de Client VPN que utilizan la autenticación federada basada en SAML (inicio de sesión único), el cliente proporcionado por AWS abrirá una ventana del navegador en el equipo. En esta ventana, deberá escribir las credenciales corporativas para poder conectarse al punto de enlace de Client VPN.

Uso del portal de autoservicio

El administrador del punto de enlace de Client VPN puede configurar un portal de autoservicio en este punto de enlace. El portal de autoservicio es una página web que le permite descargar la versión más reciente del cliente proporcionado por AWS y del archivo de configuración del punto de enlace de Client VPN. Para obtener más información acerca de la configuración del portal de autoservicio, consulte Puntos de enlace de Client VPN en la Guía del administrador de AWS Client VPN.

Antes de comenzar, debe tener el ID del punto de enlace de Client VPN. El administrador del punto de enlace de Client VPN puede proporcionarle el ID o darle una URL del portal de autoservicio que incluya el ID.

Para acceder al portal de autoservicio

1. Vaya al portal de autoservicio en https://self-service.clientvpn.amazonaws.com/ o utilice la URL que le proporcionó el administrador.
2. Si es necesario, especifique el ID del punto de enlace de Client VPN; por ejemplo, `cvpn-endpoint-0123456abcd123456`. Elija Next (Siguiente).
3. Escriba el nombre de usuario y la contraseña y elija Sign in (Iniciar sesión). El nombre de usuario y la contraseña son los mismos que utiliza para conectarse al punto de enlace de Client VPN.
4. En el portal de autoservicio, puede hacer lo siguiente:

   - Descargar la versión más reciente del archivo de configuración del cliente del punto de enlace de Client VPN.
   - Descargar la versión más reciente del cliente proporcionado por AWS para su plataforma.

Conexión mediante un cliente proporcionado por AWS

Puede conectarse a un punto de enlace de Client VPN mediante el cliente proporcionado por AWS. El cliente proporcionado por AWS es compatible con Windows, macOS, Ubuntu 18.04 LTS y Ubuntu 20.04 LTS.

Clientes

- AWS Client VPN para Windows
- AWS Client VPN para macOS
- AWS Client VPN para Linux

Directivas de OpenVPN

El cliente proporcionado por AWS admite las siguientes directivas de OpenVPN:

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- cliente
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- inactive

- keepalive
- key
- nobind
- persist-key
- persist-tun
- ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- ruta
- route-ipv6
- server-poll-timeout
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN para Windows

El siguiente procedimiento muestra cómo establecer una conexión VPN mediante el cliente AWS proporcionado para Windows. Visite AWS Client VPN download para descargar e instalar el cliente. El cliente AWS proporcionado no admite actualizaciones automáticas.

Contenido

Requisitos

Para usar el cliente AWS proporcionado para Windows, se requiere lo siguiente:

- Sistema operativo Windows 10 de 64 bits, procesador x64
- .NET Framework 4.7.2 o superior

El cliente reserva el puerto TCP 8096 de su equipo. En los puntos de enlace de Client VPN que usan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva el puerto TCP 35001.

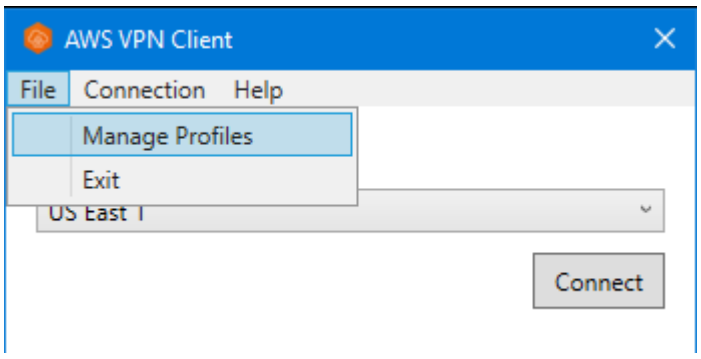
Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Conexión

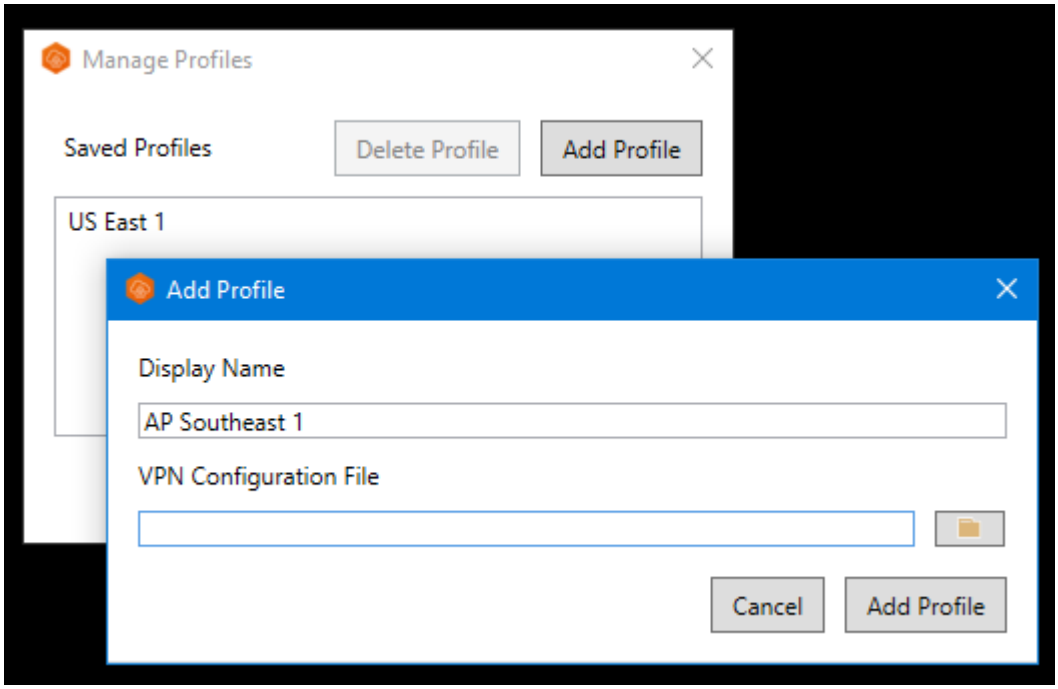
Antes de comenzar, tiene que haber leído los requisitos. El cliente AWS proporcionado también se denomina AWS VPN Cliente en los siguientes pasos.

Para conectarse mediante el cliente AWS proporcionado para Windows

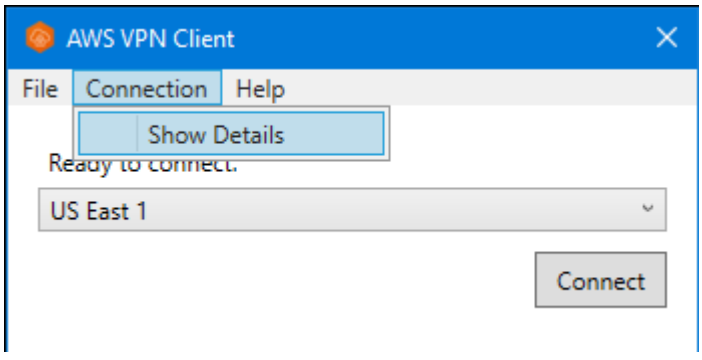
1. Abra la aplicación AWS VPN Client.
2. Seleccione File (Archivo), Manage Profiles (Administrar perfiles).



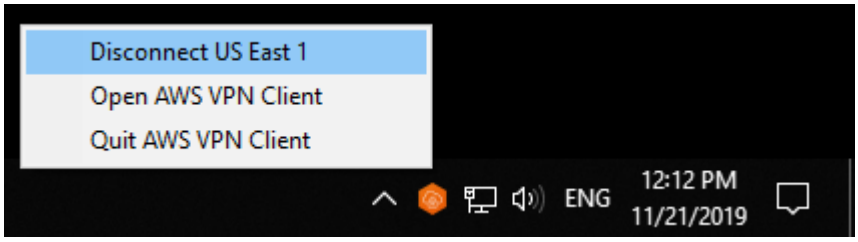
3. Seleccione Add Profile (Agregar perfil).



4. En Display name (Nombre de visualización), escriba un nombre para el perfil.
5. En VPN Configuration File (Archivo de configuración de VPN), busque y seleccione el archivo de configuración que le proporcionó el administrador de Client VPN y elija Add Profile (Agregar perfil).
6. En la ventana AWS VPN Client, compruebe que su perfil esté seleccionado y, a continuación, elija Connect (Conectar). Si el punto de enlace de Client VPN está configurado para que utilice la autenticación basada en credenciales, se le pedirá que escriba un nombre de usuario y una contraseña.
7. Para ver las estadísticas de la conexión, elija Connection (Conexión), Show Details (Mostrar detalles).



8. Para desconectarse, en la ventana AWS VPN Client, seleccione Disconnect (Desconectar). También puede elegir el icono de cliente en la barra de tareas de Windows y luego elegir Disconnect (Desconectar).



Notas de la versión

La siguiente tabla contiene las notas de la versión y los enlaces de descarga de la versión actual y anterior AWS Client VPN de Windows.

> **Note**
>
> Seguimos proporcionando correcciones de usabilidad y seguridad en cada versión. Te recomendamos encarecidamente que utilices la última versión para todas las plataformas. Las versiones anteriores pueden verse afectadas por problemas de usabilidad o seguridad; consulta las notas de la versión para obtener más información.

Versión	Cambios	Date	Enlace de descarga y SHA256
3.12.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local. • Se eliminó el enfoque automático de las aplicaciones cuando se conectaban a puntos finales SAML.	21 de mayo de 2024	Descargar la versión 3.12.0 sha256: fae30c27694a320b86c67e45043435c50c42753bddfdcc9b0112389ea881fba4
3.11.2	• Se ha resuelto un problema de autenticación SAML con los navegador	11 de abril de 2024	Descargue la versión 3.11.2

Versión	Cambios	Date	Enlace de descarga y SHA256
	es basados en Chromium desde la versión 123.		sha256:8b a258dd15b ea3e861ad ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc
3.1.1	• Se ha corregido una acción de desbordamiento del búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Posición de seguridad mejorada.	16 de febrero de 2024	Descargue la versión 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Se ha corregido un problema de conectividad provocado por las máquinas virtuales de Windows. • Se han corregido los problemas de conectividad para algunas configura ciones de LAN. • Se ha mejorado la conectividad.	6 de diciembre de 2023	Descargar la versión 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Versión	Cambios	Date	Enlace de descarga y SHA256
3.10.0	• Se ha corregido un problema de conectividad cuando NAT64 está habilitado en la red de cliente. • Se ha corregido un problema de conectividad que se producía cuando se instalaban adaptadores de red Hyper-V en el equipo cliente. • Pequeñas correcciones de errores y mejoras.	24 de agosto de 2023	Descargar la versión 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	• Posición de seguridad mejorada.	3 de agosto de 2023	Descargar la versión 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	• Posición de seguridad mejorada.	15 de julio de 2023	Ya no es compatible
3.7.0	• Se han revertido los cambios de la versión 3.6.0.	15 de julio de 2023	Ya no es compatible
3.6.0	• Posición de seguridad mejorada.	14 de julio de 2023	Ya no es compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
3.5.0	Pequeñas correcciones de errores y mejoras.	3 de abril de 2023	Ya no es compatible
3.4.0	Se han revertido los cambios de la versión 3.3.0.	28 de marzo de 2023	Ya no es compatible
3.3.0	Pequeñas correcciones de errores y mejoras.	17 de marzo de 2023	Ya no es compatible
3.2.0	• Se ha agregado soporte para el indicador de OpenVPN «verify-x509-name». • Se detecta automáticamente cuando las versiones actualizadas del cliente están disponibles. • Se ha agregado la posibilidad de instalar automáticamente nuevas versiones de cliente cuando estén disponibles.	23 de enero de 2023	Ya no es compatible
3.1.0	Posición de seguridad mejorada.	23 de mayo de 2022	Ya no es compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
3.0.0	• Se agregó compatibilidad con Windows 11. • Se corrigió el nombre del controlador TAP de Windows que hacía que otros nombres de controladores se viesen afectados. • Se corrigió el mensaje de banner que no se mostraba al utilizar la autentica ción federada. • Se corrigió la visualización del texto del banner para el texto más largo. • Posición de seguridad mejorada.	3 de marzo de 2022	Ya no es compatibl e
2.0.0	• Se ha agregado soporte para texto de banner después de establecer una nueva conexión. • Se ha eliminado la capacidad de utilizar el filtro pull-filter en relación con el echo., por ejemplo pull-filter * echo • Pequeñas correcciones de errores y mejoras.	20 de enero de 2022	Ya no es compatibl e
1.3.7	• En algunos casos, se ha corregido el intento de conexión de autenticación federada. • Pequeñas correcciones de errores y mejoras.	8 de noviembre de 2021	Ya no es compatibl e

Versión	Cambios	Date	Enlace de descarga y SHA256
1.3.6	• Se agregó soporte para los indicadores de OpenVPN: dev-type connect-retry-max, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Pequeñas correcciones de errores y mejoras.	20 de septiembre de 2021	Ya no es compatible
1.3.5	Parche para eliminar archivos de registros de Windows grandes.	16 de agosto de 2021	Ya no es compatible
1.3.4	• Soporte agregado para el indicador OpenVPN: dhcp-option. • Pequeñas correcciones de errores y mejoras.	4 de agosto de 2021	Ya no es compatible
1.3.3	• Se agregó compatibilidad con marcadores de OpenVPN: inactive, pull-filter, route. • Se corrigió un problema que provocaba que la aplicación se bloqueara al desconectarse o al salir. • Se corrigió un problema con los nombres de usuario de Active Directory con barra invertida. • Se corrigió el bloqueo de la aplicación en el momento de manipular la lista de perfiles fuera de la aplicación. • Pequeñas correcciones de errores y mejoras.	1 de julio de 2021	Ya no es compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
1.3.2	• Agregue la prevención de fugas IPv6, cuando esté configurado. • Se ha corregido un posible bloqueo al utilizar la opción Mostrar detalles en Conexión.	12 de mayo de 2021	Ya no es compatible
1.3.1	• Se agregó compatibilidad para varios certificados del cliente con el mismo asunto. Los certificados caducados se ignorarán. • Se corrigió la retención de registros locales para reducir el uso de disco. • Se agregó compatibilidad con la directiva route-ipv6 de OpenVPN. • Pequeñas correcciones de errores y mejoras.	5 de abril de 2021	Ya no es compatible
1.3.0	Se agregaron características de soporte, como informes de errores, envío de registros de diagnóstico y análisis.	8 de marzo de 2021	Ya no es compatible
1.2.7	• Se agregó compatibilidad con la directiva cryptoapicert de OpenVPN. • Se corrigieron las rutas obsoletas entre conexiones. • Pequeñas correcciones de errores y mejoras.	25 de febrero de 2021	Ya no es compatible
1.2.6	Pequeñas correcciones de errores y mejoras.	26 de octubre de 2020	Ya no es compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
1.2.5	• Se agregó compatibilidad con comentarios en la configuración de OpenVPN. • Se agregó un mensaje de error para los errores de protocolo de enlace TLS.	8 de octubre de 2020	Ya no es compatible
1.2.4	Pequeñas correcciones de errores y mejoras.	1 de septiembre de 2020	Ya no es compatible
1.2.3	Deshacer cambios en la versión 1.2.2.	20 de agosto de 2020	Ya no es compatible
1.2.1	Pequeñas correcciones de errores y mejoras.	1 de julio de 2020	Ya no es compatible
1.2.0	• Se incorporó la compatibilidad con la autenticación federada basada en SAML 2.0. • Compatibilidad obsoleta con la plataforma de Windows 7.	19 de mayo de 2020	Ya no es compatible
1.1.1	Pequeñas correcciones de errores y mejoras.	21 de abril de 2020	Ya no es compatible
1.1.0	• Se agregó compatibilidad con la funcionalidad eco de desafío estático de OpenVPN para ocultar o mostrar el texto que aparece en la interfaz de usuario. • Pequeñas correcciones de errores y mejoras.	9 de marzo de 2020	Ya no es compatible
1.0.0	La versión inicial.	4 de febrero de 2020	Ya no es compatible

AWS Client VPN para macOS

El siguiente procedimiento muestra cómo establecer una conexión VPN mediante el cliente AWS proporcionado para macOS. Visite AWS Client VPN download para descargar e instalar el cliente. El cliente AWS proporcionado no admite actualizaciones automáticas.

Contenido

Requisitos

Para usar el cliente AWS proporcionado para macOS, se requiere lo siguiente:

- macOS Monterey (12.0), Ventura (13.0) o Sonoma (14.0).
- Compatible con el procesador x86_64.
- El cliente reserva el puerto TCP 8096 de su equipo.
- En los puntos de enlace de Client VPN que usan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva el puerto TCP 35001.

> **Note**
>
> Si utilizas un Mac con un procesador de silicio de Apple, necesitarás instalar Rosetta 2 para ejecutar el software cliente. Para obtener más información, consulte Acerca del entorno de traducción de Rosetta en el sitio web de Apple.

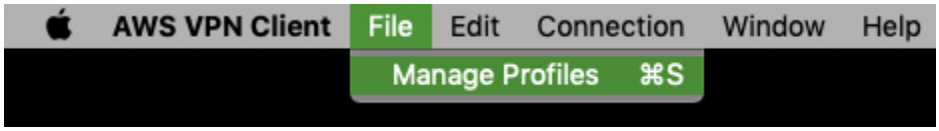
Conexión

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

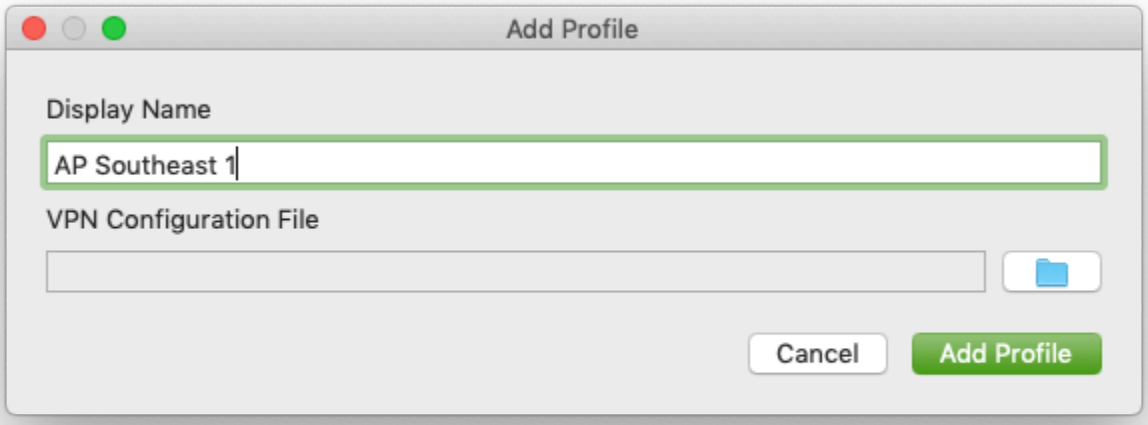
Asegúrese también de haber leído los requisitos. El cliente AWS proporcionado también se denomina AWS VPN Cliente en los siguientes pasos.

Para conectarse mediante el cliente AWS suministrado para macOS

1. Abra la aplicación AWS VPN Client.
2. Seleccione File (Archivo), Manage Profiles (Administrar perfiles).

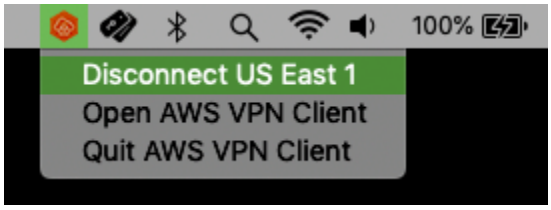


3. Seleccione Add Profile (Agregar perfil).
4. En Display name (Nombre de visualización), escriba un nombre para el perfil.



5. En VPN Configuration File (Archivo de configuración de VPN), busque el archivo de configuración que le proporcionó el administrador de Client VPN. Elija Open.
6. Seleccione Add Profile (Agregar perfil).
7. En la ventana AWS VPN Client, compruebe que su perfil esté seleccionado y, a continuación, elija Connect (Conectar). Si el punto de enlace de Client VPN está configurado para que utilice la autenticación basada en credenciales, se le pedirá que escriba un nombre de usuario y una contraseña.
8. Para ver las estadísticas de la conexión, elija Connection (Conexión), Show Details (Mostrar detalles).

9. Para desconectarse, en la ventana AWS VPN Client, seleccione Disconnect (Desconectar). También puede elegir el icono de cliente en la barra de menús y luego elegir Disconnect (Desconectar) <su-nombre-de-perfil>.



Notas de la versión

La siguiente tabla contiene las notas de la versión y los enlaces de descarga de las versiones actuales y anteriores AWS Client VPN de macOS.

> **Note**
>
> Seguimos proporcionando correcciones de usabilidad y seguridad en cada versión. Te recomendamos encarecidamente que utilices la última versión para todas las plataformas. Las versiones anteriores pueden verse afectadas por problemas de usabilidad o seguridad; consulta las notas de la versión para obtener más información.

Versión	Cambios	Fecha	Enlace de descarga
3.10.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local. • Se ha corregido un problema de restauración del DNS durante el cambio de red. • Se eliminó el enfoque automático de las aplicaciones cuando se conectaban a puntos finales SAML.	21 de mayo de 2024	Descargar la versión 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3.9.2	• Se ha resuelto un problema de autenticación SAML con los navegador	11 de abril de 2024	Descargue la versión 3.9.2

Versión	Cambios	Fecha	Enlace de descarga
	es basados en Chromium desde la versión 123. • Se agregó soporte para macOS Sonoma. Soporte obsoleto para macOS Big Sur. • Posición de seguridad mejorada.		sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480
3.9.1	• Se ha corregido una acción de desbordamiento del búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Se corrigió la barra de progreso de descarga de la actualización de la aplicación • Posición de seguridad mejorada.	16 de febrero de 2024	Descarga la versión 3.9.1 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e899e971
3.9.0	• Se han corregido los problemas de conectividad para algunas configura ciones de LAN. • Se ha mejorado la conectividad.	6 de diciembre de 2023	Descargar la versión 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8

Versión	Cambios	Fecha	Enlace de descarga
3.8.0	• Se ha corregido un problema de conectividad cuando se habilitaba NAT64 en la red de cliente. • Pequeñas correcciones de errores y mejoras.	24 de agosto de 2023	Descargar la versión 3.8.0 sha256: d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• Posición de seguridad mejorada.	3 de agosto de 2023	Descargar la versión 3.7.0 sha256: 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a
3.6.0	• Posición de seguridad mejorada.	15 de julio de 2023	Ya no es compatible
3.5.0	• Se han revertido los cambios de la versión 3.4.0.	15 de julio de 2023	Ya no es compatible
3.4.0	• Posición de seguridad mejorada.	14 de julio de 2023	Ya no es compatible

Versión	Cambios	Fecha	Enlace de descarga
3.3.0	• Se ha agregado compatibilidad con macOS Ventura (13.0). • Pequeñas correcciones de errores y mejoras.	27 de abril de 2023	Ya no es compatible
3.2.0	• Se ha agregado soporte para el indicador de OpenVPN «verify-x509-name». • Se detecta automáticamente cuando las versiones actualizadas del cliente están disponibles. • Se ha agregado la posibilidad de instalar automáticamente nuevas versiones de cliente cuando estén disponibles.	23 de enero de 2023	Ya no es compatible
3.1.0	• Se ha agregado compatibilidad con macOS Monterey. • Se ha corregido un problema de detección del tipo de unidad. • Posición de seguridad mejorada.	23 de mayo de 2022	Ya no es compatible
3.0.0	• Se corrigió el mensaje de banner que no se mostraba al utilizar la autenticación federada. • Se corrigió la visualización del texto del banner para el texto más largo. • Posición de seguridad mejorada.	3 de marzo de 2022	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
2.0.0	• Se ha agregado soporte para texto de banner después de establecer una nueva conexión. • Se ha eliminado la capacidad de utilizar el filtro pull-filter en relación con el echo., por ejemplo pull-filter * echo • Pequeñas correcciones de errores y mejoras.	20 de enero de 2022	Ya no es compatible.
1.4.0	• Se ha agregado el monitoreo del servidor DNS durante la conexión. La configuración se volverá a ajustar si no coincide con la configuración de VPN. • En algunos casos, se ha corregido el intento de conexión de autenticación federada. • Pequeñas correcciones de errores y mejoras.	9 de noviembre de 2021	Ya no es compatible.
1.3.5	• Se agregó soporte para los indicadores de OpenVPN: dev-type connect-retry-max, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Pequeñas correcciones de errores y mejoras.	20 de septiembre de 2021	Ya no es compatible.
1.3.4	• Soporte agregado para el indicador OpenVPN: dhcp-option. • Pequeñas correcciones de errores y mejoras.	4 de agosto de 2021	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
1.3.3	• Se agregó compatibilidad con marcadores de OpenVPN: inactive, pull-filter, route. • Se corrigió un problema con los nombres de archivo de configuración con espacios o Unicode. • Se corrigió un problema que provocaba que la aplicación se bloqueara al desconectarse o al salir. • Se corrigió un problema con los nombres de usuario de Active Directory con barra invertida. • Se corrigió el bloqueo de la aplicación en el momento de manipular la lista de perfiles fuera de la aplicación. • Pequeñas correcciones de errores y mejoras.	1 de julio de 2021	Ya no es compatible.
1.3.2	• Agregue la prevención de fugas IPv6, cuando esté configurado. • Se ha corregido un posible bloqueo al utilizar la opción Mostrar detalles en Conexión. • Agregue la rotación del registro de daemon.	12 de mayo de 2021	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
1.3.1	• Se agregó compatibilidad con macOS Big Sur (10.16). • Se corrigió el problema que eliminaba la configuración de DNS establecida por otras aplicaciones. • Se corrigió el problema que ocurría cuando se utilizaba un certificado no válido para la autenticación mutua, lo que causaba problemas de conectividad. • Se agregó compatibilidad con la directiva route-ipv6 de OpenVPN. • Pequeñas correcciones de errores y mejoras.	5 de abril de 2021	Ya no es compatible.
1.3.0	Se agregaron características de soporte, como informes de errores, envío de registros de diagnóstico y análisis.	8 de marzo de 2021	Ya no es compatible.
1.2.5	Pequeñas correcciones de errores y mejoras.	25 de febrero de 2021	Ya no es compatible.
1.2.4	Pequeñas correcciones de errores y mejoras.	26 de octubre de 2020	Ya no es compatible.
1.2.3	• Se agregó compatibilidad con comentarios en la configuración de OpenVPN. • Se agregó un mensaje de error para los errores de protocolo de enlace TLS. • Se corrigió un error de desinstalación que afectaba a algunos usuarios.	8 de octubre de 2020	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
1.2.2	Pequeñas correcciones de errores y mejoras.	12 de agosto de 2020	Ya no es compatible.
1.2.1	• Se incluyó soporte para desinstalar la aplicación. • Pequeñas correcciones de errores y mejoras.	1 de julio de 2020	Ya no es compatible.
1.2.0	• Se agregó la compatibilidad con la autenticación federada basada en SAML 2.0. • Se agregó compatibilidad con macOS Catalina (10.15).	19 de mayo de 2020	Ya no es compatible.
1.1.2	Pequeñas correcciones de errores y mejoras.	21 de abril de 2020	Ya no es compatible.
1.1.1	• Se corrigió un problema que impedía que el DNS se resolviera. • Se corrigió un problema que bloqueaba la aplicación y que era causado por conexiones más largas. • Se corrigió un problema de MFA.	2 de abril de 2020	Ya no es compatible.
1.1.0	• Se incluyó compatibilidad con la configuración de DNS de macOS. • Se agregó compatibilidad con la funcionalidad eco de desafío estático de OpenVPN para ocultar o mostrar el texto que aparece en la interfaz de usuario. • Pequeñas correcciones de errores y mejoras.	9 de marzo de 2020	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
1.0.0	La versión inicial.	4 de febrero de 2020	Ya no es compatible.

AWS Client VPN para Linux

Los siguientes procedimientos muestran cómo instalar el cliente AWS proporcionado para Linux y cómo establecer una conexión VPN mediante el cliente AWS proporcionado. El cliente AWS proporcionado para Linux no admite las actualizaciones automáticas.

Contenido

Requisitos

Para usar el cliente AWS proporcionado para Linux, se requiere lo siguiente:

- Ubuntu 18.04 LTS o Ubuntu 20.04 LTS (solo AMD64)

El cliente reserva el puerto TCP 8096 de su equipo. En los puntos de enlace de Client VPN que usan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva el puerto TCP 35001.

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Instalación

Existen varios métodos que se pueden utilizar para instalar el cliente AWS proporcionado para Linux. Utilice uno de los métodos proporcionados en las siguientes opciones. Antes de comenzar, tiene que haber leído los requisitos.

Opción 1: Instalar a través del repositorio de paquetes

1. Agregue la clave pública de AWS Client VPN a su sistema operativo Ubuntu.

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. Utilice el comando correspondiente para agregar el repositorio al sistema operativo Ubuntu, en función de su versión de Ubuntu:

   Ubuntu 18.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

   Ubuntu 20.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

3. Utilice el siguiente comando para actualizar los repositorios en el sistema.

```
sudo apt-get update
```

4. Use el siguiente comando para instalar el cliente AWS proporcionado para Linux.

```
sudo apt-get install awsvpnclient
```

Opción 2: Instalar mediante el archivo de paquete .deb

1. Descargue el archivo .deb desde AWS Client VPN download o mediante el siguiente comando.

```
curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
 awsvpnclient_amd64.deb
```

2. Instale el cliente AWS suministrado para Linux mediante la `dpkg` utilidad.

```
sudo dpkg -i awsvpnclient_amd64.deb
```

Opción 3: Instalar el paquete .deb a través del Centro de software de Ubuntu

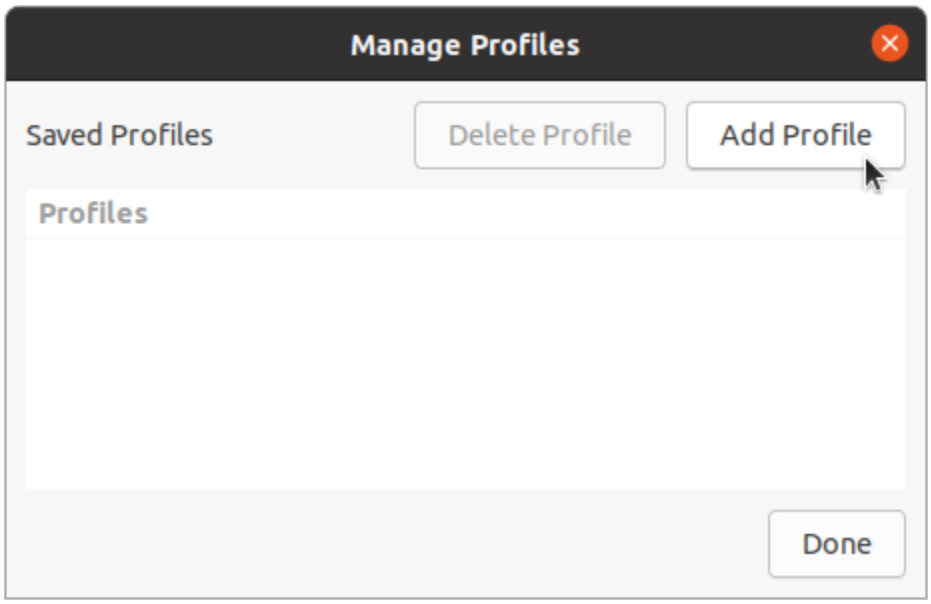
1. Descargue el archivo del paquete .deb desde AWS Client VPN download.
2. Luego de descargar el archivo del paquete .deb, utilice el Centro de software de Ubuntu para instalar el paquete. Siga los pasos que se detallan en Ubuntu Wiki para instalar un paquete .deb independiente a través del Centro de software de Ubuntu.

Conexión

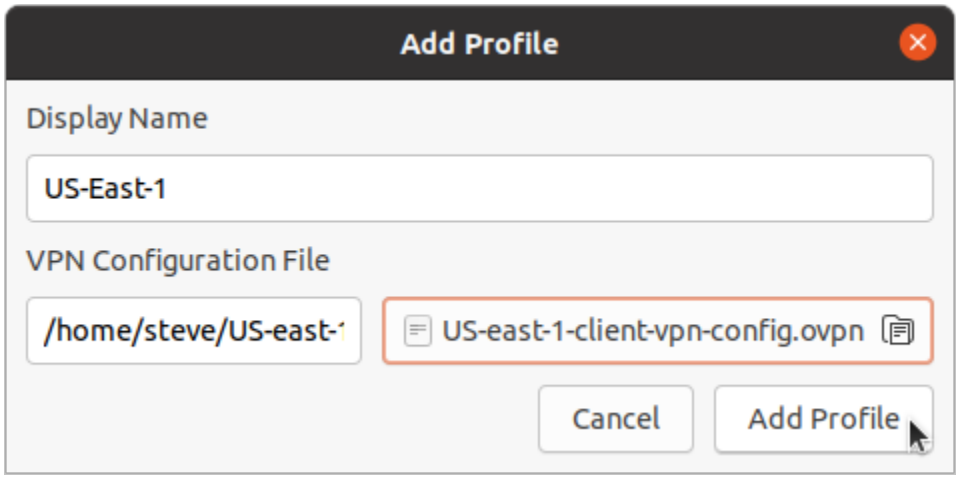
El cliente AWS proporcionado también se denomina AWS VPN Cliente en los siguientes pasos.

Para conectarse mediante el cliente AWS proporcionado para Linux

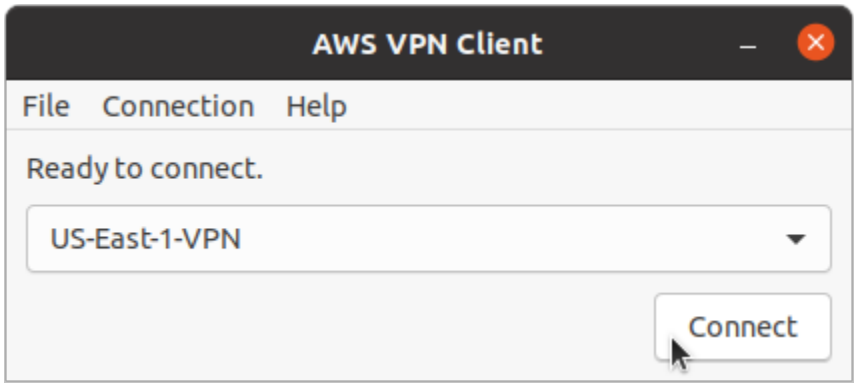
1. Abra la aplicación AWS VPN Client.
2. Seleccione File (Archivo), Manage Profiles (Administrar perfiles).
3. Seleccione Add Profile (Agregar perfil).



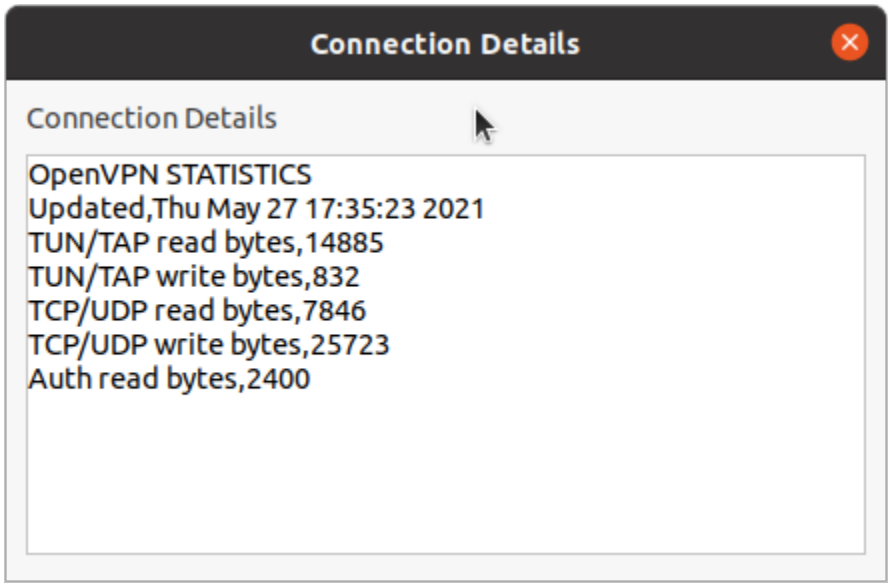
4. En Display name (Nombre de visualización), escriba un nombre para el perfil.
5. En VPN Configuration File (Archivo de configuración de VPN), busque el archivo de configuración que le proporcionó el administrador de Client VPN. Elija Open.
6. Seleccione Add Profile (Agregar perfil).



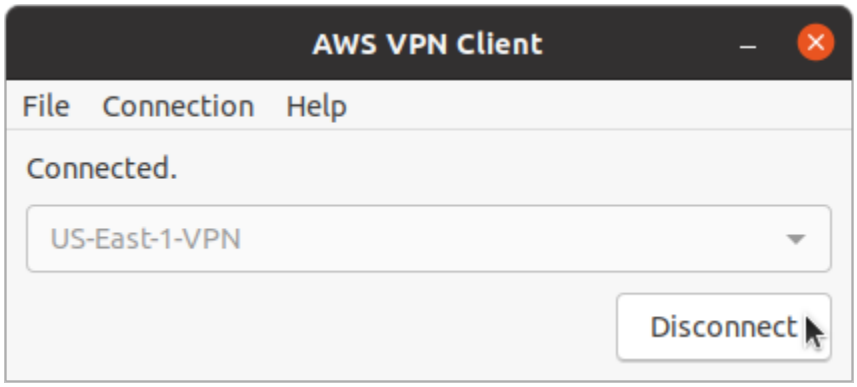
7. En la ventana AWS VPN Client, compruebe que su perfil esté seleccionado y, a continuación, elija Connect (Conectar). Si el punto de enlace de Client VPN está configurado para que utilice la autenticación basada en credenciales, se le pedirá que escriba un nombre de usuario y una contraseña.



8. Para ver las estadísticas de la conexión, elija Connection (Conexión), Show Details (Mostrar detalles).



9. Para desconectarse, en la ventana AWS VPN Client, seleccione Disconnect (Desconectar).



Notas de la versión

La siguiente tabla contiene las notas de la versión y los enlaces de descarga de las versiones actuales y anteriores AWS Client VPN de Linux.

> **Note**
>
> Seguimos proporcionando correcciones de usabilidad y seguridad en cada versión. Te recomendamos encarecidamente que utilices la última versión para todas las plataformas. Las versiones anteriores pueden verse afectadas por problemas de usabilidad o seguridad; consulta las notas de la versión para obtener más información.

Versión	Cambios	Fecha	Enlace de descarga
3.13.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local.	21 de mayo de 2024	Descargue la versión 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1
3.12.2	• Se ha resuelto un problema de autenticación SAML con los navegador es basados en Chromium desde la versión 123.	11 de abril de 2024	Descargue la versión 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	• Se ha corregido una acción de desbordamiento del búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Posición de seguridad mejorada.	16 de febrero de 2024	Descargue la versión 3.12.1 sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0
3.12.0	• Se han corregido los problemas de conectividad para algunas configura ciones de LAN.	19 de diciembre de 2023	Descargar la versión 3.12.0

Versión	Cambios	Fecha	Enlace de descarga
			sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Reversión para “Se han corregido los problemas de conectividad para algunas configuraciones de LAN”. • Se ha mejorado la conectividad.	6 de diciembre de 2023	Descargar la versión 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• Se han corregido los problemas de conectividad para algunas configura ciones de LAN. • Se ha mejorado la conectividad.	6 de diciembre de 2023	Descargar la versión 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51

Versión	Cambios	Fecha	Enlace de descarga
3.9.0	• Se ha corregido un problema de conectividad cuando se habilitaba NAT64 en la red de cliente. • Pequeñas correcciones de errores y mejoras.	24 de agosto de 2023	Descargar la versión 3.9.0 sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454
3.8.0	• Posición de seguridad mejorada.	3 de agosto de 2023	Descargar la versión 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• Posición de seguridad mejorada.	15 de julio de 2023	Ya no es compatible
3.6.0	• Se han revertido los cambios de la versión 3.5.0.	15 de julio de 2023	Ya no es compatible
3.5.0	• Posición de seguridad mejorada.	14 de julio de 2023	Ya no es compatible
3.4.0	• Se ha agregado soporte para el indicador de OpenVPN «verify-x509-name».	14 de febrero de 2023	Ya no es compatible

Versión	Cambios	Fecha	Enlace de descarga
3.1.0	• Se ha corregido un problema de detección del tipo de unidad. • Posición de seguridad mejorada.	23 de mayo de 2022	Ya no es compatible
3.0.0	• Se corrigió el mensaje de banner que no se mostraba al utilizar la autenticación federada. • Se corrigió la visualización del texto del banner para texto más largo y secuencias de caracteres específicas. • Posición de seguridad mejorada.	3 de marzo de 2022	Ya no es compatible.
2.0.0	• Se ha agregado soporte para texto de banner después de establecer una nueva conexión. • Se ha eliminado la capacidad de utilizar el filtro pull-filter en relación con el echo., por ejemplo pull-filter * echo • Pequeñas correcciones de errores y mejoras.	20 de enero de 2022	Ya no es compatible.
1.0.3	• En algunos casos, se ha corregido el intento de conexión de autenticación federada. • Pequeñas correcciones de errores y mejoras.	8 de noviembre de 2021	Ya no es compatible.
1.0.2	• Se agregó soporte para los indicadores de OpenVPN: dev-type connect-retry-max, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Pequeñas correcciones de errores y mejoras.	28 de septiembre de 2021	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
1.0.1	• Opción habilitada para salir de la barra de aplicaciones de Ubuntu. • Se agregó compatibilidad con marcadores de OpenVPN: inactive, pull-filter, route. • Pequeñas correcciones de errores y mejoras.	4 de agosto de 2021	Ya no es compatible.
1.0.0	La versión inicial.	11 de junio de 2021	Ya no es compatible.

Conexión mediante un cliente de OpenVPN

Puede conectarse a un punto de enlace de Client VPN mediante aplicaciones cliente de OpenVPN comunes.

> **Important**
>
> Si el punto de enlace de Client VPN se configuró para utilizar la autenticación federada basada en SAML, no puede usar el cliente de VPN basado en OpenVPN para conectarse a un punto de enlace de Client VPN.

Aplicaciones cliente

- Conectar mediante una aplicación cliente de Windows
- Conectarse con Client VPN mediante una aplicación de Android o iOS
- Conectar mediante una aplicación cliente de macOS
- Conexión mediante una aplicación cliente de OpenVPN

Conectar mediante una aplicación cliente de Windows

Los siguientes procedimientos muestran cómo establecer una conexión de VPN utilizando clientes de VPN basados en Windows.

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de Windows.

> **Important**
>
> Si el punto de enlace de Client VPN se configuró para utilizar la autenticación federada basada en SAML, no puede usar el cliente de VPN basado en OpenVPN para conectarse a un punto de enlace de Client VPN.

Puede usar OpenVPN mediante un certificado del Almacén del sistema de certificados de Windows

Puede configurar el cliente de OpenVPN para que use un certificado y una clave privada desde el Almacén del sistema de certificados de Windows. Esta opción resulta útil cuando utiliza una tarjeta inteligente como parte de la conexión de Client VPN. Para obtener más información acerca de la opción cryptoapicert del cliente de OpenVPN, consulte el Manual de referencia para OpenVPN en el sitio web de OpenVPN.

> **Note**
>
> El certificado debe almacenarse en el equipo local.

Para utilizar la opción cryptoapicert con OpenVPN

1. Cree un archivo .pfx que contenga el certificado del cliente y la clave privada.
2. Importe el archivo .pfx a su almacén de certificados personal en el equipo local. Para obtener más información, consulte Cómo ver certificados con el complemento MMC en el sitio web de Microsoft.
3. Compruebe que su cuenta tenga permisos para leer el certificado del equipo local. Puede utilizar la consola de administración de Microsoft para modificar los permisos. Para obtener más información, consulte Derechos para ver el almacén de certificados de equipo local en el sitio web de Microsoft Technet.
4. Actualice el archivo de configuración de OpenVPN y especifíquelo mediante el asunto o la huella digital del certificado.

   A continuación se muestra un ejemplo de cómo especificar el certificado mediante un asunto.

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   A continuación se muestra un ejemplo de cómo especificar el certificado mediante una huella digital. Puede encontrar la huella digital en la consola de administración de Microsoft. Para obtener más información, consulte Cómo recuperar la huella digital de un certificado en el sitio web de Microsoft Technet.

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```

Después de completar la configuración, utilice OpenVPN para establecer una conexión.

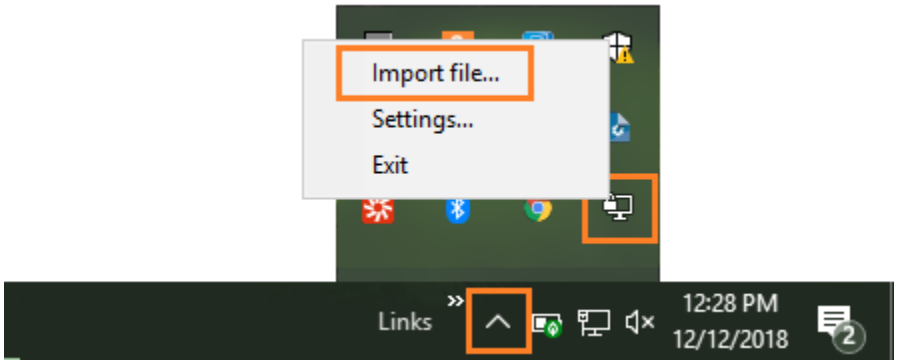
Interfaz gráfica de usuario de OpenVPN

El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación cliente de la interfaz gráfica de usuario de OpenVPN en un equipo Windows.

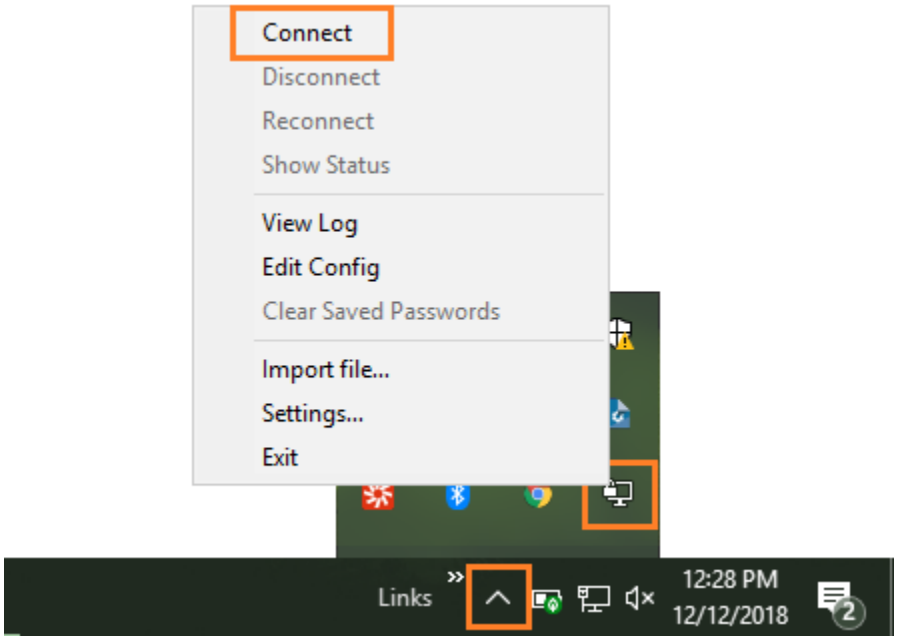
> **Note**
>
> Para obtener información acerca de la aplicación cliente de OpenVPN, consulte la sección de descargas de la comunidad en el sitio web de OpenVPN.

Para establecer una conexión de VPN

1. Inicie la aplicación cliente de OpenVPN.
2. En la barra de tareas de Windows, seleccione Show/Hide icons (Mostrar/ocultar iconos), haga clic con el botón derecho en OpenVPN GUI (GUI de OpenVPN) y elija Import file (Importar archivo).



3. En el cuadro de diálogo Open (Abrir), seleccione el archivo de configuración que le proporcionó su administrador de Client VPN y elija Open (Abrir).
4. En la barra de tareas de Windows, seleccione Show/Hide icons (Mostrar/ocultar iconos), haga clic con el botón derecho en OpenVPN GUI (GUI de OpenVPN) y elija Connect (Conectar).



OpenVPN Connect Client

El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación OpenVPN Connect Client en un equipo Windows.

> **Note**
>
> Para obtener más información, consulte la página sobre conexión al servidor de acceso con Windows en el sitio web de OpenVPN.

Para establecer una conexión de VPN

1. Inicie la aplicación OpenVPN Connect Client.
2. En la barra de tareas de Windows, haga clic en Show/Hide icons (Mostrar/ocultar iconos), haga clic con el botón derecho en OpenVPN y elija Import profile (Importar perfil).
3. Elija Import from File (Importar desde archivo) y seleccione el archivo de configuración que le proporcionó el administrador de Client VPN.
4. Elija el perfil de conexión para iniciar la conexión.

Conectarse con Client VPN mediante una aplicación de Android o iOS

> **Important**
>
> Si el punto de enlace de Client VPN se configuró para utilizar la autenticación federada basada en SAML, no puede usar el cliente de VPN basado en OpenVPN para conectarse a un punto de enlace de Client VPN.

La siguiente información muestra cómo establecer una conexión de VPN mediante la aplicación cliente de OpenVPN en un dispositivo móvil Android o iOS. Los pasos para Android e iOS son los mismos.

> **Note**
>
> Para obtener más información sobre la descarga y el uso de la aplicación cliente OpenVPN para iOS o Android, consulte la Guía del usuario de OpenVPN Connect en el sitio web de OpenVPN.

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Inicie la aplicación cliente de OpenVPN e importe el archivo que recibió del administrador de Client VPN para establecer la conexión.

Conectar mediante una aplicación cliente de macOS

Los siguientes procedimientos muestran cómo establecer una conexión de VPN utilizando clientes de VPN basados en macOS.

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de MacOS.

Important

Si el punto de enlace de Client VPN se configuró para utilizar la autenticación federada basada en SAML, no puede usar el cliente de VPN basado en OpenVPN para conectarse a un punto de enlace de Client VPN.

Tunnelblick

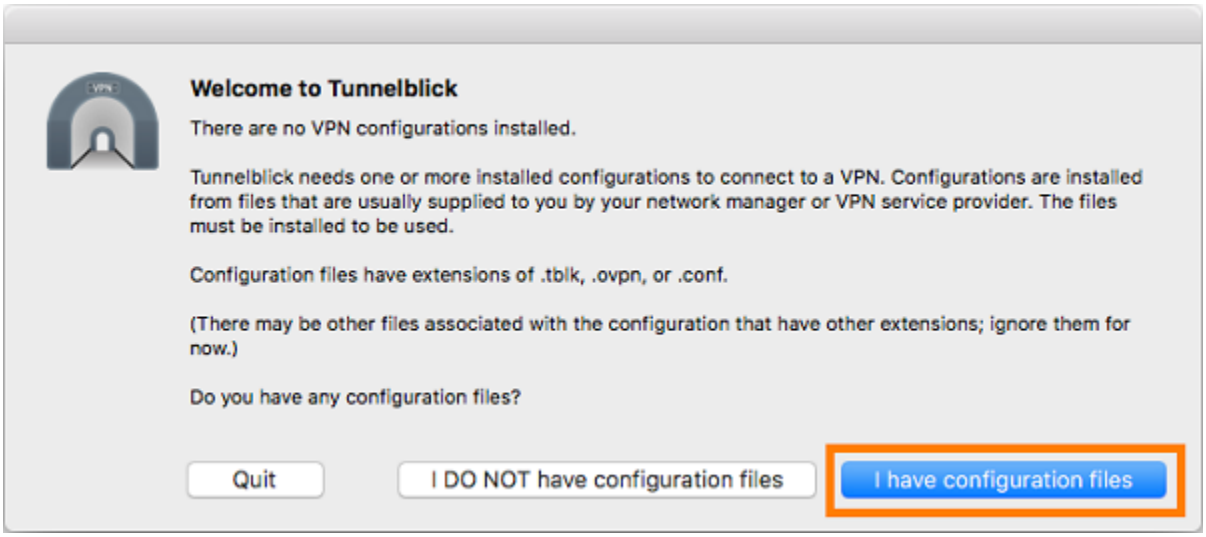
El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación cliente Tunnelblick en un equipo MacOS.

Note

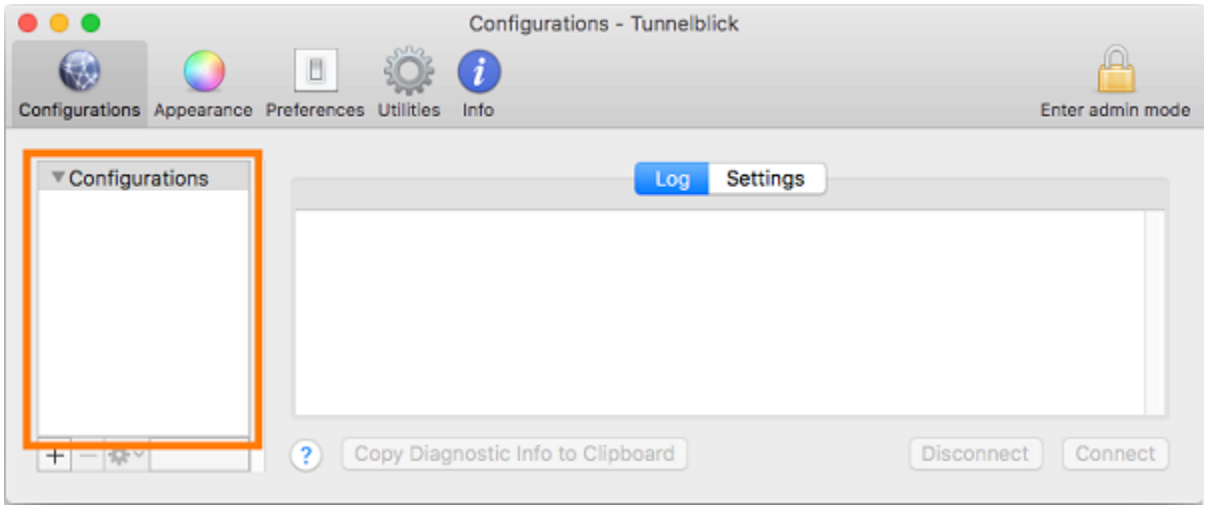
Para obtener más información acerca de la aplicación cliente Tunnelblick para MacOS, consulte la documentación de Tunnelblick en el sitio web de Tunnelblick.

Para establecer una conexión de VPN

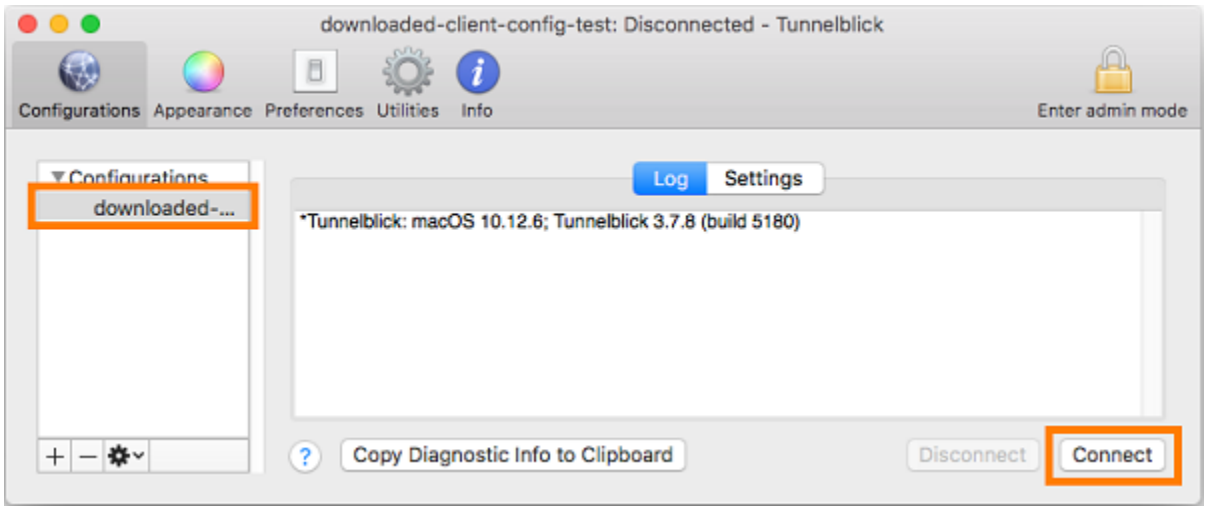
1. Inicie la aplicación cliente Tunnelblick y elija I have configuration files (Tengo los archivos de configuración).



2. Arrastre y suelte el archivo de configuración que le ha entregado su administrador de VPN en el panel Configurations (Configuraciones).



3. Seleccione el archivo de configuración en el panel Configurations (Configuraciones) y elija Connect (Conectar).



OpenVPN Connect Client

El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación OpenVPN Connect Client en un equipo macOS.

> **Note**
>
> Para obtener más información, consulte la página sobre conexión al servidor de acceso con macOS en el sitio web de OpenVPN.

Para establecer una conexión de VPN

1. Inicie la aplicación OpenVPN y elija Import (Importar) y From local file… (Desde archivo local…).
2. Desplácese hasta el archivo de configuración que recibió del administrador de VPN y elija Open (Abrir).

Conexión mediante una aplicación cliente de OpenVPN

Los siguientes procedimientos muestran cómo establecer una conexión de VPN mediante clientes de VPN basados en OpenVPN.

Antes de comenzar, asegúrese de que el administrador de Client VPN ha creado un punto de enlace de Client VPN y le ha proporcionado el archivo de configuración del punto de enlace de Client VPN.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de Linux.

> **Important**
>
> Si el punto de enlace de Client VPN se configuró para utilizar la autenticación federada basada en SAML, no puede usar el cliente de VPN basado en OpenVPN para conectarse a un punto de enlace de Client VPN.

OpenVPN: administrador de red

El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación OpenVPN a través de la interfaz gráfica de usuario del administrador de red en un equipo Ubuntu.

Para establecer una conexión de VPN

1. Instale el módulo del administrador de red mediante el siguiente comando.

   ```
   sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
   ```

2. Vaya a Settings (Configuración), Network (Red).
3. Elija el símbolo más (+) junto a VPN y, a continuación, elija Import from file... (Importar desde archivo...).

4. Desplácese hasta el archivo de configuración que recibió del administrador de VPN y elija Open (Abrir).
5. En la ventana Add VPN (Añadir VPN), seleccione Add (Añadir).
6. Inicie la conexión habilitando la opción que está junto al perfil de VPN que añadió.

OpenVPN

El siguiente procedimiento muestra cómo establecer una conexión de VPN mediante la aplicación OpenVPN en un equipo Windows.

Para establecer una conexión de VPN

1. Instale OpenVPN utilizando el siguiente comando.

```
sudo apt-get install openvpn
```

2. Para iniciar la conexión, cargue el archivo de configuración que recibió del administrador de VPN.

```
sudo openvpn --config /path/to/config/file
```

Solución de problemas de la conexión de Client VPN

Consulte los temas siguientes para solucionar problemas que puedan surgir al usar una aplicación cliente para conectarse a un punto de enlace de Client VPN.

Temas

Solución de problemas con los puntos de enlace de Client VPN para administradores

Usted mismo puede realizar algunos de los pasos de esta guía, El administrador de VPN de cliente debe realizar otros pasos en el propio punto de enlace de Client VPN. En las siguientes secciones encontrará información sobre cuándo tiene que ponerse en contacto con el administrador.

Para obtener más información acerca de cómo solucionar los problemas de los puntos de enlace de Client VPN, consulte Solución de problemas de Client VPN en la Guía del administrador de AWS Client VPN .

Envíe los registros AWS Support de diagnóstico al cliente AWS proporcionado

Si tiene problemas con el cliente AWS proporcionado y necesita ponerse en contacto con él para que le ayuden AWS Support a resolverlo, el cliente tiene la opción de enviar los registros de diagnóstico. AWS Support La opción está disponible en las aplicaciones cliente de Windows, macOS y Linux.

Antes de enviar los archivos, debe aceptar permitir el acceso AWS Support a sus registros de diagnóstico. Una vez que esté de acuerdo, le proporcionaremos un número de referencia al AWS Support que podrá dar acceso inmediato a los archivos.

Envío de registros de diagnóstico

El cliente AWS proporcionado también se denomina AWS VPN Cliente en los siguientes pasos.

Para enviar registros de diagnóstico mediante el cliente AWS proporcionado para Windows

1. Abra la aplicación AWS VPN Client.
2. Elija Help (Ayudar), Send Diagnostic Logs (Enviar registros de diagnóstico).
3. En la ventana Send Diagnostic Logs (Enviar registros de diagnóstico), elija Yes (Sí).
4. En la ventana Send Diagnostic Logs (Enviar registros de diagnóstico), realice una de las siguientes operaciones:

   - Para copiar el número de referencia en el portapapeles, elija Yes (Sí) y, a continuación, elija OK (Aceptar).
   - Para realizar un seguimiento manual del número de referencia, elija No (No).

   Cuando te pongas en contacto con ellos AWS Support, tendrás que proporcionarles el número de referencia.

Para enviar registros de diagnóstico mediante el cliente AWS proporcionado para macOS

1. Abra la aplicación AWS VPN Client.
2. Elija Help (Ayudar), Send Diagnostic Logs (Enviar registros de diagnóstico).
3. En la ventana Send Diagnostic Logs (Enviar registros de diagnóstico), elija Yes (Sí).
4. Anote el número de referencia de la ventana de confirmación y luego elija OK (De acuerdo).

   Cuando te pongas en contacto con ellos AWS Support, tendrás que proporcionarles el número de referencia.

Para enviar registros de diagnóstico mediante el cliente AWS proporcionado para Ubuntu

1. Abra la aplicación AWS VPN Client.
2. Elija Help (Ayudar), Send Diagnostic Logs (Enviar registros de diagnóstico).
3. En la ventana Send Diagnostic Logs (Enviar registros de diagnóstico), elija Send (Enviar).
4. Anote el número de referencia de la ventana de confirmación. Tiene la opción de copiar la información en su portapapeles si así lo desea.

Cuando te pongas en contacto con ellos AWS Support, tendrás que proporcionarles el número de referencia.

Solución de problemas de Windows

En las siguientes secciones, se incluye información sobre algunos problemas que pueden surgir al utilizar clientes basados en Windows para conectarse a un punto de enlace de Client VPN.

Temas

AWS cliente proporcionado

AWS cliente proporcionado

El cliente AWS proporcionado crea registros de eventos y los almacena en la siguiente ubicación de su ordenador.

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

Dispone de los siguientes tipos de registros:

- Registros de aplicación: contienen información sobre la aplicación. Estos registros tienen el prefijo 'aws_vpn_client_'.
- Registros de OpenVPN: contienen información sobre los procesos de OpenVPN. Estos registros tienen el prefijo 'ovpn_aws_vpn_client_'.

El cliente AWS proporcionado utiliza el servicio de Windows para realizar operaciones de root. Los registros de servicio de Windows se almacenan en la siguiente ubicación del equipo.

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

Temas

El cliente no puede establecer conexión

Problema

El cliente AWS proporcionado no puede conectarse al punto final Client VPN.

Causa

Este problema podría deberse a una de las siguientes causas:

- Ya hay otro proceso de OpenVPN ejecutándose en el equipo, lo que impide que el cliente establezca conexión.
- El archivo de configuración (.ovpn) no es válido.

Solución

Verifique que no haya otras aplicaciones de OpenVPN que se estén ejecutando en su equipo. En caso de haberlas, detenga o cierre estos procesos e intente volver a establecer conexión con el punto de enlace de Client VPN. Compruebe si hay errores en los registros de OpenVPN y pida al administrador de Client VPN que verifique la siguiente información:

- El archivo de configuración debe contener el certificado y la clave de cliente correctos. Para obtener más información, consulte Exportar la configuración de un cliente en la Guía del administrador de AWS Client VPN .
- La CRL debe seguir siendo válida. Para obtener más información, consulte la sección sobre el error Los clientes no pueden conectarse a un punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

El cliente no se puede conectar con el mensaje de registro “no hay adaptadores TAP-Windows”

Problema

El cliente AWS proporcionado no puede conectarse al punto final Client VPN y aparece el siguiente mensaje de error en los registros de la aplicación: «No hay adaptadores TAP-Windows en este sistema. Debería poder crear un adaptador TAP-Windows yendo a Inicio -> Todos los programas -> TAP-Windows -> Utilidades -> Agregar un nuevo adaptador Ethernet virtual TAP-Windows”.

Solución

Puede solucionar este problema realizando una o más de las siguientes acciones:

- Reinicie el adaptador TAP-Windows.
- Vuelva a instalar el controlador TAP-Windows.
- Cree un nuevo adaptador TAP-Windows.

El cliente está atascado en un estado de reconexión

Problema

El cliente AWS proporcionado está intentando conectarse al punto final Client VPN, pero está atrapado en un estado de reconexión.

Causa

Este problema podría deberse a una de las siguientes causas:

- Su equipo no está conectado a Internet.
- El nombre de host de DNS no se resuelve en una dirección IP.
- Un proceso de OpenVPN está intentando conectarse indefinidamente al punto de enlace.

Solución

Compruebe que el equipo esté conectado a Internet. Pida al administrador de Client VPN que compruebe que la directiva `remote` del archivo de configuración se resuelva en una dirección IP válida. También puede desconectar la sesión de VPN seleccionando Desconectar en la ventana del cliente AWS VPN e intentar conectarse de nuevo.

El proceso de conexión de la VPN se cierra inesperadamente

Problema

Al conectarse a un punto de enlace de Client VPN, el cliente se cierra inesperadamente.

Causa

TAP-Windows no está instalado en el equipo. Este software tiene que estar instalado para poder ejecutar el cliente.

Solución

Vuelva a ejecutar el instalador de cliente AWS proporcionado para instalar todas las dependencias necesarias.

La aplicación no se inicia

Problema

En Windows 7, el cliente AWS proporcionado no se inicia al intentar abrirlo.

Causa

.NET Framework 4.7.2 o superior no está instalado en el equipo. Es necesario que esté instalado para poder ejecutar el cliente.

Solución

Vuelva a ejecutar el instalador del cliente AWS proporcionado para instalar todas las dependencias necesarias.

El cliente no puede crear el perfil

Problema

Cuando intenta crear un perfil con el cliente proporcionado por AWS , aparece el siguiente mensaje de error.

```
The config should have either cert and key or auth-user-pass specified.
```

Causa

Si el punto de enlace de Client VPN utiliza la autenticación mutua, el archivo de configuración (.ovpn) no contiene el certificado y la clave del cliente.

Solución

Asegúrese de que el administrador de Client VPN agregue la clave y el certificado de cliente al archivo de configuración. Para obtener más información, consulte Exportar la configuración de un cliente en la Guía del administrador de AWS Client VPN .

Se produce un fallo del cliente en las computadoras Dell que utilizan Windows 10 u 11

Problema

En algunas computadoras Dell (de escritorio y portátiles) que ejecutan Windows 10 u 11, puede producirse un fallo al navegar por el sistema de archivos para importar un archivo de configuración VPN. Si se produce este problema, verás mensajes como los siguientes en los registros del cliente AWS proporcionado:

```
System.AccessViolationException: Attempted to read or write protected memory. This is
 often an indication that other memory is corrupt.
   at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
 Int32 flags, IntPtr& db)
   at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
 connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
   at System.Data.SQLite.SQLiteConnection.Open()
   at
 STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
 newConnection)
   at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
 targetSettings)
   at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

Causa

El sistema de Backup and Recovery de Dell en Windows 10 y 11 puede provocar conflictos con el cliente AWS proporcionado, especialmente con las tres DLL siguientes:

- DBR .dll ShellExtension
- OverlayIconDBR Backuped.dll
- DBR .dll OverlayIcon NotBackuped

Solución

Para evitar este problema, primero asegúrese de que su cliente esté actualizado con la última versión del cliente AWS proporcionado. Vaya a la descarga de AWS Client VPN y, si hay una versión más reciente, actualícela.

Lleve a cabo también alguna de las siguientes operaciones:

- Si utiliza la aplicación Dell Backup and Recovery, asegúrese de que esté actualizada. Una publicación en el foro de Dell indica que este problema se ha resuelto en versiones más recientes de la aplicación.
- Si no está utilizando la aplicación Dell Backup and Recovery, seguirá siendo necesario tomar algunas medidas si experimenta este problema. Si no desea actualizar la aplicación, como alternativa, puede eliminar o cambiar el nombre de los archivos DLL. Sin embargo, tenga en cuenta que esto impedirá que la aplicación Dell Backup and Recovery funcione por completo.

Eliminar o cambiar el nombre de los archivos DLL

1. Vaya al Explorador de Windows y navegue hasta la ubicación en la que esté instalada Dell Backup and Recovery. Normalmente se instala en la siguiente ubicación, pero es posible que tenga que buscar para encontrarla.

   ```
   C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
   ```

2. Elimine manualmente los siguientes archivos DLL del directorio de instalación o cámbieles el nombre. Cualquiera de estas acciones impedirá que se carguen.

   - DBR .dll ShellExtension
   - OverlayIconDBR Backuped.dll
   - DBR .dll OverlayIcon NotBackuped

   Puede cambiar el nombre de los archivos añadiendo «.bak» al final del nombre del archivo, por ejemplo, DBR Backuped.dll.bak. OverlayIcon

La VPN se desconecta con un mensaje emergente

Problema

La VPN se desconecta y aparece un mensaje emergente que dice: «La conexión VPN se interrumpe porque ha cambiado el espacio de direcciones de la red local a la que está conectado el dispositivo. Establezca una nueva conexión VPN».

Causa

El adaptador TAP-Windows no contiene la descripción requerida.

Solución

Si el `Description` campo que aparece a continuación no coincide, quite primero el adaptador TAP-Windows y, a continuación, vuelva a ejecutar el instalador de cliente AWS proporcionado para instalar todas las dependencias necesarias.

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Interfaz gráfica de usuario de OpenVPN

La siguiente información de solución de problemas se ha probado en las versiones 11.10.0.0 y 11.11.0.0 del software OpenVPN GUI en Windows 10 Home (64 bits) y Windows Server 2016 (64 bits).

El archivo de configuración se almacena en la siguiente ubicación del equipo.

```
C:\Users\User\OpenVPN\config
```

Los registros de conexión se almacenan en la siguiente ubicación del equipo.

```
C:\Users\User\OpenVPN\log
```

Cliente de conexión de OpenVPN

La siguiente información de solución de problemas se ha probado en las versiones 2.6.0.100 y 2.7.1.101 del software OpenVPN Connect Client en Windows 10 Home (64 bits) y Windows Server 2016 (64 bits).

El archivo de configuración se almacena en la siguiente ubicación del equipo.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

Los registros de conexión se almacenan en la siguiente ubicación del equipo.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

No se puede resolver el DNS

Problema

La conexión falla con el siguiente error.

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

Causa

No se puede resolver el nombre de DNS. El cliente debe prefijar una cadena aleatoria al nombre de DNS para evitar el almacenamiento en caché del DNS; sin embargo, algunos clientes no lo hacen.

Solución

Consulte la solución del problema No se puede resolver el nombre de DNS del punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

Falta el alias PKI

Problema

Se produce en siguiente error en una conexión con un punto de enlace de Client VPN que no utiliza la autenticación mutua.

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

Causa

El software de OpenVPN Connect Client tiene el siguiente problema conocido: intenta autenticarse mediante autenticación mutua, pero si el archivo de configuración no contiene una clave ni un certificado de cliente, la autenticación falla.

Solución

Especifique un certificado y una clave de cliente aleatoria en el archivo de configuración de Client VPN e importe la nueva configuración en el software OpenVPN Connect Client. También tiene la opción de utilizar otro cliente, como el cliente OpenVPN GUI (v11.12.0.0) o el cliente Viscosity (v.1.7.14).

Solución de problemas de MacOS

En las siguientes secciones, se incluye información sobre el registro y los problemas que pueden surgir al utilizar los clientes de macOS. Asegúrese de que esté ejecutando la versión más reciente de estos clientes.

Temas

- AWS cliente proporcionado
- Tunnelblick
- OpenVPN

AWS cliente proporcionado

El cliente AWS proporcionado crea registros de eventos y los almacena en la siguiente ubicación de su ordenador.

```
/Users/username/.config/AWSVPNClient/logs
```

Dispone de los siguientes tipos de registros:

- Registros de aplicación: contienen información sobre la aplicación. Estos registros tienen el prefijo 'aws_vpn_client_'.

- Registros de OpenVPN: contienen información sobre los procesos de OpenVPN. Estos registros tienen el prefijo 'ovpn_aws_vpn_client_'.

El cliente AWS proporcionado utiliza el daemon del cliente para realizar las operaciones raíz. Los registros de demonio se almacenan en la siguiente ubicación del equipo.

```
/tmp/AcvcHelperErrLog.txt
/tmp/AcvcHelperOutLog.txt
```

El cliente AWS proporcionado almacena los archivos de configuración en la siguiente ubicación de su ordenador.

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

Temas

El cliente no puede establecer conexión

Problema

El cliente AWS proporcionado no puede conectarse al punto final Client VPN.

Causa

Este problema podría deberse a una de las siguientes causas:

- Ya hay otro proceso de OpenVPN ejecutándose en el equipo, lo que impide que el cliente establezca conexión.
- El archivo de configuración (.ovpn) no es válido.

Solución

Verifique que no haya otras aplicaciones de OpenVPN que se estén ejecutando en su equipo. En caso de haberlas, detenga o cierre estos procesos e intente volver a establecer conexión con el

punto de enlace de Client VPN. Compruebe si hay errores en los registros de OpenVPN y pida al administrador de Client VPN que verifique la siguiente información:

- El archivo de configuración debe contener el certificado y la clave de cliente correctos. Para obtener más información, consulte Exportar la configuración de un cliente en la Guía del administrador de AWS Client VPN .
- La CRL debe seguir siendo válida. Para obtener más información, consulte la sección sobre el error Los clientes no pueden conectarse a un punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

El cliente está atascado en un estado de reconexión

Problema

El cliente AWS proporcionado está intentando conectarse al punto final Client VPN, pero está atrapado en un estado de reconexión.

Causa

Este problema podría deberse a una de las siguientes causas:

- Su equipo no está conectado a Internet.
- El nombre de host de DNS no se resuelve en una dirección IP.
- Un proceso de OpenVPN está intentando conectarse indefinidamente al punto de enlace.

Solución

Compruebe que el equipo esté conectado a Internet. Pida al administrador de Client VPN que compruebe que la directiva `remote` del archivo de configuración se resuelva en una dirección IP válida. También puede desconectar la sesión de VPN seleccionando Desconectar en la ventana del cliente AWS VPN e intentar conectarse de nuevo.

El cliente no puede crear el perfil

Problema

Cuando intenta crear un perfil con el cliente proporcionado por AWS , aparece el siguiente mensaje de error.

```
The config should have either cert and key or auth-user-pass specified.
```

Causa

Si el punto de enlace de Client VPN utiliza la autenticación mutua, el archivo de configuración (.ovpn) no contiene el certificado y la clave del cliente.

Solución

Asegúrese de que el administrador de Client VPN agregue la clave y el certificado de cliente al archivo de configuración. Para obtener más información, consulte Exportar la configuración de un cliente en la Guía del administrador de AWS Client VPN .

Se necesita una herramienta de ayuda (error)

Problema

Aparece el siguiente error al intentar conectar la VPN.

```
AWS VPN Client Helper Tool is required to establish the connection.
```

Solución

Consulta el siguiente artículo en AWS Re:post. Cliente VPN de AWS: error necesario para utilizar la herramienta de ayuda

Tunnelblick

La siguiente información de solución de problemas se ha probado en la versión 3.7.8 (compilación 5180) del software Tunnelblick en macOS High Sierra 10.13.6.

El archivo de configuración para configuraciones privadas se almacena en la siguiente ubicación del equipo.

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

El archivo de configuración para configuraciones compartidas se almacena en la siguiente ubicación del equipo.

```
/Library/Application Support/Tunnelblick/Shared
```

Los registros de conexión se almacenan en la siguiente ubicación del equipo.

```
/Library/Application Support/Tunnelblick/Logs
```

Para aumentar la verbosidad del registro, abra la aplicación Tunnelblick, elija Settings (Configuración) y ajuste el valor de VPN log level (Nivel de registro de VPN).

Algoritmo de cifrado 'AES-256-GCM' no encontrado

Problema

La conexión falla y devuelve el siguiente error en los registros.

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

Causa

La aplicación usa una versión de OpenVPN que no da soporte al algoritmo de cifrado AES-256-GCM.

Solución

Elija una versión compatible de OpenVPN; para ello, haga lo siguiente:

1. Abra la aplicación Tunnelblick.
2. Elija Configuración.
3. Para la OpenVPN versión (Versión de OpenVPN), elija 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - La versión de OpenSSL es v1.0.2q).

La conexión deja de responder y se restablece

Problema

La conexión falla y devuelve el siguiente error en los registros.

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
```

```
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

Causa

El certificado de cliente ha sido revocado. La conexión deja de responder después de intentar autenticarse y finalmente se restablece desde el lado del servidor.

Solución

Solicite al administrador de Client VPN un archivo de configuración.

Uso extendido de claves (EKU)

Problema

La conexión falla y devuelve el siguiente error en los registros.

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

Causa

La autenticación del servidor se ha realizado correctamente, pero la autenticación del cliente genera un error porque el certificado de cliente tiene habilitado el campo de uso de la clave extendida (EKU) para la autenticación del servidor.

Solución

Compruebe que esté utilizando un certificado y una clave de cliente correctos. Si es necesario, verifíquelo con el administrador de Client VPN. Es posible que este error se produzca si utiliza el certificado de servidor en lugar del certificado de cliente para conectarse al punto de enlace de Client VPN.

Certificado caducado

Problema

La autenticación del servidor se realiza correctamente, pero la autenticación del cliente genera el siguiente error.

```
WARNING: “Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
 process restarting”
```

Causa

La validez del certificado de cliente ha caducado.

Solución

Solicite un nuevo certificado de cliente al administrador de Client VPN.

OpenVPN

La siguiente información de solución de problemas se ha probado en la versión 2.7.1.100 del software OpenVPN Connect Client en macOS High Sierra 10.13.6.

El archivo de configuración se almacena en la siguiente ubicación del equipo.

```
/Library/Application Support/OpenVPN/profile
```

Los registros de conexión se almacenan en la siguiente ubicación del equipo.

```
Library/Application Support/OpenVPN/log/connection_name.log
```

No se puede resolver el DNS

Problema

La conexión falla con el siguiente error.

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

Causa

OpenVPN Connect no puede resolver el nombre de DNS de Client VPN.

Solución

Consulte la solución del problema No se puede resolver el nombre de DNS del punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

Solución de problemas de Linux

En las siguientes secciones, se incluye información sobre el registro y los problemas que pueden surgir al utilizar los clientes basados en Linux Asegúrese de que esté ejecutando la versión más reciente de estos clientes.

Temas

- AWS cliente proporcionado
- OpenVPN (línea de comandos)
- OpenVPN a través de Network Manager (GUI)

AWS cliente proporcionado

El cliente AWS proporcionado almacena los archivos de registro y de configuración en la siguiente ubicación del sistema:

```
/home/username/.config/AWSVPNClient/
```

El proceso daemon del cliente AWS proporcionado almacena los archivos de registro en la siguiente ubicación del sistema:

```
/var/log/aws-vpn-client/username/
```

Problema

En algunas circunstancias, después de establecer una conexión de VPN, las consultas de DNS seguirán dirigiéndose al servidor de nombres del sistema predeterminado, en lugar de hacerlo al servidor de nombres configurados para el punto de enlace de Client VPN.

Causa

El cliente interactúa con systemd-resolved, un servicio que está disponible en sistemas Linux, que sirve como pieza central de administración de DNS. Se utiliza para configurar servidores de DNS que se envían desde el punto de enlace de Client VPN. El problema se produce porque systemd-resolved no establece la máxima prioridad para los servidores de DNS que proporciona el punto de enlace de Client VPN. En su lugar, adjunta los servidores a la lista existente de servidores de DNS que se han configurado en el sistema local. En consecuencia, es posible que los servidores de DNS originales sigan teniendo la máxima prioridad y, por lo tanto, se utilicen para solucionar las consultas de DNS.

Solución

1. Agregue la siguiente directiva en la primera línea del archivo de configuración de OpenVPN para asegurarse de que todas las consultas de DNS se envían al túnel de VPN.

   ```
   dhcp-option DOMAIN-ROUTE .
   ```

2. Utilice el solucionador stub que proporciona systemd-resolved. Para hacer esto, haga un enlace simbólico de `/etc/resolv.conf` a `/run/systemd/resolve/stub-resolv.conf` mediante la ejecución del siguiente comando en el sistema.

   ```
   sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
   ```

3. (Opcional) Si no desea que systemd-resolved realice las consultas de DNS por proxy y, en su lugar, desea que las consultas se envíen directamente a los servidores de nombres de DNS reales, haga un enlace simbólico de `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`.

   ```
   sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

Es posible que desee realizar este procedimiento para omitir la configuración systemd-resolved, como, por ejemplo, para el almacenamiento en caché de respuestas de DNS, la configuración de DNS por interfaz, la aplicación de DNSSec, etc. Esta opción es especialmente útil en el caso de que se necesite anular un registro de DNS público con un registro privado cuando está conectado a una VPN. Por ejemplo, puede disponer de un solucionador de DNS privado en su VPC privada con un registro para www.ejemplo.com, que se soluciona con una IP privada. Esta opción podría utilizarse para anular el registro público de www.example.com, que se soluciona con una IP pública.

OpenVPN (línea de comandos)

Problema

La conexión no funciona correctamente porque la resolución de DNS no funciona.

Causa

El servidor DNS no está configurado en el punto de enlace de Client VPN o el software cliente no lo respeta.

Solución

Siga los pasos siguientes para comprobar que el servidor DNS esté configurado y funcione correctamente.

1. Asegúrese de que haya una entrada de servidor DNS en los registros. En el ejemplo siguiente, el servidor DNS `192.168.0.2` (configurado en el punto de enlace de Client VPN) se devuelve en la última línea.

```
Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
 10.0.0.98 255.255.255.224,peer-id 0
```

   Si no se ha especificado ningún servidor DNS, solicite al administrador de Client VPN que modifique el punto de enlace de Client VPN y no olvide especificar un servidor DNS (por ejemplo, el servidor DNS de la VPC) para el punto de enlace de Client VPN. Para obtener más información, consulte Puntos de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

2. Asegúrese de que el paquete `resolvconf` esté instalado; para ello, ejecute el siguiente comando.

```
sudo apt list resolvconf
```

   La salida debe devolver lo siguiente.

```
Listing... Done
resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
```

   Si no está instalado, instálelo con el siguiente comando.

```
sudo apt install resolvconf
```

3. Abra el archivo de configuración de Client VPN (el archivo.ovpn) en un editor de texto y agregue las siguientes líneas.

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

   Compruebe los registros para comprobar que se haya invocado al script `resolvconf`. Los registros deben contener una línea similar a la siguiente.

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

OpenVPN a través de Network Manager (GUI)

Problema

Cuando se utiliza el cliente OpenVPN de Network Manager, la conexión falla con el siguiente error.

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
```

```
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

Causa

El indicador `remote-random-hostname` no se respeta y el cliente no puede establecer conexión mediante el paquete `network-manager-gnome`.

Solución

Consulte la solución del problema No se puede resolver el nombre de DNS del punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

Problemas comunes

A continuación, indicamos algunos problemas comunes que podrían surgir al utilizar un cliente para conectarse a un punto de enlace de Client VPN.

Error en la negociación de clave TLS

Problema

La negociación TLS falla con el siguiente error.

```
TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
TLS Error: TLS handshake failed
```

Causa

Este problema podría deberse a una de las siguientes causas:

- Las reglas del firewall bloquean el tráfico UDP o TCP.
- Está utilizando una clave y un certificado de cliente incorrectos en su archivo de configuración (.ovpn).
- La lista de revocación de certificados de cliente (CRL) ha caducado.

Solución

Verifique que las reglas del firewall de su equipo no bloqueen el tráfico TCP o UDP de entrada o de salida en los puertos 443 o 1194. Pida al administrador de Client VPN que verifique la siguiente información:

- Las reglas del firewall del punto de enlace de Client VPN no deben bloquear el tráfico TCP o UDP en los puertos 443 o 1194.
- El archivo de configuración debe contener el certificado y la clave de cliente correctos. Para obtener más información, consulte Exportar la configuración de un cliente en la Guía del administrador de AWS Client VPN .
- La CRL debe seguir siendo válida. Para obtener más información, consulte la sección sobre el error Los clientes no pueden conectarse a un punto de enlace de Client VPN en la Guía del administrador de AWS Client VPN .

Historial de revisión

En la siguiente tabla se describen las actualizaciones de la Guía del usuario de AWS Client VPN.

Cambio	Descripción	Fecha
AWS Publicado el cliente proporcionado (3.13.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	21 de mayo de 2024
AWS Publicado el cliente proporcionado (3.12.0) para Windows	Consulte las notas de la versión para obtener más detalles.	21 de mayo de 2024
AWS Lanzamiento del cliente proporcionado (3.10.0) para macOS	Consulte las notas de la versión para obtener más detalles.	21 de mayo de 2024
AWS Lanzamiento del cliente proporcionado (3.9.2) para macOS	Consulte las notas de la versión para obtener más detalles.	11 de abril de 2024
AWS Publicado el cliente proporcionado (3.12.2) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	11 de abril de 2024
AWS Publicado el cliente proporcionado (3.11.2) para Windows	Consulte las notas de la versión para obtener más detalles.	11 de abril de 2024
AWS Lanzamiento del cliente proporcionado (3.9.1) para macOS	Consulte las notas de la versión para obtener más detalles.	16 de febrero de 2024
AWS Publicado el cliente proporcionado (3.12.1) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	16 de febrero de 2024

AWS Publicado el cliente proporcionado (3.11.1) para Windows	Consulte las notas de la versión para obtener más detalles.	16 de febrero de 2024
AWS Publicado el cliente proporcionado (3.12.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	19 de diciembre de 2023
AWS Lanzamiento del cliente proporcionado (3.9.0) para macOS	Consulte las notas de la versión para obtener más detalles.	6 de diciembre de 2023
AWS Se lanzó el cliente proporcionado (3.11.0) para Windows	Consulte las notas de la versión para obtener más detalles.	6 de diciembre de 2023
AWS Publicado el cliente proporcionado (3.11.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	6 de diciembre de 2023
AWS Publicado el cliente proporcionado (3.10.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	6 de diciembre de 2023
AWS Publicado el cliente proporcionado (3.9.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	24 de agosto de 2023
AWS Lanzamiento del cliente proporcionado (3.8.0) para macOS	Consulte las notas de la versión para obtener más detalles.	24 de agosto de 2023
AWS Publicado el cliente proporcionado (3.10.0) para Windows	Consulte las notas de la versión para obtener más detalles.	24 de agosto de 2023
AWS Publicado el cliente proporcionado (3.9.0) para Windows	Consulte las notas de la versión para obtener más detalles.	3 de agosto de 2023

AWS Publicado el cliente proporcionado (3.8.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	3 de agosto de 2023
AWS Lanzamiento del cliente proporcionado (3.7.0) para macOS	Consulte las notas de la versión para obtener más detalles.	3 de agosto de 2023
AWS Publicado el cliente proporcionado (3.8.0) para Windows	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Publicado el cliente proporcionado (3.7.0) para Windows	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Publicado el cliente proporcionado (3.7.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Lanzamiento del cliente proporcionado (3.6.0) para macOS	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Publicado el cliente proporcionado (3.6.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Lanzamiento del cliente proporcionado (3.5.0) para macOS	Consulte las notas de la versión para obtener más detalles.	15 de julio de 2023
AWS Se lanzó el cliente proporcionado (3.6.0) para Windows	Consulte las notas de la versión para obtener más detalles.	14 de julio de 2023
AWS Publicado el cliente proporcionado (3.5.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	14 de julio de 2023

AWS Lanzamiento del cliente proporcionado (3.4.0) para macOS	Consulte las notas de la versión para obtener más detalles.	14 de julio de 2023
AWS Lanzamiento del cliente proporcionado (3.3.0) para macOS	Consulte las notas de la versión para obtener más detalles.	27 de abril de 2023
AWS Se lanzó el cliente proporcionado (3.5.0) para Windows	Consulte las notas de la versión para obtener más detalles.	3 de abril de 2023
AWS Publicado el cliente proporcionado (3.4.0) para Windows	Consulte las notas de la versión para obtener más detalles.	28 de marzo de 2023
AWS Publicado el cliente proporcionado (3.3.0) para Windows	Consulte las notas de la versión para obtener más detalles.	17 de marzo de 2023
AWS Publicado el cliente proporcionado (3.4.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	14 de febrero de 2023
AWS Lanzamiento del cliente proporcionado (3.2.0) para macOS	Consulte las notas de la versión para obtener más detalles.	23 de enero de 2023
AWS Se lanzó el cliente proporcionado (3.2.0) para Windows	Consulte las notas de la versión para obtener más detalles.	23 de enero de 2023
AWS Lanzamiento del cliente proporcionado (3.1.0) para macOS	Consulte las notas de la versión para obtener más detalles.	23 de mayo de 2022
AWS Publicado el cliente proporcionado (3.1.0) para Windows	Consulte las notas de la versión para obtener más detalles.	23 de mayo de 2022

AWS Publicado el cliente proporcionado (3.1.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	23 de mayo de 2022
AWS Lanzamiento del cliente proporcionado (3.0.0) para macOS	Consulte las notas de la versión para obtener más detalles.	3 de marzo de 2022
AWS Se lanzó el cliente proporcionado (3.0.0) para Windows	Consulte las notas de la versión para obtener más detalles.	3 de marzo de 2022
AWS Publicado el cliente proporcionado (3.0.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	3 de marzo de 2022
AWS Lanzamiento del cliente proporcionado (2.0.0) para macOS	Consulte las notas de la versión para obtener más detalles.	20 de enero de 2022
AWS Publicado el cliente proporcionado (2.0.0) para Windows	Consulte las notas de la versión para obtener más detalles.	20 de enero de 2022
AWS Publicado el cliente proporcionado (2.0.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	20 de enero de 2022
AWS Lanzamiento del cliente proporcionado (1.4.0) para macOS	Consulte las notas de la versión para obtener más detalles.	9 de noviembre de 2021
AWS publicado el cliente proporcionado para Windows (1.3.7)	Consulte las notas de la versión para obtener más detalles.	8 de noviembre de 2021
AWS Publicado el cliente proporcionado (1.0.3) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	8 de noviembre de 2021

AWS Publicado el cliente proporcionado (1.0.2) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	28 de septiembre de 2021
AWS Lanzamiento del cliente proporcionado para Windows (1.3.6) y macOS (1.3.5)	Consulte las notas de la versión para obtener más detalles.	20 de septiembre de 2021
AWS Se lanzó el cliente suministrado para Ubuntu 18.04 LTS y Ubuntu 20.04 LTS	Puede usar el cliente AWS proporcionado en Ubuntu 18.04 LTS y Ubuntu 20.04 LTS.	11 de junio de 2021
Compatibilidad con OpenVPN mediante un certificado del Almacén del sistema de certificados de Windows	Puede utilizar OpenVPN con un certificado del Almacén del sistema de certificados de Windows.	25 de febrero de 2021
Portal de autoservicio	Puede acceder a un portal de autoservicio para obtener el último AWS cliente y el archivo de configuración proporcio nados.	29 de octubre de 2020
AWS cliente proporcionado	Puede usar el cliente AWS proporcionado para conectars e a un punto final Client VPN.	4 de febrero de 2020
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.