Guía del usuario

AWS Cliente VPN

AWS Cliente VPN: Guía del usuario

Table of Contents

¿Qué es el AWS clienteVPN?

AWS Client VPN es un VPN servicio gestionado basado en clientes que le permite acceder de forma segura a AWS los recursos y recursos de su red local.

Esta guía proporciona los pasos para establecer una VPN conexión a un VPN punto final del cliente mediante una aplicación cliente en el dispositivo.

VPNComponentes del cliente

Los siguientes son los componentes clave para usar el AWS ClienteVPN.

- VPNPunto final del cliente: el VPN administrador del cliente crea y configura un VPN punto final del cliente en AWS. El administrador controla a qué redes y recursos puede acceder al establecer una VPN conexión.
- VPNaplicación cliente: la aplicación de software que se utiliza para conectarse al VPN punto final del cliente y establecer una VPN conexión segura.
- Archivo de configuración del VPN punto final del cliente: archivo de configuración que le proporciona el VPN administrador del cliente. El archivo incluye información sobre el VPN punto final del cliente y los certificados necesarios para establecer una VPN conexión. Debe cargar este archivo en la aplicación VPN cliente que elija.

Recursos adicionales para configurar el cliente VPN

Si es VPN administrador de un cliente, consulte la Guía del AWS Client VPN administrador para obtener más información sobre cómo crear y configurar un VPN punto final de cliente.

Comience con AWS Client VPN

Antes de poder establecer una VPN sesión, el VPN administrador del cliente debe crear y configurar un VPN punto final del cliente. El administrador controla a qué redes y recursos puede acceder al establecer una VPN sesión. A continuación, utilice una aplicación VPN cliente para conectarse a un VPN punto final del cliente y establecer una VPN conexión segura.

Si es un administrador y necesita crear un VPN punto final de cliente, consulte la Guía AWS Client VPN del administrador.

Temas

Requisitos previos para usar el cliente VPN

Para establecer una VPN conexión, debe tener lo siguiente:

- Acceso a Internet
- Un dispositivo compatible
- Para los VPN puntos finales del cliente que utilizan la autenticación federada SAML basada (inicio de sesión único), uno de los siguientes navegadores:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Paso 1: Obtenga una aplicación cliente VPN

Puede conectarse a un VPN punto final del cliente y establecer una VPN conexión mediante el cliente AWS proporcionado u otra aplicación cliente VPN basada en Open.

El cliente AWS proporcionado es compatible con Windows, macOS, Ubuntu 18.04 LTS y Ubuntu LTS 20.04.

Puede descargar la VPN aplicación cliente mediante uno de estos dos métodos, en función de si el administrador creó el archivo de configuración del punto final para la aplicación:

- Si su administrador no configuró el archivo de configuración del punto final, descargue e instale el cliente desde AWS Client VPN Download. Tras descargar e instalar la aplicación, solicite the section called “Paso 2: Obtenga el archivo de configuración del VPN punto final del cliente” al administrador el archivo de configuración del punto final.
- Si el administrador ya ha preconfigurado el archivo de configuración del punto final, puede descargar la VPN aplicación cliente, junto con el archivo de configuración, desde el portal de autoservicio. Para conocer los pasos para descargar el cliente y el archivo de configuración desde el portal de autoservicio, consulte. the section called “Descargue el cliente VPN” Tras descargar e instalar la aplicación y el archivo, vaya athe section called “Paso 3: Conectarse al VPN”.

Como alternativa, descargue e instale una aplicación VPN cliente de Open en el dispositivo desde el que desee establecer la VPN conexión.

Paso 2: Obtenga el archivo de configuración del VPN punto final del cliente

El administrador le proporciona el archivo de configuración del VPN punto final del cliente. El archivo de configuración incluye la información sobre el VPN punto final del cliente y los certificados necesarios para establecer una VPN conexión.

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

Paso 3: Conectarse al VPN

Importe el archivo de configuración del VPN punto final del cliente al cliente AWS proporcionado o a la aplicación Open VPN Client y conéctese alVPN. Para conocer los pasos para conectarse a un dispositivoVPN, incluida la importación del archivo de configuración del punto final, consulte los siguientes temas:

- Conectarse a un VPN punto final del cliente mediante un cliente AWS proporcionado
- Conectarse a un VPN punto final de cliente mediante un VPN cliente abierto

En el caso de VPN los terminales cliente que utilizan la autenticación de Active Directory, se le pedirá que introduzca su nombre de usuario y contraseña. Si se ha activado la autenticación multifactorial (MFA) en el directorio, también se le pedirá que introduzca MFA el código.

En el caso de VPN los terminales cliente que utilizan la autenticación federada SAML basada en el inicio de sesión único, el cliente AWS proporcionado abre una ventana del navegador en su ordenador. Se le pedirá que introduzca sus credenciales corporativas antes de poder conectarse al punto final del cliente. VPN

Descárguelo AWS Client VPN desde el portal de autoservicio

El portal de autoservicio es una página web que le permite descargar la última versión del cliente AWS proporcionado y la última versión del archivo de configuración del VPN punto final del cliente. Si el administrador del VPN punto final del cliente ha preconfigurado el archivo de configuración para el VPN cliente cliente, puede descargar e instalar esa VPN aplicación cliente junto con el archivo de configuración desde este portal.

> **Note**
>
> Si es administrador y desea configurar el portal de autoservicio, consulte los VPNpuntos finales del cliente en la Guía del AWS Client VPN administrador.

Antes de empezar, debe tener el ID del punto final del clienteVPN. El administrador del VPN punto final del cliente puede proporcionarle el ID o puede proporcionarle un portal de autoservicio URL que incluya el ID.

Para acceder al portal de autoservicio

1. Diríjase al portal de autoservicio en https://self-service.clientvpn.amazonaws.com/ o utilice el URL que le proporcionó su administrador.
2. Si es necesario, introduzca el ID del VPN punto final del cliente, por ejemplo. `cvpn-endpoint-0123456abcd123456` Elija Next (Siguiente).

3. Escriba el nombre de usuario y la contraseña y elija Sign in (Iniciar sesión). Se trata del mismo nombre de usuario y contraseña que utiliza para conectarse al VPN punto final del cliente.
4. En el portal de autoservicio, puede hacer lo siguiente:

   - Descargue la última versión del archivo de configuración del cliente para el VPN punto final del cliente.
   - Descargue la última versión del cliente AWS proporcionado para su plataforma.

Conectarse a un VPN punto final del cliente mediante un cliente AWS proporcionado

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

Clientes

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

Directivas abiertas VPN

El cliente AWS proporcionado es compatible con las siguientes VPN directivas de apertura:

- 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

En estas secciones se describe cómo establecer una VPN conexión mediante el cliente AWS proporcionado para Windows. Puede descargar e instalar el cliente en AWS Client VPN download. El cliente AWS proporcionado no admite actualizaciones automáticas.

Requisitos

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

- Windows 10 o Windows 11 (sistema operativo de 64 bits, procesador x64)
- . NETFramework 4.7.2 o superior

El cliente reserva el TCP puerto 8096 en su equipo. Para los VPN puntos finales del cliente que utilizan la autenticación federada SAML basada (inicio de sesión único), el cliente reserva el puerto 35001. TCP

Antes de empezar, asegúrese de que el VPN administrador del cliente haya creado un punto final del cliente y le haya proporcionado el archivo de configuración del VPN punto final del cliente. VPN

Temas

- Conectarse al cliente VPN con un cliente AWS proporcionado para Windows
- AWS Client VPN para notas de la versión de Windows

Conectarse al cliente VPN con un cliente AWS proporcionado para Windows

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. Para el archivo de VPN configuración, busque y, a continuación, seleccione el archivo de configuración que recibió del VPN administrador del cliente y, a continuación, seleccione Agregar perfil.
6. En la ventana AWS VPN Client, compruebe que su perfil esté seleccionado y, a continuación, elija Connect (Conectar). Si el VPN punto final del cliente se ha configurado para utilizar la

autenticación basada en credenciales, se le pedirá que introduzca 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).

AWS Client VPN para notas de la versión de Windows

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. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Date	Enlace de descarga y SHA256
3.14.0	• Se ha añadido soporte para la bandera `tap-sleep` abiertaVPN. • Se actualizaron las SSL bibliotecas Open VPN y Open.	12 de agosto de 2024	Descargar la versión 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96b96354516

Versión	Cambios	Date	Enlace de descarga y SHA256
3.13.0	Se actualizaron las bibliotecas abiertas VPN y abiertasSSL.	29 de julio de 2024	Descargue la versión 3.13.0 sha256: c9cc896e81a7441184 0951e349eed9384507 c53337fb703c5ec64d 522c29388b
3.12.1	Se ha corregido un problema que impedía que la versión 3.12.0 del cliente de Windows estableciera la VPN conexión para algunos usuarios.	18 de julio de 2024	Descargue la versión 3.12.1 sha256:5ed34aee6c0 3aa281e625acdbed27 2896c67046364a9e58 46ca697e05dbfec08
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 SAML finales.	21 de mayo de 2024	Ya no es compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
3.11.2	Se ha resuelto un problema SAML de autenticación con los navegadores basados en Chromium desde la versión 123.	11 de abril de 2024	Descargue la versión 3.11.2 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 Windows. VMs • Se corrigieron los problemas de conectividad de algunas LAN configura ciones. • 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 estaba activado en la red del 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 agregó soporte para la bandera abierta «verify-x509-name». VPN • 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 la denominación de los controladores de TAP Windows que afectaba a otros nombres de controladores. • 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
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
1.3.7	• 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 compatible

Versión	Cambios	Date	Enlace de descarga y SHA256
1.3.6	• Se agregó soporte para Open VPN flags: 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	• Se agregó soporte para Open flag: dhcp-option. VPN • Pequeñas correcciones de errores y mejoras.	4 de agosto de 2021	Ya no es compatible
1.3.3	• Se agregó soporte para las VPN banderas abiertas: 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	• Añada la prevención de IPv6 fugas cuando esté configurada. • 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 soporte para la directiva abierta «route-ipv6». VPN • 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 soporte para la directiva open cryptoapicert. VPN • 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 ha añadido soporte para los comentarios en la configuración abierta. VPN • Se agregó un mensaje de error para los errores del TLS apretón de manos.	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 agregó compatibilidad con la autenticación federada SAML basada en la versión 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 Open VPN static challenge echo para ocultar o mostrar el texto que se muestra 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

En estas secciones se describe cómo establecer una VPN conexión mediante el cliente AWS proporcionado para macOS. Puede descargar e instalar el cliente en AWS Client VPN download. El cliente AWS proporcionado no admite actualizaciones automáticas.

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 TCP puerto 8096 en su ordenador.
- Para los VPN puntos finales del cliente que utilizan la autenticación federada SAML basada (inicio de sesión único), el cliente reserva el puerto 35001. TCP

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

Temas

Conéctese al cliente VPN con un cliente AWS proporcionado para macOS

Antes de empezar, asegúrese de que el VPN administrador del cliente haya creado un VPN punto final del cliente y le haya proporcionado el archivo de configuración del VPN punto final del cliente.

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 el caso del archivo de configuración, busque el archivo de configuración que recibió del VPN administrador del cliente. 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 VPN terminal del cliente se ha configurado para utilizar la autenticación basada en credenciales, se le pedirá que introduzca 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 del cliente en la barra de menús y, a continuación, seleccionar Desconectar **<** **>** your-profile-name.

AWS Client VPN notas de la versión para macOS

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. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Fecha	Enlace de descarga
3.12.0	• Se ha añadido soporte para la VPN bandera `tap-sleep` abierta. • Se actualizaron las SSL bibliotecas Open VPN y Open.	12 de agosto de 2024	Descargar la versión 3.12.0 sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13
3.11.0	• Se actualizaron las bibliotecas Open y Open. VPN SSL	29 de julio de 2024	Descargar la versión 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f
3.10.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local. • Se ha corregido un problema DNS de restauración durante el cambio de red. • Se eliminó el enfoque automático de las aplicaciones cuando se conectaban a SAML puntos finales.	21 de mayo de 2024	Descargar la versión 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd

Versión	Cambios	Fecha	Enlace de descarga
3.9.2	• Se ha resuelto un problema SAML de autenticación con los navegadores basados en Chromium desde la versión 123. • Se agregó soporte para macOS Sonoma. Soporte obsoleto para macOS Big Sur. • Posición de seguridad mejorada.	11 de abril de 2024	Descargue la versión 3.9.2 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 corrigieron los problemas de conectividad de algunas configura ciones. 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 NAT64 estaba activado en la red del 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 agregó soporte para la bandera abierta «verify-x509-name». VPN • 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 agregó la supervisión del servidor durante la conexión. DNS Los ajustes se reconfigurarán si no coinciden con los VPN ajustes. • 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 ha añadido soporte para Open VPN flags: 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	• Se agregó soporte para Open flag: dhcp-option. VPN • 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 soporte para las VPN banderas abiertas: 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	• Añada la prevención de IPv6 fugas cuando esté configurada. • 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 ha corregido un problema que DNS eliminaba los ajustes configurados 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 soporte para la directiva abierta «route-ipv6». VPN • 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 ha añadido soporte para los comentarios en la configuración abierta. VPN • Se agregó un mensaje de error para los errores del TLS apretón de manos. • 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 compatibilidad con la autenticación federada SAML basada en la versión 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 ha corregido un problema que no DNS se solucionaba. • Se corrigió un problema que bloqueaba la aplicación y que era causado por conexiones más largas. • Se ha corregido un MFA problema.	2 de abril de 2020	Ya no es compatible.
1.1.0	• Se agregó soporte para la DNS configuración de macOS. • Se ha añadido compatibilidad con la función Open VPN Static Challenge Echo, que permite ocultar o mostrar el texto que se muestra 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

En estas secciones se describe la instalación del cliente AWS proporcionado para Linux y, a continuación, el establecimiento y el establecimiento de una VPN conexión mediante el cliente AWS proporcionado. El cliente AWS suministrado para Linux no admite actualizaciones automáticas. Para ver las actualizaciones y descargas más recientes, consulte lathe section called “Notas de la versión”.

Requisitos para conectarse al cliente VPN con un cliente AWS proporcionado para Linux

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

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

El cliente reserva el TCP puerto 8096 en su ordenador. Para los VPN puntos finales del cliente que utilizan la autenticación federada SAML basada (inicio de sesión único), el cliente reserva el puerto 35001. TCP

Antes de empezar, asegúrese de que el VPN administrador del cliente ha creado un punto final del cliente y le ha proporcionado el archivo de configuración del VPN punto final del cliente. VPN

Temas

- Instale el cliente AWS suministrado para Linux
- Conéctese al cliente AWS suministrado para Linux
- AWS Client VPN notas de la versión para Linux

Instale el cliente AWS suministrado para Linux

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 del AWS VPN cliente 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: realizar la instalación 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 de 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.

Conéctese al cliente AWS suministrado para Linux

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 el caso del archivo de configuración, busque el archivo de configuración que recibió del VPN administrador del cliente. 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 VPN terminal del cliente se ha configurado para utilizar la autenticación basada en credenciales, se le pedirá que introduzca 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).

AWS Client VPN notas de la versión para Linux

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. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Fecha	Enlace de descarga
3.15.0	• Se ha añadido soporte para la bandera `tap-sleep` abiertaVPN. • Se actualizaron las SSL bibliotecas Open VPN y Open.	12 de agosto de 2024	Descargue la versión 3.15.0 sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6d89d012
3.14.0	• Se actualizaron las bibliotecas abiertas VPN y abiertasSSL.	29 de julio de 2024	Descargue la versión 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020

Versión	Cambios	Fecha	Enlace de descarga
			d379e44f3 19b5334f60
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 SAML de autenticación con los navegadores 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

Versión	Cambios	Fecha	Enlace de descarga
3.12.0	• Se corrigieron los problemas de conectividad de algunas configura ciones. LAN	19 de diciembre de 2023	Descargar la versión 3.12.0 sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Reversión para «Se corrigieron los problemas de conectividad en algunas LAN configuraciones». • 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 corrigieron los problemas de conectividad de algunas LAN configura ciones. • 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 NAT64 estaba activado en la red del 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 agregó soporte para la bandera abierta «verify-x509-name». VPN	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 Open VPN flags: dev-type, keepalive connect-retry-max, 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 soporte para Open VPN flags: 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.

Conectarse a un VPN punto final de cliente mediante un VPN cliente abierto

Puede conectarse a un VPN punto final del cliente mediante aplicaciones Open VPN Client comunes.

> **Important**
>
> Si el VPN punto final del cliente se ha configurado para usar la autenticación federada SAML basada en código abierto, no puede usar el VPN cliente VPN basado en código abierto para conectarse a un VPN punto final del cliente.

Aplicaciones cliente

- Conectarse a un VPN punto final del cliente mediante una aplicación cliente de Windows
- Conectarse a un VPN punto final de cliente mediante una aplicación VPN cliente de Android o iOS
- Conectarse a un VPN punto final del cliente mediante una aplicación cliente macOS
- Conectarse a un VPN punto final de cliente mediante una aplicación de VPN cliente abierta

Conectarse a un VPN punto final del cliente mediante una aplicación cliente de Windows

En estas secciones se describe cómo establecer una VPN conexión mediante VPN clientes basados en Windows.

Antes de empezar, asegúrese de que el VPN administrador del cliente haya creado un VPN punto final del cliente y le haya proporcionado el archivo de configuración del VPN punto final del cliente.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de VPN conexiones de clientes con clientes basados en Windows.

> **Important**
>
> Si el VPN punto final del cliente se ha configurado para utilizar la autenticación federada SAML basada en datos abiertos, no podrá utilizar el VPN cliente VPN basado en código abierto para conectarse a un VPN punto final del cliente.

Tareas

- Utilice un certificado del almacén del sistema de certificados de Windows con Open VPN
- Utilice el botón Abrir VPN GUI
- Utilice el cliente Open VPN Connect

Utilice un certificado del almacén del sistema de certificados de Windows con Open VPN

Puede configurar el VPN cliente Open para que utilice un certificado y una clave privada del almacén del sistema de certificados de Windows. Esta opción resulta útil cuando se utiliza una tarjeta inteligente como parte de la VPN conexión de cliente. Para obtener información sobre la opción Open VPN client cryptoapicert, consulte el manual de referencia del sitio web Open VPN on the Open. VPN

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

Para usar la opción cryptoapicert con Open VPN

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 los certificados con el MMC complemento 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 VPN de configuración de Open y especifique el certificado utilizando el asunto del certificado 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"
```

Tras completar la configuración, utilice Abrir VPN para establecer una conexión.

Utilice el botón Abrir VPN GUI

El siguiente procedimiento muestra cómo establecer una VPN conexión mediante la aplicación VPN GUI cliente Open en un equipo con Windows.

> **Note**
>
> Para obtener información acerca de la aplicación VPN cliente Open, consulte Community Downloads en el VPN sitio web de Open.

Para establecer una VPN conexión

1. Inicie la aplicación VPN cliente Open.
2. En la barra de tareas de Windows, elija Mostrar u ocultar iconos. Haga clic con el botón derecho en Abrir y VPNGUI, a continuación, seleccione Importar archivo.
3. En el cuadro de diálogo Abrir, seleccione el archivo de configuración que ha recibido del VPN administrador del cliente y pulse Abrir.
4. En la barra de tareas de Windows, elija Mostrar u ocultar iconos. Haga clic con el botón derecho en Abrir y VPNGUI, a continuación, seleccione Conectar.

Utilice el cliente Open VPN Connect

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

> **Note**
>
> Para obtener más información, consulte Conexión a Access Server con Windows en el sitio VPN web de Open.

Para establecer una VPN conexión

1. Inicie la aplicación Open VPN Connect Client.
2. En la barra de tareas de Windows, elija Mostrar u ocultar iconos. Haga clic con el botón derecho en Abrir yVPN, a continuación, seleccione Importar perfil.
3. Elija Importar desde un archivo y seleccione el archivo de configuración que recibió del VPN administrador del cliente.
4. Elija el perfil de conexión para iniciar la conexión.

Conectarse a un VPN punto final de cliente mediante una aplicación VPN cliente de Android o iOS

> **Important**
>
> Si el VPN punto final del cliente se ha configurado para usar la autenticación federada SAML basada en código abierto, no puede usar el VPN cliente VPN basado en código abierto para conectarse a un VPN punto final del cliente.

La siguiente información muestra cómo establecer una VPN conexión mediante la aplicación Open VPN client 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 VPN cliente Open para iOS o Android, consulte la Guía del usuario de Open VPN Connect en el VPN sitio web de Open.

Antes de empezar, asegúrese de que el VPN administrador del cliente ha creado un VPN punto final del cliente y le ha proporcionado el archivo de configuración del VPN punto final del cliente.

Para establecer la conexión, inicie la aplicación VPN cliente Open y, a continuación, importe el archivo que recibió del VPN administrador del cliente.

Conectarse a un VPN punto final del cliente mediante una aplicación cliente macOS

En estas secciones se describe cómo establecer una VPN conexión mediante clientes basados en macOSVPN.

Antes de empezar, asegúrese de que el VPN administrador del cliente haya creado un VPN punto final del cliente y le haya proporcionado el archivo de configuración del VPN punto final del cliente.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de VPN conexiones de clientes con clientes macOS.

> **Important**
>
> Si el VPN punto final del cliente se ha configurado para utilizar la autenticación federada SAML basada en datos abiertos, no podrá utilizar el VPN cliente VPN basado en código abierto para conectarse a un VPN punto final del cliente.

Temas

- Inicie Tunnelblick para establecer una conexión AWS Client VPN
- Conéctese a un AWS Client VPN punto final mediante el cliente Open VPN Connect

Inicie Tunnelblick para establecer una conexión AWS Client VPN

El siguiente procedimiento muestra cómo establecer una VPN conexión mediante la aplicación cliente Tunnelblick en un ordenador 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 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 recibió del VPN administrador en el panel de configuraciones.
3. Seleccione el archivo de configuración en el panel Configurations (Configuraciones) y elija Connect (Conectar).

Conéctese a un AWS Client VPN punto final mediante el cliente Open VPN Connect

El siguiente procedimiento muestra cómo establecer una VPN conexión mediante la aplicación Open VPN Connect Client en un ordenador macOS.

> **Note**
>
> Para obtener más información, consulte Conexión a Access Server con macOS en el VPN sitio web de Open.

Para establecer una VPN conexión

1. Inicie la VPN aplicación Abrir y elija Importar, Desde un archivo local... .
2. Navegue hasta el archivo de configuración que recibió VPN del administrador y seleccione Abrir.

Conectarse a un VPN punto final de cliente mediante una aplicación de VPN cliente abierta

En estas secciones se describe cómo establecer una VPN conexión mediante VPN clientes de VPN base abierta.

Antes de empezar, asegúrese de que el VPN administrador del cliente haya creado un VPN punto final del cliente y le haya proporcionado el archivo de configuración del VPN punto final del cliente.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de VPN conexiones de clientes con clientes basados en Linux.

> **Important**
>
> Si el VPN punto final del cliente se ha configurado para utilizar la autenticación federada SAML basada en datos abiertos, no podrá utilizar el VPN cliente VPN basado en código abierto para conectarse a un VPN punto final del cliente.

Temas

Cree una conexión para AWS Client VPN usar Open VPN - Network Manager

El siguiente procedimiento muestra cómo establecer una VPN conexión mediante la VPN aplicación Open a través del Administrador de red GUI en un equipo Ubuntu.

Para establecer una VPN conexión

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 (+) situado junto a y VPN, a continuación, elija Importar desde un archivo... .
4. Navegue hasta el archivo de configuración que recibió del VPN administrador y seleccione Abrir.
5. En la VPN ventana Añadir, seleccione Añadir.
6. Inicia la conexión activando el botón situado junto al VPN perfil que has añadido.

Crea una conexión para AWS Client VPN usar Open VPN

El siguiente procedimiento muestra cómo establecer una VPN conexión mediante la VPN aplicación Open en un ordenador Ubuntu.

Para establecer una VPN conexión

1. Instale Open VPN mediante el siguiente comando.

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

2. Inicie la conexión cargando el archivo de configuración que recibió del VPN administrador.

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

Solución de problemas de la VPN conexión del cliente

Utilice los siguientes temas para solucionar los problemas que pueda tener al utilizar una aplicación cliente para conectarse a un punto final del clienteVPN.

Temas

Solución de problemas de VPN terminales de clientes para administradores

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

Para obtener información adicional sobre la solución de problemas con los VPN terminales del cliente, consulte Solución de problemas con el cliente VPN en la Guía AWS Client VPN del administrador.

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 AWS proporcionado 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 a su portapapeles.

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

Solución de problemas de VPN conexiones de clientes con clientes basados en Windows

Las siguientes secciones contienen información sobre los problemas que puede tener al utilizar clientes basados en Windows para conectarse a un VPN punto final del cliente.

Temas

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_'.
- VPNRegistros abiertos: contienen información sobre VPN los procesos abiertos. 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 VPN punto final del cliente.

Causa

Este problema podría deberse a una de las siguientes causas:

- Ya se está ejecutando otro VPN proceso de Open en su ordenador, lo que impide que el cliente se conecte.
- El archivo de configuración (.ovpn) no es válido.

Solución

Compruebe si hay otras VPN aplicaciones de Open ejecutándose en su ordenador. Si las hay, detenga o cierre estos procesos e intente conectarse de nuevo al VPN punto final del cliente. Compruebe si hay errores en los VPN registros abiertos y pida al VPN administrador del cliente que compruebe 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 .
- Que el CRL sigue siendo válido. Para obtener más información, consulte Los clientes no pueden conectarse a un VPN terminal de cliente en la Guía AWS Client VPN del administrador.

El cliente no se puede conectar con el mensaje TAP de registro «no hay adaptadores de Windows»

Problema

El cliente AWS proporcionado no puede conectarse al VPN punto final del cliente 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 desde Inicio -> Todos los programas -> TAP -Windows -> Utilidades -> Añadir un nuevo adaptador Ethernet virtual TAP -Windows».

Solución

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

- Reinicie el adaptador -WindowsTAP.
- Vuelva a instalar el TAP controlador -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 VPN punto final del cliente, pero está atascado en un estado de reconexión.

Causa

Este problema podría deberse a una de las siguientes causas:

- Su equipo no está conectado a Internet.
- El DNS nombre de host no se convierte en una dirección IP.
- Un VPN proceso abierto intenta conectarse al punto final de forma indefinida.

Solución

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

VPNel proceso de conexión se cierra inesperadamente

Problema

Al conectarse a un VPN punto final del cliente, el cliente se cierra inesperadamente.

Causa

TAP-Windows no está instalado en su ordenador. 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

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

Solución

Vuelva a ejecutar el instalador de 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 VPN punto final del cliente utiliza la autenticación mutua, el archivo de configuración (.ovpn) no contiene el certificado ni la clave del cliente.

Solución

Asegúrese de que el VPN administrador del cliente añada el certificado y la clave del 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 .

El cliente se bloquea en Dell PCs con Windows 10 u 11

Problema

En algunos equipos Dell PCs (ordenadores de sobremesa y portátiles) que utilizan Windows 10 u 11, se puede producir un bloqueo al navegar por el sistema de archivos para importar un archivo de VPN configuración. Si se produce este problema, verá 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 los tres siguientesDLLs:

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.dll

Solución

Para evitar este problema, primero asegúrese de que su cliente esté actualizado con la última versión del cliente AWS proporcionado. Ve a VPNDescarga AWS del cliente y, si hay disponible una versión más reciente, actualiza a la versión más reciente.

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, también puede eliminar los DLL archivos o cambiarles el nombre. Sin embargo, tenga en cuenta que esto impedirá que la aplicación Dell Backup and Recovery funcione por completo.

Elimine o cambie 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 DLL archivos del directorio de instalación o cámbieles el nombre. Cualquiera de estas acciones impedirá que se carguen.

   - DBRShellExtension.dll
   - DBROverlayIconBackuped.dll
   - DBROverlayIconNotBackuped.dll

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

VPNse desconecta con un mensaje emergente

Problema

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

Causa

TAP-El adaptador de 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
```

Abrir VPN GUI

La siguiente información de solución de problemas se probó en las versiones 11.10.0.0 y 11.11.0.0 del VPN GUI software Open 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
```

Abra el cliente Connect VPN

La siguiente información de solución de problemas se probó en las versiones 2.6.0.100 y 2.7.1.101 del software Open VPN 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 ha podido resolver 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 DNS nombre. El cliente debe anteponer una cadena aleatoria al DNS nombre para evitar el almacenamiento en DNS caché; sin embargo, algunos clientes no lo hacen.

Solución

Consulte la solución para No se puede resolver el DNS nombre del VPN terminal del cliente en la AWS Client VPN Guía del administrador.

Falta PKI un alias

Problema

Se produce el siguiente error en la conexión a un VPN punto final del cliente que no utiliza la autenticación mutua.

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

Causa

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

Solución

Especifique una clave de cliente y un certificado aleatorios en el archivo de VPN configuración del cliente e importe la nueva configuración al software Open VPN Connect Client. Como alternativa, utilice un cliente diferente, como el cliente Open (v11.12.0.0) o el VPN GUI cliente Viscosity (v.1.7.14).

Solución de problemas de VPN conexiones de clientes con clientes 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
- Abre VPN

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_'.
- VPNRegistros abiertos: contienen información sobre VPN los procesos abiertos. 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 VPN punto final del cliente.

Causa

Este problema podría deberse a una de las siguientes causas:

- Ya se está ejecutando otro VPN proceso de Open en su ordenador, lo que impide que el cliente se conecte.
- El archivo de configuración (.ovpn) no es válido.

Solución

Compruebe si hay otras VPN aplicaciones de Open ejecutándose en su ordenador. Si las hay, detenga o cierre estos procesos e intente conectarse de nuevo al VPN punto final del cliente. Compruebe si hay errores en los VPN registros abiertos y pida al VPN administrador del cliente que compruebe 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 .
- Que el CRL sigue siendo válido. Para obtener más información, consulte Los clientes no pueden conectarse a un VPN terminal de cliente en la Guía AWS Client VPN del administrador.

El cliente está atascado en un estado de reconexión

Problema

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

Causa

Este problema podría deberse a una de las siguientes causas:

- Su equipo no está conectado a Internet.
- El DNS nombre de host no se convierte en una dirección IP.
- Un VPN proceso abierto intenta conectarse al punto final de forma indefinida.

Solución

Compruebe que el equipo esté conectado a Internet. Pida al VPN administrador del cliente que verifique que la `remote` directiva del archivo de configuración se dirija a una dirección IP válida. También puede desconectar la VPN sesión seleccionando Desconectar en la ventana del AWS VPN cliente 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 VPN punto final del cliente utiliza la autenticación mutua, el archivo de configuración (.ovpn) no contiene el certificado ni la clave del cliente.

Solución

Asegúrese de que el VPN administrador del cliente añada el certificado y la clave del 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 auxiliar (error)

Problema

Aparece el siguiente error al intentar conectar elVPN.

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

Solución

Consulte el siguiente artículo sobre AWS Re:post. AWSVPNCliente: error: se necesita una 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, seleccione Configuración y ajuste el valor del nivel de registro. VPN

No se encontró el algoritmo de cifrado '-256-' AES GCM

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 utiliza una VPN versión abierta que no admite el algoritmo AES de cifrado -256-. GCM

Solución

Elija una VPN versión abierta compatible de la siguiente manera:

1. Abra la aplicación Tunnelblick.
2. Elija Configuración.
3. Para la VPNversión abierta, elija 2.4.6; la SSL versión abierta es la 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 un nuevo archivo de configuración al administrador del cliente. VPN

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, Sin embargo, la autenticación del cliente falla porque el certificado del cliente tiene el campo de uso de clave extendido (EKU) habilitado para la autenticación del servidor.

Solución

Compruebe que esté utilizando un certificado y una clave de cliente correctos. Si es necesario, compruébelo con el VPN administrador del cliente. Este error puede producirse si utiliza el certificado del servidor y no el certificado del cliente para conectarse al VPN punto final del cliente.

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 VPN administrador del cliente.

Abre VPN

La siguiente información de solución de problemas se probó en la versión 2.7.1.100 del software Open VPN 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 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

Open VPN Connect no puede resolver el VPN DNS nombre del cliente.

Solución

Consulte la solución para ver si no se puede resolver el DNS nombre del VPN terminal del cliente en la Guía AWS Client VPN del administrador.

Solución de problemas de VPN conexiones de clientes con clientes basados en 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
- Abrir VPN (línea de comandos)
- Abrir VPN 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, una vez establecida la VPN conexión, DNS las consultas seguirán dirigiéndose al servidor de nombres del sistema predeterminado, en lugar de a los servidores de nombres configurados para el punto final del cliente. VPN

Causa

El cliente interactúa con systemd-resolved, un servicio disponible en los sistemas Linux, que actúa como elemento central de la administración. DNS Se utiliza para configurar los DNS servidores que se envían desde el punto final del cliente. VPN El problema se debe a que systemd-resolved no establece la máxima prioridad para DNS los servidores proporcionados por el punto final del clienteVPN. En su lugar, agrega los servidores a la lista existente de DNS servidores que están configurados en el sistema local. Como resultado, es posible que los DNS servidores originales sigan teniendo la máxima prioridad y, por lo tanto, se utilicen para resolver DNS consultas.

Solución

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

   ```
   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 quieres que las DNS consultas estén resueltas por systemd como proxy, sino que prefieres que las consultas se envíen directamente a los servidores de DNS nombres reales, haz un enlace simbólico a. `/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

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

   Puede que desee realizar este procedimiento para omitir la configuración resuelta por el sistema, por ejemplo, para el almacenamiento en caché de las DNS respuestas, la configuración por

interfaz, la aplicación, etc. DNS DNSSec Esta opción resulta especialmente útil cuando se necesita sustituir un DNS registro público por un registro privado al conectarse a él. VPN Por ejemplo, puede tener un DNS solucionador privado en su entorno privado VPC con un registro para www.example.com, que se resuelve en una IP privada. Esta opción podría utilizarse para anular el registro público de www.example.com, que se soluciona con una IP pública.

Abrir VPN (línea de comandos)

Problema

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

Causa

El DNS servidor no está configurado en el VPN punto final del cliente o el software del cliente no lo acepta.

Solución

Siga los siguientes pasos para comprobar que el DNS servidor está configurado y funciona correctamente.

1. Asegúrese de que DNS haya una entrada del servidor en los registros. En el siguiente ejemplo, el DNS servidor `192.168.0.2` (configurado en el VPN punto final del cliente) 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 DNS servidor, pida al VPN administrador del cliente que modifique el VPN punto final del cliente y se asegure de que se ha especificado un DNS VPC DNS servidor (por ejemplo, el servidor) para el VPN punto final del cliente. Para obtener más información, consulte los VPNpuntos finales del cliente en la Guía del AWS Client VPN administrador.
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 VPN configuración del cliente (el archivo.ovpn) en un editor de texto y añada 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
```

Abrir VPN a través de Network Manager () GUI

Problema

Cuando se utiliza el VPN cliente Network Manager Open, la conexión falla y se produce 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 para el caso de que no se pueda resolver el DNS nombre del VPN terminal del cliente en la Guía AWS Client VPN del administrador.

Solución de problemas comunes de VPN los clientes

Los siguientes son problemas comunes que puede tener al utilizar un cliente para conectarse a un VPN punto final del cliente.

TLSerror en la negociación de la clave

Problema

La TLS negociación fracasa y se produce 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 UDP TCP el tráfico.
- Está utilizando una clave y un certificado de cliente incorrectos en su archivo de configuración (.ovpn).
- La lista de revocaciones de certificados de cliente (CRL) ha caducado.

Solución

Compruebe si las reglas del firewall de su equipo bloquean la entrada o la salida o el UDP tráfico en los puertos 443 TCP o 1194. Pídale al VPN administrador de su cliente que verifique la siguiente información:

- Que las reglas del firewall del VPN punto final del cliente no TCP bloqueen el UDP tráfico 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 .
- Que sigue CRL siendo válido. Para obtener más información, consulte Los clientes no pueden conectarse a un VPN terminal de cliente en la Guía AWS Client VPN del administrador.

Historial de documentos

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

Cambio	Descripción	Fecha
AWS Publicado el cliente proporcionado (3.15.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	12 de agosto de 2024
AWS Publicado el cliente proporcionado (3.14.0) para Windows	Consulte las notas de la versión para obtener más detalles.	12 de agosto de 2024
AWS Lanzamiento del cliente proporcionado (3.12.0) para macOS	Consulte las notas de la versión para obtener más detalles.	12 de agosto de 2024
AWS Publicado el cliente proporcionado (3.14.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	29 de julio de 2024
AWS Publicado el cliente proporcionado (3.13.0) para Windows	Consulte las notas de la versión para obtener más detalles.	29 de julio de 2024
AWS Lanzamiento del cliente proporcionado (3.11.0) para macOS	Consulte las notas de la versión para obtener más detalles.	29 de julio de 2024
AWS Publicado el cliente proporcionado (3.12.1) para Windows	Consulte las notas de la versión para obtener más detalles.	18 de julio de 2024
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 publicó el cliente proporcionado para Ubuntu 18.04 LTS y Ubuntu 20.04 LTS	Puede usar el cliente AWS proporcionado en Ubuntu 18.04 y Ubuntu 20.04LTS. LTS	11 de junio de 2021
Support for Open VPN mediante un certificado de la tienda del sistema de certificados de Windows	Puede utilizar Abrir VPN con un certificado de la tienda 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 archivo de cliente y configuración AWS proporcionado.	29 de octubre de 2020
AWS cliente proporcionado	Puede usar el cliente AWS proporcionado para conectarse a un VPN punto final del cliente.	4 de febrero de 2020
Versión inicial	Esta versión presenta AWS ClientVPN.	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.