Guía del usuario de

AWS Client VPN

AWS Client VPN: Guía del usuario de

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 de forma segura a los recursos de AWS y los recursos 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 de Client VPN

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

- Punto de conexión de Client VPN: el administrador de Client VPN crea y configura un punto de conexión 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. El archivo incluye información sobre el punto de conexión de Client VPN y los certificados que son necesarios para establecer una conexión de VPN. Cargue este archivo en la aplicación cliente de VPN que haya elegido. El cliente proporcionado por AWS le permite conectarse a cinco sesiones simultáneas, cada una con su propio archivo de configuración proporcionado por el administrador de Client VPN. Para obtener más información sobre sesiones simultáneas, consulte Compatibilidad con conexiones simultáneas.

Recursos adicionales para configurar Client VPN

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 conexión de Client VPN.

Empiece a utilizar AWS 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

Requisitos previos para usar Client VPN

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

- Acceso a Internet
- Un dispositivo compatible
- Una versión compatible de Windows, macOS o Linux.
- 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.

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

- Si el administrador no ha configurado archivos de configuración de punto de conexión, descargue e instale el cliente desde Descarga de AWS Client VPN. Tras descargar e instalar la aplicación, continúe con the section called “Paso 2: Obtener el archivo de configuración del punto de enlace de Client VPN” para obtener el archivo de configuración del punto de conexión del administrador. Si se conecta a varios perfiles, necesitará un archivo de configuración para cada perfil.
- Si el administrador ya ha preconfigurado el archivo de configuración del punto de conexión, puede descargar la aplicación de Client VPN, junto con el archivo de configuración, desde el portal de autoservicio. Para informarse de los pasos para descargar el cliente y el archivo de configuración del portal de autoservicio, consulte the section called “Descarga de Client VPN”. Tras descargar e instalar la aplicación y el archivo, vaya a the section called “Paso 3: Conectarse a la VPN”.

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 le proporciona el archivo de configuración del punto de conexión 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 Descarga de AWS Client VPN 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, incluida la importación de uno o varios archivos de configuración de punto de conexión para un cliente proporcionado por AWS, consulte los siguientes temas:

- Conexión a un punto de conexión de AWS Client VPN mediante un cliente proporcionado por AWS
- Conéctese a un AWS Client VPN punto final mediante un cliente 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.

Descarga de AWS Client VPN del portal de autoservicio

El portal de autoservicio es una página web que le permite descargar la versión más reciente del cliente proporcionado por AWS y de las versiones más recientes de los archivos de configuración de punto de conexión de Client VPN. Si el administrador del punto de conexión de Client VPN ya ha preconfigurado uno o varios archivos de configuración del cliente de Client VPN, puede descargar e instalar la aplicación de Client VPN, junto con esos archivos de configuración, desde este portal.

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

Antes de empezar, debe tener el ID de cada punto de conexión de Client VPN que desee descargar. El administrador del punto de conexión de Client VPN puede proporcionarle el ID o facilitarle una URL del portal de autoservicio que incluya el ID. Para varias conexiones de punto de conexión, necesitará el ID de punto de conexión de cada perfil al que desee conectarse.

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. Si desea conectarse a varios puntos de conexión, deberá descargar el archivo de configuración de uno.
   - Descargar la versión más reciente del cliente proporcionado por AWS para su plataforma.
5. Repita estos pasos para cada archivo de configuración de punto de conexión para el que desee crear un perfil de conexión.

Conexión a un punto de conexión de AWS Client VPN mediante un cliente proporcionado por AWS

Puede conectarse a un punto de conexión de Client VPN utilizando el cliente proporcionado por AWS, compatible con Windows, macOS y Ubuntu. El cliente proporcionado por AWS también admite hasta cinco conexiones simultáneas, así como las directivas de OpenVPN.

Temas

Seguridad

La seguridad es nuestra mayor prioridad en el cliente proporcionado por AWS. Publicamos parches de forma periódica para mejorar la posición de seguridad de la aplicación. El cliente proporcionado por AWS incluye varias características de seguridad únicas en comparación con otros clientes de OpenVPN, como autenticación SAML, Client Routes Enforcement y monitorización de la configuración del dispositivo.

Si bien el cliente proporcionado por AWS está diseñado para mitigar las amenazas que se originan en un entorno de red configurado incorrectamente o comprometido, no es responsable de modificar el entorno ni de eliminar las amenazas externas en su origen. El cliente proporcionado por AWS depende de los clientes para mantener un entorno seguro y bien configurado. Esto incluye:

- Prevención de la modificación no autorizada o de abusos por parte de usuarios locales
- Restricción de privilegios administrativos a usuarios de confianza
- Mantenimiento de parches de seguridad actualizados

Compatibilidad con conexiones simultáneas utilizando un cliente proporcionado por AWS

El cliente proporcionado por AWS permite conectarse a varias sesiones simultáneas. Esto resulta útil si necesita acceder a recursos en varios entornos de AWS y tiene diferentes puntos de conexión para esos recursos. Por ejemplo, es posible que necesite acceder a una base de datos

en un entorno de un punto de conexión diferente del punto de conexión al que está conectado actualmente, pero que no desee desconectar la conexión actual. Para permitir que el cliente proporcionado por AWS se conecte a las sesiones actuales, descargue el archivo de configuración que el administrador ha creado para cada punto de conexión y, a continuación, cree un perfil de conexión para cada archivo. Con el cliente proporcionado por AWS, puede conectarse a varias sesiones sin desconectarse de ninguna sesión abierta actualmente. Esto solo se admite con clientes proporcionados por AWS. Para informarse de los pasos para conectarse a sesiones simultáneas, consulte lo siguiente:

- Conexión mediante el cliente proporcionado por AWS para Windows
- Conexión mediante el cliente proporcionado por AWS para macOS
- Conexión mediante el cliente proporcionado por AWS para Linux

Al conectarse a varios puntos de conexión, Client VPN implementa comprobaciones para garantizar que no haya conflictos con otras conexiones de punto de conexión abiertas, por ejemplo, si dos sesiones tienen bloques de CIDR o políticas de enrutamiento en conflicto, o si ya está conectado con una conexión de túnel completa. Si la comprobación detecta conflictos, no se establecerá una conexión hasta que elija una conexión diferente que no entre en conflicto con la conexión abierta o hasta que se desconecte de la sesión abierta que está causando el conflicto.

Se permiten conexiones de DNS simultáneas. Se aplicará el servidor de DNS de una de las conexiones habilitadas para DNS. Según el servidor de DNS, es posible que se le pida que se autentique durante esa reconexión.

> **Note**
>
> El número máximo de sesiones simultáneas es cinco.

Directivas de OpenVPN

El cliente proporcionado por AWS admite las siguientes directivas de OpenVPN. Para obtener más información sobre estas directivas, consulte la documentación en el sitio web de OpenVPN.

- auth-federate
- auth-nocache
- auth-retry

- auth-user-pass
- block-outside-dns
- ca
- cert
- cipher
- cliente
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive
- clave
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- ping-exit
- 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
- tap-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN para Windows

En estas secciones se describe cómo establecer una conexión VPN mediante el cliente AWS proporcionado para los sistemas Windows x64 y Windows Arm64. Visite AWS Client VPN download para descargar e instalar el cliente. El cliente AWS proporcionado no admite actualizaciones automáticas.

Requisitos

El cliente AWS proporcionado es compatible con los sistemas Windows x64 y Arm64. Se requiere lo siguiente para cada sistema operativo:

Sistemas operativos Windows Arm64

- Windows 11 (sistema operativo de 64 bits, procesador Arm64)
- .NET Framework 4.8.1 o superior

> **Note**
>
> Esta aplicación incluye procesos en segundo plano que utilizan emulación de Arm64. Esto es totalmente compatible y está habilitado de forma predeterminada en los dispositivos Windows 11 Arm64, lo que garantiza un funcionamiento perfecto sin necesidad de

configuración adicional. Para obtener más información, consulte Funcionamiento de la emulación de en ARM.

Sistemas operativos Windows x64

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

> **Note**
>
> En el caso de los sistemas operativos Windows x64 y Arm64, los puntos de conexión de Client VPN que utilizan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva los puertos 8096-8115 TCP en el equipo.

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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Temas

- Conexión a AWS Client VPN con un cliente proporcionado por AWS para Windows
- AWS Client VPN para notas de la versión para Windows

Conexión a AWS Client VPN con un cliente proporcionado por AWS para Windows

Antes de comenzar, tiene que haber leído los requisitos. El cliente proporcionado por AWS también se denomina Site-to-Site VPN Client en los siguientes pasos.

Para conectarse mediante el cliente proporcionado por AWS para sistemas basados en Windows x64 o Windows Arm64:

1. Abra la aplicación Site-to-Site 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. Si desea crear varias conexiones, repita los pasos de Agregar perfil para cada archivo de configuración que desee agregar. Puede añadir tantos perfiles como desee, pero solo puede tener un máximo de cinco conexiones abiertas.
7. En la ventana Cliente de Site-to-Site VPN, elija el perfil al que desee conectarse y, a continuación, seleccione 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. Repita este paso para cada conexión de perfil que desee iniciar, conectando hasta cinco puntos de conexión simultáneos.

   > **Note**
   >
   > Si algún perfil al que se conecta entra en conflicto con una sesión abierta actualmente, no podrá establecer la conexión. Elige una conexión nueva o desconéctese de la sesión que está causando el conflicto.

8. Para ver las estadísticas de una conexión, seleccione Conexión en la ventana Cliente de AWS VPN, seleccione Mostrar detalles y, a continuación, elija la conexión sobre la que desee ver detalles.
9. Para desconectar una conexión, elija una conexión en la ventana Cliente de AWS VPN y, a continuación, seleccione Desconectar. Si tiene varias conexiones abiertas, debe cerrar cada conexión individualmente. 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 para Windows

La siguiente tabla contiene las notas de la versión y los enlaces de descarga de la versión actual y las versiones anteriores de AWS Client VPN para sistemas Windows basados en x64 y en Arm64.

> **Note**
>
> Seguimos proporcionando correcciones de uso y seguridad con cada versión. Le recomendamos encarecidamente que utilice la versión más reciente de cada plataforma. Es posible que las versiones anteriores se vean afectadas por problemas de uso o seguridad. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Date	Enlace de descarga y SHA256
5.3.1 (x64 y Arm64)	Pequeñas correcciones de errores y mejoras.	30 de septiembre de 2025	• Descargue Windows x64 versión 5.3.1 sha256: b71ddbc78230630963acf3ebba7afeb6e52599843091ff589aed6afce4c9eb06 • Descargue Windows Arm64 versión 5.3.1 sha256: e691bdb0bdcb55b3da36f4fb2e5198f20f1878dc22a00

Versión	Cambios	Date	Enlace de descarga y SHA256
			bf55bc660 999698500b
5.3.0 (Arm64)	Nueva compatibilidad de AWS Client VPN con los sistemas operativos basados en Arm64 de Windows. Esta versión incluye todas las actualizaciones de Windows (x64) versión 5.3.0.	26 de agosto de 2025	Descargue Windows Arm64 versión 5.3.0 sha256: 3f1be6b48 7af8307da fbb0f7737 cd597cf71 dc64dcd31 775aeeebf 91d04b8dce
5.3.0	• Pequeñas mejoras. • Se ha agregado compatibilidad con conexiones IPv6	14 de agosto de 2025	Descargue Windows x64 versión 5.3.0 sha256: e3cf1aff6 e14d79aa4 4378229a3 a0602a9e9 c2a0c6d0d 055df9014 40b6d1454a

Versión	Cambios	Date	Enlace de descarga y SHA256
5.2.2	Posición de seguridad mejorada.	2 de junio de 2025	Descargar versión 5.2.2 sha256: f27cb0eed7c9c5354caa5d7e37595eefbb048d7481bf698b2e5fb653b667c190
5.2.1	• Se ha agregado compatibilidad para el indicador `ping-exit` OpenVPN. • Se ha actualizado la biblioteca de OpenSSL. • Pequeñas correcciones de errores y mejoras.	21 de abril de 2025	Ya no es compatible.
5.2.0	• Pequeñas mejoras. • Se ha agregado compatibilidad con Client Route Enforcement.	8 de abril de 2025	Ya no es compatible.
5.1.0	• Se ha corregido un problema que provocaba que AWS Client VPN versión 5.0.x se volviera a conectar automáticamente a la VPN tras un tiempo de espera por inactividad. • Pequeñas correcciones de errores y mejoras.	17 de marzo de 2025	Ya no es compatible.

Versión	Cambios	Date	Enlace de descarga y SHA256
5.0.2	• Se ha corregido un problema de conexiones simultáneas de DNS. • Se han corregido problemas esporádicos de instalación de nuevos adaptadores TAP.	24 de febrero de 2025	Ya no es compatible.
5.0.1	Se ha corregido un problema que provocaba errores de conexión de la VPN de forma esporádica en el cliente de Windows version 5.0.0	30 de enero de 2025	Ya no es compatible.
5.0.0	• Se ha agregado compatibilidad con conexiones simultáneas. • Se ha actualizado la versión del controlador TAP. • Se ha actualizado la interfaz gráfica de usuario. • Pequeñas correcciones de errores y mejoras	21 de enero de 2025	Ya no es compatible.
4.1.0	Pequeñas correcciones de errores y mejoras.	12 de noviembre de 2024	Ya no es compatible.
4.0.0	Pequeñas mejoras.	25 de septiembre de 2024	Descarga de la versión 4.0.0 sha256: 6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc

Versión	Cambios	Date	Enlace de descarga y SHA256
3.14.2	Se ha agregado compatibilidad para el indicador `mssfix` OpenVPN.	4 de septiembre de 2024	Descarga de la versión 3.14.2 sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Pequeñas correcciones de errores y mejoras.	22 de agosto de 2024	Descarga de la versión 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	• Se ha agregado compatibilidad para el indicador `tap-sleep` OpenVPN. • Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	12 de agosto de 2024	Descarga de la versión 3.14.0 sha256: 812fb2f6d 263288c66 4d598f6bd 70e3f601d 11dcb89e6 3b281b0a9 6b96354516

Versión	Cambios	Date	Enlace de descarga y SHA256
3.13.0	Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	29 de julio de 2024	Descarga de la versión 3.13.0 sha256: c9cc896e81a7441184 0951e349eed9384507 c53337fb703c5ec64d 522c29388b
3.12.1	Se ha corregido un problema que impide que la versión 3.12.0 del cliente de Windows establezca una conexión VPN para algunos usuarios.	18 de julio de 2024	Descarga de la versión 3.12.1 sha256: 5ed34aee6c03aa281e 625acdbed272896c67 046364a9e5846ca697 e05dbfec08
3.12.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local. • Se ha eliminado el enfoque automático de las aplicaciones cuando se conectaban a puntos de conexión SAML.	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 de autentica ción SAML con los navegadores basados en Chromium desde la versión 123.	11 de abril de 2024	Descarga de la versión 3.11.2 sha256: 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc
3.11.1	• Se ha corregido una acción de desbordamiento de búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Posición de seguridad mejorada.	16 de febrero de 2024	Descarga de 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	• Soporte agregado para los indicador es OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • Pequeñas correcciones de errores y mejoras.	20 de septiembre de 2021	Ya no es compatibl e
1.3.5	Parche para eliminar archivos de registros de Windows grandes.	16 de agosto de 2021	Ya no es compatibl e
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 compatibl e
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 compatibl e

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

En estas secciones se describe 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.

Requisitos

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

- macOS Sonoma (14.0), Sequoia (15.0) o Tahoe (26.0)
- ARM64 x86_64 o compatible con procesadores.
- Para Client VPN, los puntos de conexión que usan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva los puertos 8096-8115 TCP en su equipo.

Temas

Conexión a AWS Client VPN con un cliente proporcionado por AWS para 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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Asegúrese también de haber leído los requisitos. El cliente proporcionado por AWS también se denomina Site-to-Site VPN Client en los siguientes pasos.

Para conectarse mediante el cliente proporcionado por AWS para macOS

1. Abra la aplicación Site-to-Site 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. Si desea crear varias conexiones, repita los pasos de Agregar perfil para cada archivo de configuración que desee agregar. Puede añadir tantos perfiles como desee, pero solo puede tener un máximo de cinco conexiones abiertas.
7. En la ventana Cliente de Site-to-Site VPN, elija el perfil al que desee conectarse y, a continuación, seleccione 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. Repita este paso para cada conexión de perfil que desee iniciar, conectando hasta cinco puntos de conexión simultáneos.

   > **Note**
   >
   > Si algún perfil al que se conecta entra en conflicto con una sesión abierta actualmente, no podrá establecer la conexión. Elige una conexión nueva o desconéctese de la sesión que está causando el conflicto.

8. Para ver las estadísticas de una conexión, seleccione Conexión en la ventana Cliente de AWS VPN, seleccione Mostrar detalles y, a continuación, elija la conexión sobre la que desee ver detalles.
9. Para desconectar una conexión, elija una conexión en la ventana Cliente de AWS VPN y, a continuación, seleccione Desconectar. Si tiene varias conexiones abiertas, debe cerrar cada conexión individualmente.

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 uso y seguridad con cada versión. Le recomendamos encarecidamente que utilice la versión más reciente de cada plataforma. Las versiones anteriores pueden verse afectadas por problemas de and/or seguridad de usabilidad. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Fecha	Enlace de descarga
5.3.3	• Pequeñas correcciones de errores y mejoras. • Posición de seguridad mejorada.	26 de diciembre de 2025	• Descargar macOS ARM64 versión 5.3.3 sha256:97c4b869ea5a544a4a4fe661580ec21f412b141bb2187fd32fcd97e75581b018 • Descargar macOS x64 versión 5.3.3 sha256: cf8d16ec35b330969510a6cfc828db1157088ad7bb77e0344b87bd7a59921c1f
5.3.2	• Se agregó soporte nativo para la arquitectura Apple Silicon y un nuevo ARM64 instalador de macOS. • Pequeñas correcciones de errores y mejoras.	27 de octubre de 2025	• Descargar macOS ARM64 versión 5.3.2 sha256: ef0e323f7c262263018ae303d1cfd0333c976963a5e1055706b988d7463e1dd2 • Descargue macOS x64 versión 5.3.2 sha256: 29c0fc329b7ac457bbbb3ee71004bf4f7ef76a928b08c8c589a04f65804f8986
5.3.1	• Pequeñas correcciones de errores y mejoras.	9 de septiembre de 2025	Descargar la versión 5.3.1 sha256: e71c70072c338bd41f3925a541f

Versión	Cambios	Fecha	Enlace de descarga
			5d7a73d9e063a00786 a603ea9043ced1baa16
5.3.0	• Pequeñas mejoras. • Se agregó soporte para IPv6 conexiones.	14 de agosto de 2025	Descargue la versión 5.3.0 sha256: ec5b7c562 b1e91d902168f32c42 6c0a074ee0fdbfc061 ef862165d6a42d2cf79
5.2.1	• Se ha agregado compatibilidad con la marca ping-exit OpenVPN. • Se ha actualizado la biblioteca de OpenSSL. • Posición de seguridad mejorada. • Pequeñas correcciones de errores y mejoras.	18 de junio de 2025	Descargar la versión 5.2.1 sha256: 906f77fbc a3334fbdcd1145dd6f 2725beab82a30b9b51 eafd1a25c3fe7d669eb
5.2.0	• Pequeñas mejoras. • Se ha agregado compatibilidad con Client Route Enforcement.	8 de abril de 2025	Ya no es compatible.
5.1.0	• Se ha corregido un problema que provocaba que la AWS Client VPN versión 5.0.x se volviera a conectar automáticamente a la VPN tras un tiempo de espera por inactividad. • Se ha corregido un problema que AWS Client VPN impedía establecer una conexión VPN para los archivos de configuración con terminaciones de línea similares a las de Windows. • Pequeñas correcciones de errores y mejoras.	17 de marzo de 2025	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
5.0.3	Pequeñas correcciones de errores y mejoras.	6 de marzo de 2025	Ya no es compatible.
5.0.2	Se ha corregido un problema que provocaba errores esporádicos al elegir Conectar.	17 de febrero de 2025	Ya no es compatible.
5.0.1	Se ha corregido un problema que impedía que la versión 5.0.0 del cliente estableciera una conexión de VPN para nombres de perfil que contenían espacios.	22 de enero de 2025	Ya no es compatible.
5.0.0	• Se ha agregado compatibilidad con conexiones simultáneas. • Se ha actualizado la interfaz gráfica de usuario. • Pequeñas correcciones de errores y mejoras.	21 de enero de 2025	Ya no es compatible.
4.1.0	Pequeñas correcciones de errores y mejoras.	12 de noviembre de 2024	Ya no es compatible.
4.0.0	Pequeñas mejoras.	25 de septiembre de 2024	Ya no es compatible.
3.12.1	Se ha agregado compatibilidad para el indicador `mssfix` OpenVPN.	4 de septiembre de 2024	Ya no es compatible.
3.12.0	• Se ha agregado compatibilidad para el indicador `tap-sleep` OpenVPN. • Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	12 de agosto de 2024	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
3.11.0	• Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	29 de julio de 2024	Ya no es compatible.
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 ha eliminado el enfoque automátic o de las aplicaciones cuando se conectaban a puntos de conexión SAML.	21 de mayo de 2024	Ya no es compatible.
3.9.2	• Se ha resuelto un problema de autenticación SAML con los navegadores basados en Chromium desde la versión 123. • Se ha agregado compatibilidad para macOS Sonoma. Dé de baja la compatibilidad para macOS Big Sur. • Posición de seguridad mejorada.	11 de abril de 2024	Ya no es compatible.
3.9.1	• Se ha corregido una acción de desbordamiento de búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Se ha corregido la barra de progreso de descarga de la actualización de la aplicación. • Posición de seguridad mejorada.	16 de febrero de 2024	Ya no es compatible.

Versión	Cambios	Fecha	Enlace de descarga
3.9.0	• Se han corregido los problemas de conectividad para algunas configuraciones de LAN. • Se ha mejorado la conectividad.	6 de diciembre de 2023	Ya no es compatible.
3.8.0	• Se ha corregido un problema de conectividad cuando NAT64 está activado en la red del cliente. • Pequeñas correcciones de errores y mejoras.	24 de agosto de 2023	Ya no es compatible.
3.7.0	• Posición de seguridad mejorada.	3 de agosto de 2023	Ya no es compatible.
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.
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.

Versión	Cambios	Fecha	Enlace de descarga
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	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 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 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.

Versión	Cambios	Fecha	Enlace de descarga
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 indicador es de OpenVPN: dev-type connect-r etry-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 aplicació n 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 función de prevención de fugas cuando esté configurada. IPv6 • 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

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

Requisitos para conectarse a Client VPN con un cliente proporcionado por AWS para Linux

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

- Ubuntu 22.04 LTS (AMD64) o Ubuntu 24.04 LTS (solo AMD64)

Para Client VPN, los puntos de conexión que usan la autenticación federada basada en SAML (inicio de sesión único), el cliente reserva los puertos 8096-8115 TCP en su equipo.

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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Temas

- Instalación de AWS Client VPN proporcionado para Linux
- Conexión a la AWS Client VPN proporcionada para Linux
- AWS Client VPN notas de la versión para Linux

Instalación de AWS Client VPN proporcionado para Linux

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

Opción 1: Instalación a través del repositorio de paquetes

1. Agregue la clave pública de AWS VPN Client 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 siguiente para agregar el repositorio al sistema operativo Ubuntu (versión 22.04 y superior):

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu 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. Utilice el siguiente comando para instalar el cliente proporcionado por AWS para Linux.

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

Opción 2: 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 proporcionado por AWS para Linux mediante la utilidad dpkg.

```
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 a la AWS Client VPN proporcionada para Linux

El cliente proporcionado por AWS también se denomina Site-to-Site VPN Client en los siguientes pasos.

Para conectarse mediante el cliente proporcionado por AWS para Linux

1. Abra la aplicación Site-to-Site 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. Si desea crear varias conexiones, repita los pasos de Agregar perfil para cada archivo de configuración que desee agregar. Puede añadir tantos perfiles como desee, pero solo puede tener un máximo de cinco conexiones abiertas.
8. En la ventana Cliente de Site-to-Site VPN, elija el perfil al que desee conectarse y, a continuación, seleccione 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. Repita este paso para cada conexión de perfil que desee iniciar, conectando hasta cinco puntos de conexión simultáneos.

> **Note**
>
> Si algún perfil al que se conecta entra en conflicto con una sesión abierta actualmente, no podrá establecer la conexión. Elige una conexión nueva o desconéctese de la sesión que está causando el conflicto.

9. Para ver las estadísticas de una conexión, seleccione Conexión en la ventana Cliente de AWS VPN, seleccione Mostrar detalles y, a continuación, elija la conexión sobre la que desee ver detalles.
10. Para desconectar una conexión, elija una conexión en la ventana Cliente de AWS VPN y, a continuación, seleccione Desconectar. Si tiene varias conexiones abiertas, debe cerrar cada conexión individualmente.

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 uso y seguridad con cada versión. Le recomendamos encarecidamente que utilice la versión más reciente de cada plataforma. Las versiones anteriores pueden verse afectadas por problemas de and/or seguridad de usabilidad. Consulte las notas de la versión para obtener más detalles.

Versión	Cambios	Fecha	Enlace de descarga
5.3.2	• Pequeñas correcciones de errores y mejoras. • Posición de seguridad mejorada.	17 de diciembre de 2025	Descargue la versión 5.3.2 sha256:89 e4b9f2c9f 7def37167 f5f137f4ff9c6c5246 fd6e0a724 4b70c196a 17683569
5.3.1	• Pequeñas mejoras.	25 de septiembre de 2025	Descargue la versión 5.3.1

Versión	Cambios	Fecha	Enlace de descarga
			sha256: 4a426cc22 6382748d6 83a494634 0447dab87 ec4258397 7d9488ee4 5d11cdcec0
5.3.0	• Pequeñas mejoras. • Se agregó soporte para IPv6 conexione s.	14 de agosto de 2025	Descargue la versión 5.3.0 sha256: 31edb55f1 2dcd68a7a 4ca9b6233 ddbeebcd3 7e01f8765 5a520cc7e 7542bbfcb4
5.2.0	• Pequeñas mejoras. • Se ha agregado compatibilidad con Client Route Enforcement.	8 de abril de 2025	Descargue la versión 5.2.0 sha256: ef7189f08 5db30ef0c 521adcdfe c892075cb 005c8e001 4fdbcc590 218509891f

Versión	Cambios	Fecha	Enlace de descarga
5.1.0	• Se ha corregido un problema que provocaba que la AWS Client VPN versión 5.0.x se volviera a conectar automáticamente a la VPN tras un tiempo de espera por inactividad. • Pequeñas correcciones de errores y mejoras.	17 de marzo de 2025	Descargue la versión 5.1.0 sha256: 14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba
5.0.0	• Se ha agregado compatibilidad con conexiones simultáneas. • Se ha actualizado la interfaz gráfica de usuario. • Pequeñas correcciones de errores y mejoras.	21 de enero de 2025	Descargue la versión 5.0.0 sha256: 645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c
4.1.0	• Se ha agregado compatibilidad con Ubuntu 22.04 y 24.04. • Correcciones de errores.	12 de noviembre de 2024	Descargar la versión 4.1.0 sha256: 334d00222458fbfe9dade16c99fe97e9ebcbd51fff017d0d6b1d1b764e7af472

Versión	Cambios	Fecha	Enlace de descarga
4.0.0	Pequeñas mejoras.	25 de septiembre de 2024	Descarga de la versión 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Se ha agregado compatibilidad para el indicador `mssfix` OpenVPN.	4 de septiembre de 2024	Descarga de la versión 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2
3.15.0	• Se ha agregado compatibilidad para el indicador `tap-sleep` OpenVPN. • Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	12 de agosto de 2024	Descarga de la versión 3.15.0 sha256: 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012

Versión	Cambios	Fecha	Enlace de descarga
3.14.0	• Se han actualizado las bibliotecas de OpenVPN y OpenSSL.	29 de julio de 2024	Descarga de la versión 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3.13.0	• Vuelva a conectarse automáticamente cuando cambien los rangos de la red de área local.	21 de mayo de 2024	Descarga de 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	Descarga de la versión 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d

Versión	Cambios	Fecha	Enlace de descarga
3.12.1	• Se ha corregido una acción de desbordamiento de búfer que podía permitir a un actor local ejecutar comandos arbitrarios con permisos elevados. • Posición de seguridad mejorada.	16 de febrero de 2024	Descarga de la versión 3.12.1 sha256: 547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• Se han corregido los problemas de conectividad para algunas configuraciones de LAN.	19 de diciembre de 2023	Descargar la versión 3.12.0 sha256: 9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1
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: 86c0fa1bf1c97194082835a739ec7f1c87e540194955f414a35c679b94538970

Versión	Cambios	Fecha	Enlace de descarga
3.10.0	• 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 3.10.0 sha256: e7450b2490f3b96ab7d589a8000d838d9fd2adcdd72ae80666c4c0d900687e51
3.9.0	• Se ha corregido un problema de conectividad cuando NAT64 está 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

Versión	Cambios	Fecha	Enlace de descarga
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
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.

Versión	Cambios	Fecha	Enlace de descarga
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.
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.

Conéctese a un AWS Client VPN punto final mediante un cliente OpenVPN

Puede establecer una conexión con un punto de conexión de Client VPN mediante aplicaciones cliente de Open VPN comunes. Client VPN es compatible con los siguientes sistemas operativos:

- Windows

  Utilice un certificado y una clave privada del almacén de certificados de Windows. Una vez que haya generado el certificado y la clave, puede establecer una conexión de AWS cliente mediante la aplicación cliente GUI de OpenVPN o el cliente OpenVPN GUI Connect. Para conocer los pasos para crear el certificado y la clave, consulte Establecimiento de una conexión de VPN mediante un certificado en Windows.

- Android e iOS

  Establezca una conexión de VPN mediante la aplicación cliente de OpenVPN en un dispositivo móvil Android o iOS. Para obtener más información, consulte Conexiones de Client VPN en Android e iOS.

- macOS

  Establezca una conexión de VPN mediante un archivo de configuración para Tunnelblick basado en macOS o para AWS Client VPN. Para obtener más información, consulte Establecimiento de una conexión de VPN en macOS.

- Linux

  Establezca una conexión de VPN en Linux mediante la interfaz OpenVPN: administrador de red o la aplicación de OpenVPN. Para usar la interfaz OpenVPN: administrador de red, primero tendrá que instalar el módulo administrador de red si aún no está instalado. Para obtener más información, consulte Establecimiento de una conexión de VPN en 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. Esto incluye cualquier arquitectura basada en ARM. Si utiliza un dispositivo con un procesador ARM (como Apple Silicon Macs o dispositivos

Windows basados en ARM), debe utilizar puntos de conexión VPN basados en SAML con el AWS cliente proporcionado en lugar de clientes OpenVPN.

Aplicaciones cliente

- Conectarse a un AWS Client VPN punto final mediante una aplicación cliente de Windows
- AWS Client VPN conexiones en aplicaciones de Android e iOS
- Conectarse a un AWS Client VPN punto final mediante una aplicación cliente de macOS
- Conéctese a un AWS Client VPN punto final mediante una aplicación cliente OpenVPN

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

Estas secciones describen cómo establecer una conexión de VPN mediante 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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de conexiones AWS Client VPN con clientes basados en 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. Esto incluye cualquier arquitectura basada en ARM. Si utiliza un dispositivo con un procesador ARM (como Apple Silicon Macs o dispositivos Windows basados en ARM), debe utilizar puntos de conexión VPN basados en SAML con el AWS cliente proporcionado en lugar de clientes OpenVPN.

Tareas

- Use un certificado y establezca una conexión AWS Client VPN en Windows

Use un certificado y establezca una conexión AWS Client VPN en 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.

Uso de un certificado y establecimiento de una conexión

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.
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.

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

5. Después de completar la configuración, utilice OpenVPN para establecer una conexión de VPN al realizar una de las siguientes acciones:

   - Uso de la aplicación cliente de la interfaz gráfica de usuario de OpenVPN
     1. Inicie la aplicación cliente de OpenVPN.
     2. En la barra de tareas de Windows, elija Mostrar/ocultar iconos. Haga clic con el botón derecho en la Interfaz gráfica de usuario de OpenVPN y, a continuación, elija 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, elija Mostrar/ocultar iconos. Haga clic con el botón derecho en la Interfaz gráfica de usuario de OpenVPN y, a continuación, elija Conectar.

   - Uso del cliente de conexión de interfaz gráfica de usuario de OpenVPN
     1. Inicie la aplicación de OpenVPN y elija Importar, Desde archivo local….
     2. Desplácese hasta el archivo de configuración que recibió del administrador de VPN y elija Open (Abrir).

AWS Client VPN conexiones en aplicaciones de Android e 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. Esto incluye cualquier arquitectura basada en ARM. Si utiliza un dispositivo con un procesador ARM (como Apple Silicon Macs o dispositivos Windows basados en ARM), debe utilizar puntos de conexión VPN basados en SAML con el AWS cliente proporcionado en lugar de clientes OpenVPN.

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 acerca de la descarga y el uso de la aplicación cliente de 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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

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

Conectarse a un AWS Client VPN punto final mediante una aplicación cliente de macOS

En estas secciones se describe cómo establecer una conexión VPN mediante el cliente VPN basado en macOS, Tunnelblick o Client VPN.AWS

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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de conexiones AWS Client VPN con clientes 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. Esto incluye cualquier arquitectura basada en ARM. Si utiliza un dispositivo con un procesador ARM (como Apple Silicon Macs o dispositivos Windows basados en ARM), debe utilizar puntos de conexión VPN basados en SAML con el AWS cliente proporcionado en lugar de clientes OpenVPN.

Temas

Establecer una AWS Client VPN conexión en macOS

Puede 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.

Establecimiento de una conexión de VPN mediante Tunnelblick

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).

Para establecer una conexión VPN mediante AWS Client 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).

Conéctese a un AWS Client VPN punto final mediante una aplicación cliente OpenVPN

Estas secciones describen cómo establecer una conexión de VPN mediante OpenVPN: administrador de red u 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. Si desea conectarse a varios perfiles simultáneamente, necesitará un archivo de configuración para cada uno.

Para obtener información sobre la resolución de problemas, consulte Solución de problemas de conexiones AWS Client VPN con clientes basados en 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. Esto incluye cualquier arquitectura basada en ARM. Si utiliza un dispositivo con un procesador ARM (como Apple Silicon Macs o dispositivos Windows basados en ARM), debe utilizar puntos de conexión VPN basados en SAML con el AWS cliente proporcionado en lugar de clientes OpenVPN.

Temas

- Establezca una conexión en Linux AWS Client VPN

Establezca una conexión en Linux AWS Client VPN

Establezca una conexión de VPN mediante la interfaz gráfica de usuario del administrador de red en un equipo Ubuntu o la aplicación OpenVPN.

Establecimiento de una conexión de VPN mediante OpenVPN: administrador de red

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.

Establecimiento de una conexión de VPN mediante OpenVPN

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 conexiones AWS 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 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 Site-to-Site VPN Cliente en los siguientes pasos.

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

1. Abra la aplicación Site-to-Site 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 Site-to-Site 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 Site-to-Site 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 el portapapeles.

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

Solución de problemas de conexiones AWS Client VPN con clientes basados en 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.

AWS proporcionó los registros de eventos del cliente

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\Site-to-Site VPN Client\WinServiceLogs\username
```

Temas de solución de problemas

- El cliente no puede establecer conexión
- El cliente no se puede conectar con el mensaje de registro “no hay adaptadores TAP-Windows”
- El cliente está atascado en un estado de reconexión
- El proceso de conexión de la VPN se cierra inesperadamente
- La aplicación no se inicia

- El cliente no puede crear el perfil
- La VPN se desconecta con un mensaje emergente
- Se produce un bloqueo del cliente en Dell que PCs utiliza Windows 10 u 11
- Interfaz gráfica de usuario de OpenVPN
- Cliente de conexión de OpenVPN
- No se puede resolver el DNS
- Falta el alias PKI

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.

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 de 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
```

Se produce un bloqueo del cliente en Dell que PCs utiliza 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 cuando se navega por el sistema de archivos para importar un archivo de configuración de la VPN. 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 siguientes DLLs:

- 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. 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.

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

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

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 conexiones AWS Client VPN 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.

AWS proporcionó los registros de eventos del cliente

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

```
/var/log/AWSVPNClient/AcvcHelperErrLog.txt
/var/log/AWSVPNClient/AcvcHelperOutLog.txt
```

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

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

Temas de solución de problemas

- El cliente no puede establecer conexión
- El cliente está atascado en un estado de reconexión
- El cliente no puede crear el perfil
- Se necesita una herramienta de ayuda para el error
- Tunnelblick
- Algoritmo de cifrado 'AES-256-GCM' no encontrado
- La conexión deja de responder y se restablece
- Uso extendido de claves (EKU)
- Certificado caducado
- OpenVPN
- No se puede resolver el DNS

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 para el error

Problema

Obtiene el siguiente error cuando intenta conectar la VPN.

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

Solución

Consulta el siguiente artículo en AWS Re:post. AWS VPN Client - Helper tool is required error

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. Seleccione 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 conexiones AWS Client VPN 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 proporcionó los registros de eventos del cliente
- Las consultas de DNS van a un servidor de nombres predeterminado

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

AWS proporcionó los registros de eventos del cliente

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/
```

Por ejemplo, puede comprobar los siguientes archivos de registro para encontrar errores en los up/down scripts de DNS que provoquen un error en la conexión:

- `/var/log/aws-vpn-client/configure-dns-up.log`
- `/var/log/aws-vpn-client/configure-dns-down.log`

Las consultas de DNS van a un servidor de nombres predeterminado

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
   ```

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

Solución de problemas comunes de AWS Client VPN

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 lanzamiento del cliente proporcionado (5.3.3) para macOS ARM64 y x64	Consulte las notas de la versión para obtener más detalles.	26 de diciembre de 2025
AWS Publicado el cliente proporcionado (5.3.2) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	17 de diciembre de 2025
AWS Lanzamiento del cliente proporcionado (5.3.2) para macOS x64	Consulte las notas de la versión para obtener más detalles.	27 de octubre de 2025
AWS lanzamiento del cliente proporcionado (5.3.2) para ARM64 sistemas macOS	Ahora se ha añadido soporte para los sistemas operativos ARM64 basados en macOS. Esto incluye una descarga de AWS Client VPN la nueva versión 5.3.2 específica para ARM64 sistemas macOS. Consulte Requisitos de Client VPN para macOS para obtener más información y las Notas de la versión de AWS Client VPN para macOS sobre el enlace de descarga.	27 de octubre de 2025
AWS Publicado el cliente suministrado (5.3.1) para Windows x64 y Arm64	Consulte las notas de la versión para obtener más detalles.	30 de septiembre de 2025

AWS El cliente proporcionado para macOS ahora es compatible con Tahoe (26.0)	Consulte los requisitos para obtener más información.	25 de septiembre de 2025
AWS Lanzamiento del cliente proporcionado (5.3.1) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	25 de septiembre de 2025
AWS Lanzamiento del cliente proporcionado (5.3.1) para macOS	Consulte las notas de la versión para obtener más detalles.	9 de septiembre de 2025
AWS Se lanzó el cliente proporcionado (5.3.0) para los sistemas Windows Arm64	Se ha añadido compatibilidad con los sistemas operativos basados en Arm64 de Windows. Se incluye la descarga de una nueva versión 5.3.0 de AWS Client VPN específica para sistemas Arm64 de Windows. Consulte Requisitos de Client VPN para Windows para obtener más información y las Notas de la versión de AWS Client VPN para Windows sobre el enlace de descarga.	26 de agosto de 2025
AWS Lanzamiento del cliente proporcionado (5.3.0) para macOS	Consulte las notas de la versión para obtener más detalles.	14 de agosto de 2025
AWS Se lanzó el cliente proporcionado (5.3.0) para Windows	Consulte las notas de la versión para obtener más detalles.	14 de agosto de 2025
AWS Publicado el cliente proporcionado (5.3.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	14 de agosto de 2025

AWS Lanzamiento del cliente proporcionado (5.2.1) para macOS	Consulte las notas de la versión para obtener más detalles.	18 de junio de 2025
AWS Se lanzó el cliente proporcionado (5.2.2) para Windows	Consulte las notas de la versión para obtener más detalles.	2 de junio de 2025
AWS Publicado el cliente proporcionado (5.2.1) para Windows	Consulte las notas de la versión para obtener más detalles.	21 de abril de 2025
AWS Lanzamiento del cliente proporcionado (5.2.0) para macOS	Consulte las notas de la versión para obtener más detalles.	8 de abril de 2025
AWS Se lanzó el cliente proporcionado (5.2.0) para Windows	Consulte las notas de la versión para obtener más detalles.	8 de abril de 2025
AWS Publicado el cliente proporcionado (5.2.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	8 de abril de 2025
AWS Lanzamiento del cliente proporcionado (5.1.0) para macOS	Consulte las notas de la versión para obtener más detalles.	17 de marzo de 2025
AWS Se lanzó el cliente proporcionado (5.1.0) para Windows	Consulte las notas de la versión para obtener más detalles.	17 de marzo de 2025
AWS Publicado el cliente proporcionado (5.1.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	17 de marzo de 2025

Se ha eliminado la compatibilidad con macOS Monterey y se ha añadido compatibilidad con macOS Sonoma (14.0)	Consulte Requisitos de Client VPN para macOS para obtener más información.	12 de marzo de 2025
Se ha eliminado la compatibilidad con Ubuntu 18.0.4 (LTS) y Ubuntu 20.04 LTS (únicamente) AMD64	Consulte Requisitos de Client VPN para Linux para obtener más información.	12 de marzo de 2025
AWS Lanzamiento del cliente proporcionado (5.0.3) para macOS	Consulte las notas de la versión para obtener más detalles.	6 de marzo de 2025
AWS Se lanzó el cliente proporcionado (5.0.2) para Windows	Consulte las notas de la versión para obtener más detalles.	24 de febrero de 2025
AWS Lanzamiento del cliente proporcionado (5.0.2) para macOS	Consulte las notas de la versión para obtener más detalles.	17 de febrero de 2025
AWS Se lanzó el cliente proporcionado (5.0.1) para Windows	Consulte las notas de la versión para obtener más detalles.	30 de enero de 2025
AWS Lanzamiento del cliente proporcionado (5.0.1) para macOS	Consulte las notas de la versión para obtener más detalles.	22 de enero de 2025
El cliente AWS proporcionado ahora admite hasta cinco conexiones simultáneas	Consulte Support for concurrent connections using a client AWS provided for details for details.	21 de enero de 2025
AWS Lanzamiento del cliente proporcionado (5.0.0) para macOS	Consulte las notas de la versión para obtener más detalles.	21 de enero de 2025

AWS Se lanzó el cliente proporcionado (5.0.0) para Windows	Consulte las notas de la versión para obtener más detalles.	21 de enero de 2025
AWS Publicado el cliente proporcionado (5.0.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	12 de noviembre de 2024
AWS Lanzamiento del cliente proporcionado (4.1.0) para macOS	Consulte las notas de la versión para obtener más detalles.	12 de noviembre de 2024
AWS Publicado el cliente proporcionado (4.1.0) para Windows	Consulte las notas de la versión para obtener más detalles.	12 de noviembre de 2024
AWS Publicado el cliente proporcionado (4.1.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	12 de noviembre de 2024
AWS Lanzamiento del cliente proporcionado (4.0.0) para macOS	Consulte las notas de la versión para obtener más detalles.	25 de septiembre de 2024
AWS Publicado el cliente proporcionado (4.0.0) para Windows	Consulte las notas de la versión para obtener más detalles.	25 de septiembre de 2024
AWS Publicado el cliente proporcionado (4.0.0) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	25 de septiembre de 2024
AWS Publicado el cliente proporcionado (3.15.1) para Ubuntu	Consulte las notas de la versión para obtener más detalles.	4 de septiembre de 2024
AWS Publicado el cliente proporcionado (3.14.2) para Windows	Consulte las notas de la versión para obtener más detalles.	4 de septiembre de 2024

AWS Lanzamiento del cliente proporcionado (3.12.1) para macOS	Consulte las notas de la versión para obtener más detalles.	4 de septiembre de 2024
AWS Publicado el cliente proporcionado (3.14.1) para Windows	Consulte las notas de la versión para obtener más detalles.	22 de agosto de 2024
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 Publicado 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.