Benutzer-Leitfaden

AWS Client-VPN

AWS Client-VPN: Benutzer-Leitfaden

Table of Contents

Was ist AWS Client VPN?

AWS Client VPN ist ein verwalteter clientbasierter VPN-Dienst, mit dem Sie sicher auf AWS Ressourcen und Ressourcen in Ihrem lokalen Netzwerk zugreifen können.

Diese Anleitung enthält Schritte zum Herstellen einer VPN-Verbindung zu einem Client-VPN-Endpunkt mithilfe einer Client-Anwendung auf Ihrem Gerät.

Client-VPN-Komponenten

Im Folgenden sind die wichtigsten Komponenten für die Verwendung von AWS Client VPN.

- Client-VPN-Endpunkt — Ihr Client-VPN-Administrator erstellt und konfiguriert einen Client-VPN-Endpunkt in AWS. Ihr Administrator bestimmt, auf welche Netzwerke und Ressourcen Sie zugreifen können, wenn Sie eine VPN-Verbindung herstellen.
- VPN-Client-Anwendung – die Software-Anwendung, mit der Sie eine Verbindung mit dem Client-VPN-Endpunkt herstellen und eine sichere VPN-Verbindung einrichten.
- Client-VPN-Endpunktkonfigurationsdatei – eine Konfigurationsdatei, die Ihnen vom Client-VPN-Administrator zur Verfügung gestellt wird. Die Datei enthält Informationen über den Client-VPN-Endpunkt und die Zertifikate, die für den Aufbau einer VPN-Verbindung erforderlich sind. Sie laden diese Datei in die von Ihnen gewählte VPN-Client-Anwendung. Mit dem AWS bereitgestellten Client können Sie eine Verbindung zu fünf gleichzeitigen Sitzungen herstellen, wobei jede Sitzung über eine eigene Konfigurationsdatei verfügt, die vom Client-VPN-Administrator bereitgestellt wird. Weitere Hinweise zu gleichzeitigen Sitzungen finden Sie unter. Support für gleichzeitige Verbindungen

Zusätzliche Ressourcen für die Konfiguration von Client VPN

Wenn Sie ein Client-VPN-Administrator sind, finden Sie im AWS Client VPN Administratorhandbuch weitere Informationen zum Erstellen und Konfigurieren eines Client-VPN-Endpunkts.

Fangen Sie an mit AWS Client VPN

Bevor Sie eine VPN-Sitzung einrichten können, muss Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellen und konfigurieren. Ihr Administrator legt fest, auf welche Netzwerke und Ressourcen Sie zugreifen können, wenn Sie eine VPN-Sitzung einrichten. Anschließend stellen Sie mit einer VPN-Client-Anwendung eine Verbindung mit einem Client VPN-Endpunkt her und bauen eine sichere VPN-Verbindung auf.

Falls Sie ein Administrator sind, der einen Client-VPN-Endpunkt erstellen muss, finden Sie weitere Informationen im AWS Client VPN -Administratorhandbuch.

Topics

Voraussetzungen für die Verwendung von Client VPN

Zum Herstellen einer VPN-Verbindung ist Folgendes erforderlich:

- Zugriff auf das Internet
- Ein unterstütztes Gerät
- Eine unterstützte Version von Windows, macOS oder Linux.
- Für Client VPN-Endpunkte, die eine SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, einer der folgenden Browser:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Schritt 1: Herunterladen einer VPN-Clientanwendung

Sie können eine Verbindung mit einem Client VPN-Endpunkt herstellen und eine VPN-Verbindung mit dem von AWS bereitgestellten Client oder einer anderen OpenVPN-basierten Client-Anwendung herstellen.

Sie können die Client-VPN-Anwendung mit einer von zwei Methoden herunterladen, je nachdem, ob der Administrator die Endpunktkonfigurationsdatei für die Anwendung erstellt hat:

- Wenn Ihr Administrator keine Endpunktkonfigurationsdateien eingerichtet hat, laden Sie den Client über den AWS Client-VPN-Download herunter und installieren Sie ihn. Nachdem Sie die Anwendung heruntergeladen und installiert haben, fahren Sie mit the section called “Schritt 2: Abrufen der Client VPN-Endpunkt-Konfigurationsdatei” dem Abrufen der Endpunktkonfigurationsdatei von Ihrem Administrator fort. Wenn Sie eine Verbindung zu mehreren Profilen herstellen, benötigen Sie für jedes Profil eine Konfigurationsdatei.
- Wenn Ihr Administrator die Endpunktkonfigurationsdatei bereits vorkonfiguriert hat, können Sie die Client VPN VPN-Anwendung zusammen mit der Konfigurationsdatei vom Self-Service-Portal herunterladen. Die Schritte zum Herunterladen des Clients und der Konfigurationsdatei vom Self-Service-Portal finden Sie unter. the section called “Client VPN herunterladen” Nachdem Sie die Anwendung und Datei heruntergeladen und installiert haben, gehen Sie zuthe section called “Schritt 3: Verbinden mit dem VPN”.

Laden Sie alternativ eine OpenVPN-Clientanwendung auf das Gerät herunter, über das Sie eine VPN-Verbindung einrichten möchten. Installieren Sie dann die Anwendung.

Schritt 2: Abrufen der Client VPN-Endpunkt-Konfigurationsdatei

Sie erhalten die Konfigurationsdatei für den Client-VPN-Endpunkt von Ihrem Administrator. Die Konfigurationsdatei enthält die Informationen über den Client VPN-Endpunkt sowie die Zertifikate, die für das Einrichten einer VPN-Verbindung erforderlich sind.

Wenn Ihr Client-VPN-Administrator ein Self-Service-Portal für den Client-VPN-Endpunkt konfiguriert hat, können Sie alternativ die neueste Version des AWS bereitgestellten Clients und die neueste Version der Client-VPN-Endpunktkonfigurationsdatei selbst herunterladen. Weitere Informationen finden Sie unter Laden Sie das AWS Client VPN vom Self-Service-Portal herunter.

Schritt 3: Verbinden mit dem VPN

Importieren Sie die Client-VPN-Endpunktkonfigurationsdatei in den AWS bereitgestellten Client oder in Ihre OpenVPN-Clientanwendung und stellen Sie eine Verbindung zum VPN her. Schritte zum Herstellen einer Verbindung mit einem VPN, einschließlich des Imports einer oder mehrerer Endpunktkonfigurationsdateien für einen AWS bereitgestellten Client, finden Sie in den folgenden Themen:

- Stellen Sie mithilfe eines AWS bereitgestellten Clients eine Verbindung zu einem AWS Client VPN Endpunkt her
- Connect zu einem her AWS Client VPN Endpunkt, der einen OpenVPN-Client verwendet

Bei Client VPN-Endpunkten, die die Active Directory-Authentifizierung verwenden, werden Sie aufgefordert, Ihren Benutzernamen und Ihr Passwort einzugeben. Wenn Multi-Factor Authentication (MFA) für das Verzeichnis aktiviert wurde, werden Sie außerdem aufgefordert, Ihren MFA-Code einzugeben.

Für Client-VPN-Endpunkte, die SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, öffnet der AWS bereitgestellte Client ein Browserfenster auf Ihrem Computer. Sie werden aufgefordert, Ihre Unternehmensanmeldeinformationen einzugeben, bevor Sie eine Verbindung mit dem Client VPN-Endpunkt herstellen können.

Laden Sie das AWS Client VPN vom Self-Service-Portal herunter

Das Self-Service-Portal ist eine Webseite, auf der Sie die neueste Version des AWS bereitgestellten Clients und die neuesten Versionen der Client-VPN-Endpunktkonfigurationsdateien herunterladen können. Wenn Ihr Client-VPN-Endpunktadministrator eine oder mehrere Konfigurationsdateien für den Client VPN vorkonfiguriert hat, können Sie diese Client-VPN-Anwendung zusammen mit diesen Konfigurationsdateien von diesem Portal herunterladen und installieren.

> **Note**
>
> Wenn Sie Administrator sind und das Self-Service-Portal konfigurieren möchten, finden Sie im AWS Client VPN Administratorhandbuch weitere Informationen unter Client-VPN-Endpunkte.

Bevor Sie beginnen, benötigen Sie die ID jedes Client-VPN-Endpunkts, den Sie herunterladen möchten. Ihr Client-VPN-Endpunktadministrator kann Ihnen die ID zur Verfügung stellen oder Ihnen eine Self-Service-Portal-URL geben, die die ID enthält. Für Verbindungen mit mehreren Endpunkten benötigen Sie die Endpunkt-ID für jedes Profil, mit dem Sie eine Verbindung herstellen möchten.

So greifen Sie auf das Self-Service-Portal zu

1. Rufen Sie das Self-Service-Portal unter https://self-service.clientvpn.amazonaws.com/auf, oder verwenden Sie die URL, die Sie von Ihrem Administrator erhalten haben.
2. Geben Sie bei Bedarf die ID des Client-VPN-Endpunkts ein, z. B, `cvpn-endpoint-0123456abcd123456`. Wählen Sie Weiter aus.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und wählen Sie Sign In (Anmelden). Dies ist derselbe Benutzername und dasselbe Passwort, das Sie für die Verbindung mit dem Client-VPN-Endpunkt verwenden.
4. Im Self-Service-Portal haben Sie folgende Möglichkeiten:
   - Laden Sie die neueste Version der Client-Konfigurationsdatei für den Client-VPN-Endpunkt herunter. Wenn Sie eine Verbindung zu mehreren Endpunkten herstellen möchten, müssen Sie die Konfigurationsdatei für jeden Endpunkt herunterladen.
   - Laden Sie die neueste Version des AWS bereitgestellten Clients für Ihre Plattform herunter.
5. Wiederholen Sie diese Schritte für jede Endpunktkonfigurationsdatei, für die Sie ein Verbindungsprofil erstellen möchten.

Stellen Sie mithilfe eines AWS bereitgestellten Clients eine Verbindung zu einem AWS Client VPN Endpunkt her

Sie können mit dem AWS bereitgestellten Client, der unter Windows, macOS und Ubuntu unterstützt wird, eine Verbindung zu einem Client-VPN-Endpunkt herstellen. Der AWS bereitgestellte Client unterstützt außerdem bis zu fünf gleichzeitige Verbindungen sowie OpenVPN-Direktiven.

Topics

Sicherheit

Sicherheit hat im AWS bereitgestellten Client höchste Priorität. Wir veröffentlichen regelmäßig Patches, um den Sicherheitsstatus der Anwendung zu verbessern. Der von AWS bereitgestellte Client bietet im Vergleich zu anderen OpenVPN-Clients mehrere einzigartige Sicherheitsfunktionen, darunter SAML-Authentifizierung, Client Routes Enforcement und Überwachung der Geräteeinstellungen.

Der AWS bereitgestellte Client ist zwar darauf ausgelegt, Bedrohungen abzuwehren, die von einer falsch konfigurierten oder kompromittierten Netzwerkumgebung ausgehen, er ist jedoch nicht dafür verantwortlich, die Umgebung zu ändern oder externe Bedrohungen an ihrer Quelle zu beseitigen. Der AWS bereitgestellte Client ist darauf angewiesen, dass der Kunde für eine sichere und gut konfigurierte Umgebung sorgt. Dies umfasst:

- Verhinderung unbefugter Änderungen oder missbräuchlicher Nutzung durch lokale Benutzer
- Beschränkung der Administratorrechte auf vertrauenswürdige Benutzer
- Wartung von up-to-date Sicherheitspatches

Support für gleichzeitige Verbindungen mit einem AWS bereitgestellten Client

Der AWS bereitgestellte Client ermöglicht die Verbindung zu mehreren gleichzeitigen Sitzungen. Dies ist hilfreich, wenn Sie Zugriff auf Ressourcen in mehreren AWS Umgebungen benötigen

und unterschiedliche Endpunkte für diese Ressourcen haben. Beispielsweise benötigen Sie möglicherweise Zugriff auf eine Datenbank in einer Umgebung an einem Endpunkt, der sich von dem Endpunkt unterscheidet, mit dem Sie derzeit verbunden sind, aber Sie möchten die aktuelle Verbindung nicht trennen. Damit der von Ihnen AWS angegebene Client eine Verbindung zu aktuellen Sitzungen herstellen kann, laden Sie die Konfigurationsdatei herunter, die Ihr Administrator für jeden Endpunkt erstellt hat, und erstellen Sie anschließend für jede Datei ein Verbindungsprofil. Mithilfe des AWS bereitgestellten Clients können Sie dann eine Verbindung zu mehreren Sitzungen herstellen, ohne die Verbindung zu einer derzeit geöffneten Sitzung zu trennen. Dies wird nur für die AWS bereitgestellten Clients unterstützt. Die Schritte zum Herstellen einer Verbindung zu gleichzeitigen Sitzungen finden Sie im Folgenden:

- Connect mit dem AWS bereitgestellten Client für Windows her
- Connect mit dem AWS bereitgestellten Client für macOS her
- Connect mit dem AWS bereitgestellten Client für Linux her

Wenn Sie eine Verbindung zu mehreren Endpunkten herstellen, führt Client VPN Prüfungen durch, um sicherzustellen, dass es keine Konflikte mit anderen offenen Endpunktverbindungen gibt — zum Beispiel, wenn zwei Sitzungen widersprüchliche CIDR-Blöcke oder Routing-Richtlinien haben oder wenn Sie bereits mit einer vollständigen Tunnelverbindung verbunden sind. Wenn bei der Überprüfung Konflikte festgestellt werden, wird eine Verbindung erst hergestellt, wenn Sie entweder eine andere Verbindung wählen, die nicht im Konflikt mit der offenen Verbindung steht, oder Sie die Verbindung zu der offenen Sitzung trennen, die den Konflikt verursacht.

Gleichzeitige DNS-Verbindungen sind zulässig. Der DNS-Server einer der DNS-fähigen Verbindungen wird angewendet. Je nach DNS-Server werden Sie bei der Wiederverbindung möglicherweise zur Authentifizierung aufgefordert.

> **Note**
>
> Die maximale Anzahl an zulässigen gleichzeitigen Sitzungen beträgt fünf.

OpenVPN-Richtlinien

Der AWS bereitgestellte Client unterstützt die folgenden OpenVPN-Direktiven. Weitere Informationen zu diesen Richtlinien finden Sie in der Dokumentation auf der OpenVPN-Website.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- block-outside-dns
- ca
- cert
- cipher
- Client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive
- Schlüssel
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- Ping-Ausgang
- ping-restart
- proto
- pull

- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- Route
- route-ipv6
- server-poll-timeout
- static-challenge
- Tippen Sie auf Sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN für Windows

In diesen Abschnitten wird beschrieben, wie Sie mit dem AWS bereitgestellten Client eine VPN-Verbindung für Windows x64- und Windows Arm64-Systeme herstellen. Sie können den Client unter AWS Client VPN-Download herunterladen und installieren. Der AWS bereitgestellte Client unterstützt keine automatischen Updates.

Voraussetzungen

Der AWS bereitgestellte Client unterstützt sowohl Windows x64- als auch Arm64-Systeme. Folgendes ist für jedes Betriebssystem erforderlich:

Windows Arm64-Betriebssysteme

- Windows 11 (64-Bit-Betriebssystem, Arm64-Prozessor)
- .NET Framework 4.8.1 oder höher

> **Note**
>
> Diese Anwendung enthält Hintergrundprozesse, die die Arm64-Emulation verwenden. Dies wird auf Windows 11-Arm64-Geräten standardmäßig vollständig unterstützt und aktiviert, sodass ein reibungsloser Betrieb ohne zusätzliche Einrichtung gewährleistet ist. Weitere Informationen finden Sie unter So funktioniert die Emulation auf Arm.

Windows x64-Betriebssysteme

- Windows 11 (64-Bit-Betriebssystem, x64-Prozessor)
- .NET Framework 4.7.2 oder höher

> **Note**
>
> Sowohl für Windows x64- als auch für Arm64-Betriebssysteme, Client-VPN-Endpunkte, die SAML-based Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client die TCP-Ports 8096-8115 auf Ihrem Computer.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie eine Verbindung zu mehreren Profilen gleichzeitig herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Themen

- Connect to (Verbinden mit) AWS Client VPN mit einem AWS bereitgestellter Client für Windows
- Softwarekompatibilität für Endpunktsicherheit
- AWS Client VPN für Windows-Versionshinweise

Connect to (Verbinden mit) AWS Client VPN mit einem AWS bereitgestellter Client für Windows

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Anforderungen gelesen haben. Der AWS bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN-Client bezeichnet.

Um eine Verbindung mit dem herzustellen AWS bereitgestellter Client für Windows x64- oder Arm64-based Windows-Systeme:

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.
3. Wählen Sie Add Profile (Profil hinzufügen) aus.
4. Geben Sie für Display name (Anzeigelname) einen Namen für das Profil ein.
5. Wählen Sie unter VPN Configuration File (VPN-Konfigurationsdatei) die Konfigurationsdatei aus, die Sie von Ihrem Client VPN-Administrator erhalten haben. Wählen Sie dann Add Profile (Profil hinzufügen) aus.
6. Wenn Sie mehrere Verbindungen erstellen möchten, wiederholen Sie die Schritte zum Hinzufügen von Profilen für jede Konfigurationsdatei, die Sie hinzufügen möchten. Sie können so viele Profile hinzufügen, wie Sie möchten, aber Sie können nur bis zu fünf offene Verbindungen haben.
7. Wählen Sie im AWS VPN-Client-Fenster das Profil aus, mit dem Sie Connect möchten, und wählen Sie dann Verbinden aus. Wenn der Client VPN-Endpunkt für die Verwendung der auf Anmeldeinformationen basierenden Authentifizierung konfiguriert wurde, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wiederholen Sie diesen Schritt für jede Profilverbindung, die Sie initiieren möchten, und verbinden Sie bis zu fünf Endpunkte gleichzeitig.

   > **Note**
   >
   > Wenn ein Profil, mit dem Sie eine Verbindung herstellen, Konflikte mit einer aktuell geöffneten Sitzung aufweist, können Sie die Verbindung nicht herstellen. Wählen Sie entweder eine neue Verbindung oder trennen Sie die Verbindung zu der Sitzung, die den Konflikt verursacht hat.

8. Um Statistiken für eine Verbindung anzuzeigen, wählen Sie im AWS VPN-Client-Fenster Verbindung aus, wählen Sie Details anzeigen und wählen Sie dann die Verbindung aus, zu der Sie Details sehen möchten.
9. Um eine Verbindung zu trennen, wählen Sie im AWS VPN-Client-Fenster eine Verbindung aus und klicken Sie dann auf Trennen. Wenn Sie mehrere offene Verbindungen haben, müssen Sie jede Verbindung einzeln schließen. Alternativ wählen Sie das Client-Symbol in der Windows-Taskleiste und dann Disconnect (Trennen) aus.

Softwarekompatibilität für Endpunktsicherheit

Endpunktsicherheitsprodukte für Unternehmen wie hostbasierte Firewalls, EDR-Agenten (Endpoint Detection and Response) und Antivirensoftware können manchmal AWS Client-VPN-Verbindungen stören. Wenn bei der Verwendung des AWS bereitgestellten Clients für Windows Verbindungsprobleme auftreten, müssen Sie möglicherweise Ausnahmen in Ihrer Endpunktsicherheitssoftware konfigurieren.

AWS Ausführbare Pfade für Client VPN

Der AWS bereitgestellte Client für Windows installiert die folgenden wichtigen ausführbaren Dateien. Möglicherweise benötigen Sie diese Pfade, wenn Sie Firewallregeln, Zulassungslisten für Anwendungen oder Sicherheitsrichtlinien für Endgeräte konfigurieren.

VPN-Client-Anwendung

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

OpenVPN-Prozess

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

Dies ist der Kernprozess, der die VPN-Tunnelverbindung herstellt und aufrechterhält.

Windows-Dienst

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

Netzwerkanforderungen

Der AWS bereitgestellte Client benötigt ausgehenden Netzwerkzugriff auf den Client-VPN-Endpunkt, um eine VPN-Verbindung herzustellen. Stellen Sie sicher, dass Ihre Firewall oder Endpunktsicherheitssoftware ausgehenden Datenverkehr vom `acvc-openvpn.exe` Prozess zum Port und Protokoll zulässt, die auf Ihrem Client-VPN-Endpunkt konfiguriert sind.

Konfiguration von Ausnahmen für die Endpunktsicherheit

Wenn Ihr Endpoint Security-Produkt die AWS bereitgestellte Client-Konnektivität beeinträchtigt, überprüfen Sie mit Ihrem Sicherheitsadministrator die folgenden Ausschlusskategorien:

Process-based Ausschlüsse

Fügen Sie die in aufgeführten ausführbaren Dateien the section called “AWS Ausführbare Pfade für Client VPN” zur Liste der zulässigen Prozesse oder der Ausschlussliste Ihres Endpoint Security-Produkts hinzu.

Network-based Ausschlüsse

Erlauben Sie ausgehenden Datenverkehr vom `acvc-openvpn.exe` Prozess zum Port und Protokoll Ihres Client-VPN-Endpunkts.

Path-based Ausschlüsse

Schließen Sie das AWS angegebene Client-Installationsverzeichnis von der Echtzeitsuche oder Verhaltensanalyse aus:

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

Important

Präskriptive Konfigurationsanweisungen für bestimmte Endpunktsicherheitsprodukte von Drittanbietern fallen aufgrund der unterschiedlichen Produktversionen und Konfigurationen nicht in den Umfang der AWS Dokumentation. Detaillierte Anweisungen zur Konfiguration von Ausnahmen für Ihr spezielles Produkt finden Sie in der Dokumentation Ihres Endpoint Security-Anbieters.

AWS Client VPN für Windows-Versionshinweise

Die folgende Tabelle enthält die Versionshinweise und Download-Links für die aktuelle und frühere Version von AWS Client VPN für Windows x64- und Windows ARM64-basierte Systeme.

Note

Wir bieten weiterhin mit jeder Version Verbesserungen in Bezug auf Benutzerfreundlichkeit und Sicherheit. Wir empfehlen dringend, für jede Plattform die neueste Version zu verwenden. Frühere Versionen können von Problemen mit der Benutzerfreundlichkeit und and/or Sicherheit betroffen sein. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Date	Link herunterladen und SHA256
5.3.4 (x64 und Arm64)	• Kleinere Fehlerbehebungen und Verbesserungen • Verbesserter Sicherheitsstatus	27. März 2026	• Laden Sie Windows x64 Version 5.3.4 herunter sha256:81 a5c510162 4c5f74de8 afdcb816f 03ea8ff9e 8c6a5eaa8 890a95779 a94dbe41 • Laden Sie Windows Arm64 Version 5.3.4 herunter sha256:34 10282ebb0 24e64812a 63668b301 17657d470 ed4c51f05 e96fc812b 8871587d
5.3.3 (x64 und Arm64)	• Verbindungsfehler in Version 5.3.2 wurden behoben	28. Februar 2026	• Laden Sie Windows x64 Version 5.3.3 herunter

Version	Änderungen	Date	Link herunterladen und SHA256
			sha256: bbaebb977 b270add64 97c941505 fed5913b5 8056e980e 372170733 7dc051ac86 • Laden Sie Windows Arm64 Version 5.3.3 herunter sha256: c30b6d012 1a5070643 fdbebc27e 7f9569d57 4a5698631 480becb5c b96cac9fde

Version	Änderungen	Date	Link herunterladen und SHA256
5.3.2 (x64 und Arm64)	• Kleinere Fehlerbehebungen und Verbesserungen. • Verbesserter Sicherheitsstatus.	17. Februar 2026	• Laden Sie Windows x64 Version 5.3.2 herunter sha256: dd1e4fb67 18dddbf13 a5aee5421 75761bf8e d854290c5 76a488b98 173a0ccf92 • Laden Sie Windows Arm64 Version 5.3.2 herunter sha256: d2d18d91c a9ef53cc5 57434db18 ef5d0002e 7825a998f 2d739eac4 43b034af00

Version	Änderungen	Date	Link herunterladen und SHA256
5.3.1 (x64 und Arm64)	Kleinere Fehlerbehebungen und Verbesserungen.	30. September 2025	• Laden Sie Windows x64 Version 5.3.1 herunter sha256: b71ddbc78230630963acf3ebba7afeb6e52599843091ff589aed6afce4c9eb06 • Laden Sie Windows Arm64 Version 5.3.1 herunter sha256: e691bdb0bdcb55b3da36f4fb2e5198f20f1878dc22a00bf55bc660999698500b

Version	Änderungen	Date	Link herunterladen und SHA256
5.3.0 (Arm64)	Neue AWS Client VPN Unterstützung für Windows ARM64-basierte Betriebssysteme. Diese Version enthält alle Updates der Version Windows (x64) 5.3.0.	26. August 2025	Laden Sie Windows Arm64 Version 5.3.0 herunter sha256:3f1be6b487af8307dafbb0f7737cd597cf71dc64dcd31775aeeebf91d04b8dce
5.3.0	• Kleinere Verbesserungen. • Unterstützung für IPv6 Verbindungen hinzugefügt	14. August 2025	Laden Sie Windows x64 Version 5.3.0 herunter sha256: e3cf1aff6e14d79aa44378229a3a0602a9e9c2a0c6d0d055df901440b6d1454a

Version	Änderungen	Date	Link herunterladen und SHA256
5.2.2	Verbesserter Sicherheitsstatus.	2. Juni 2025	Version 5.2.2 herunterladen sha256: f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	• Unterstützung für das `ping-exit` OpenVPN-Flag hinzugefügt. • Die OpenSSL-Bibliothek wurde aktualisi ert. • Kleinere Fehlerbehebungen und Verbesserungen.	21. April 2025	Nicht mehr unterstützt.
5.2.0	• Kleinere Verbesserungen. • Unterstützung für Client Route Enforce hinzugefügt.	8. April 2025	Nicht mehr unterstützt.
5.1.0	• Es wurde ein Problem behoben, das dazu führte, dass AWS Client VPN Version 5.0.x nach einer Unterbrechung des Inaktivitäts-Timeouts automatis ch wieder eine Verbindung zum VPN herstellte. • Kleinere Fehlerbehebungen und Verbesserungen.	17. März 2025	Nicht mehr unterstützt.

Version	Änderungen	Date	Link herunterladen und SHA256
5.0.2	• Ein DNS-Problem für gleichzeitige Verbindungen wurde behoben. • Sporadische Probleme bei der Installation neuer TAP-Adapter wurden behoben.	24. Februar 2025	Nicht mehr unterstützt.
5.0.1	Es wurde ein Problem behoben, das zu sporadischen VPN-Verbindungsfehlern auf der Windows-Client-Version 5.0.0 führte.	30. Januar 2025	Nicht mehr unterstützt.
5.0.0	• Unterstützung für gleichzeitige Verbindungen hinzugefügt. • Die TAP-Treiberversion wurde aktualisiert. • Die grafische Benutzeroberfläche wurde aktualisiert. • Kleinere Fehlerbehebungen und Verbesserungen	21. Januar 2025	Nicht mehr unterstützt.
4.1.0	Kleinere Fehlerbehebungen und Verbesserungen.	12. November 2024	Nicht mehr unterstützt.
4.0.0	Kleinere Verbesserungen.	25. September 2024	Version 4.0.0 herunterladen sha256:6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc

Version	Änderungen	Date	Link herunterladen und SHA256
3,14,2	Unterstützung für das `mssfix` OpenVPN-Flag hinzugefügt.	4. September 2024	Laden Sie Version 3.14.2 herunter sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3,14,1	Kleinere Fehlerbehebungen und Verbesserungen.	22. August 2024	Version 3.14.1 herunterladen sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3,14.0	• Unterstützung für das `tap-sleep` OpenVPN-Flag hinzugefügt. • Die OpenVPN- und OpenSSL-B ibliotheken wurden aktualisiert.	12. August 2024	Version 3.14.0 herunterladen sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516

Version	Änderungen	Date	Link herunterladen und SHA256
3,13,0	Die OpenVPN- und OpenSSL-Bibliotheken wurden aktualisiert.	29. Juli 2024	Version 3.13.0 herunterladen sha256: c9cc896e81a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12,1	Es wurde ein Problem behoben, das verhindert, dass der Windows-Client, Version 3.12.0, für einige Benutzer eine VPN-Verbindung herstellt.	18. Juli 2024	Laden Sie Version 3.12.1 herunter sha256:5e d34aee6c0 3aa281e62 5acdbed27 2896c6704 6364a9e58 46ca697e0 5dbfec08
3.12.0	• Stellt die Verbindung automatisch wieder her, wenn sich die Bereiche des lokalen Netzwerks ändern. • Der automatische Anwendungsfokus bei einer Verbindung mit SAML-Endpunkten wurde entfernt.	21. Mai 2024	Nicht mehr unterstützt

Version	Änderungen	Date	Link herunterladen und SHA256
3.11.2	Es wurde ein Problem mit der SAML-Authentifizierung bei Chromium-basierten Browsern seit Version 123 behoben.	11. April 2024	Laden Sie Version 3.11.2 herunter sha256:8b a258dd15b ea3e861ad 108f8a6d6 d4bcd8fe4 2cb9ef8bb c294e72f365c7cc
3.11.1	• Es wurde eine Pufferüberlauf-Akt ion behoben, die es einem lokalen Akteur potenziell ermöglichen konnte, beliebige Befehle mit erhöhten Rechten auszuführen. • Verbesserter Sicherheitsstatus.	16. Februar 2024	Version 3.11.1 herunterladen sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Ein durch Windows verursachtes Verbindungsproblem wurde behoben. VMs • Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.11.0 herunterladen sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version	Änderungen	Date	Link herunterladen und SHA256
3.10.0	• Es wurde ein Verbindungsproblem behoben, wenn NAT64 es im Client-Netzwerk aktiviert war. • Es wurde ein Verbindungsproblem behoben, das auftrat, wenn Hyper-V-Netzwerkadapter auf dem Client-Computer installiert waren. • Kleinere Fehlerbehebungen und Verbesserungen.	24. August 2023	Version 3.10.0 herunterladen sha256: d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	Verbesserter Sicherheitsstatus.	3. August 2023	Version 3.9.0 herunterladen sha256: de9a3800ea2349155540bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
3.8.0	Verbesserter Sicherheitsstatus.	15. Juli 2023	Nicht mehr unterstützt
3.7.0	Die Änderungen von 3.6.0 wurden zurückgenommen.	15. Juli 2023	Nicht mehr unterstützt
3.6.0	Verbesserter Sicherheitsstatus.	14. Juli 2023	Nicht mehr unterstützt
3.5.0	Kleinere Fehlerbehebungen und Verbesserungen.	03. April 2023	Nicht mehr unterstützt

Version	Änderungen	Date	Link herunterladen und SHA256
3.4.0	Die Änderungen von Version 3.3.0 wurden zurückgenommen.	28. März 2023	Nicht mehr unterstützt
3.3.0	Kleinere Fehlerbehebungen und Verbesserungen.	17. März 2023	Nicht mehr unterstützt
3.2.0	• Unterstützung für das OpenVPN-Flag „verify-x509-name“ hinzugefügt. • Automatische Erkennung, wenn aktualisierte Versionen des Clients verfügbar sind. • Möglichkeit zur automatischen Installation neuer Client-Versionen bei Verfügbarkeit hinzugefügt.	23. Januar 2023	Nicht mehr unterstützt
3.1.0	Verbesserter Sicherheitsstatus.	23. Mai 2022	Nicht mehr unterstützt
3.0.0	• Zusätzlicher Windows 11 Support. • Die Benennung des TAP-Windows-Treibers wurde korrigiert, wodurch andere Treibernamen betroffen sind. • Es wurde behoben, dass die Bannermeldung bei Verwendung der Verbundauthentifizierung nicht angezeigt wird. • Bannertextanzeige für längeren Text wurde korrigiert. • Erhöhter Sicherheitsstatus.	3. März 2022	Nicht mehr unterstützt.

Version	Änderungen	Date	Link herunterladen und SHA256
2.0.0	• Unterstützung für Bannertext nach dem Herstellen einer neuen Verbindung wurde hinzugefügt. • Die Fähigkeit, pull-filter in Bezug auf Echo zu verwenden, z. B. pull-filter * echo, wurde entfernt. • Kleinere Fehlerbehebungen und Verbesserungen.	20. Januar 2022	Nicht mehr unterstützt
1.3.7	• In einigen Fällen wurde der Verbindungsversuch mit einer Verbundauthentifizierung korrigiert. • Kleinere Fehlerbehebungen und Verbesserungen.	8. November 2021	Nicht mehr unterstützt
1.3.6	• Unterstützung für OpenVPN-Flags hinzugefügt: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Kleinere Fehlerbehebungen und Verbesserungen.	20. September 2021	Nicht mehr unterstützt
1.3.5	Patch, um große Windows-Protokolldateien zu löschen.	16. August 2021	Nicht mehr unterstützt
1.3.4	• Unterstützung für OpenVPN-Flag hinzugefügt: dhcp-Option. • Kleinere Fehlerbehebungen und Verbesserungen.	4. August 2021	Nicht mehr unterstützt

Version	Änderungen	Date	Link herunterladen und SHA256
1.3.3	• Unterstützung für OpenVPN-Flags hinzugefügt: inaktiv, Pull-Filter, Route. • Es wurde ein Fehler behoben, der beim Trennen oder Beenden der App zu Abstürzen führte. • Es wurde ein Problem mit Active-Di rectory-Benutzernamen mit umgekehrt em Schrägstrich behoben. • Es wurde ein App-Absturz beim Bearbeiten der Profilliste außerhalb der App behoben. • Kleinere Fehlerbehebungen und Verbesserungen.	1. Juli 2021	Nicht mehr unterstützt
1.3.2	• Fügen Sie den Schutz vor Datenlecks hinzu, wenn er konfiguriert ist. IPv6 • Es wurde ein potenzieller Absturz behoben, bei dem Sie die Option Details anzeigen unter Verbindung verwenden.	12. Mai 2021	Nicht mehr unterstützt
1.3.1	• Support für mehrere Client-Zertifikate mit demselben Betreff hinzugefü gt. Abgelaufene Zertifikate werden ignoriert. • Feste lokale Aufbewahrung von Protokollen zur Reduzierung der Festplattennutzung. • Support für OpenVPN-Direktive 'route-IPv6' hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	05. April 2021	Nicht mehr unterstützt

Version	Änderungen	Date	Link herunterladen und SHA256
1.3.0	Zusätzliche Supportfunktionen wie Fehlerberichte, Senden von Diagnosep rotokollen und Analysen.	8. März 2021	Nicht mehr unterstützt
1.2.7	• Unterstützung für die OpenVPN-D irektive cryptoapicert hinzugefügt. • Korrektur veralteter Routen zwischen Verbindungen. • Kleinere Fehlerbehebungen und Verbesserungen.	25. Februar 2021	Nicht mehr unterstützt
1.2.6	Kleinere Fehlerbehebungen und Verbesserungen.	26. Oktober 2020	Nicht mehr unterstützt
1.2.5	• Unterstützung für Kommentare in der OpenVPN-Konfiguration hinzugefügt. • Fehlermeldung für TLS-Handshake-Fehler hinzugefügt.	8. Oktober 2020	Nicht mehr unterstützt
1.2.4	Kleinere Fehlerbehebungen und Verbesserungen.	1. September 2020	Nicht mehr unterstützt
1.2.3	Rollback von Änderungen in Version 1.2.2.	20. August 2020	Nicht mehr unterstützt
1.2.1	Kleinere Fehlerbehebungen und Verbesserungen.	1. Juli 2020	Nicht mehr unterstützt
1.2.0	• Unterstützung für die SAML 2.0-basie rte Verbundauthentifizierung hinzugefü gt. • Unterstützung für die Windows 7-Plattfo rm eingestellt.	19. Mai 2020	Nicht mehr unterstützt

Version	Änderungen	Date	Link herunterladen und SHA256
1.1.1	Kleinere Fehlerbehebungen und Verbesserungen.	21. April 2020	Nicht mehr unterstützt
1.1.0	• Unterstützung für die statische OpenVPN-Challenge-Echo-Funktionalität zum Ein- und Ausblenden des in der Benutzeroberfläche angezeigten Textes hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	9. März 2020	Nicht mehr unterstützt
1.0.0	Die Erstversion.	4. Februar 2020	Nicht mehr unterstützt

AWS Client VPN für macOS

In diesen Abschnitten wird beschrieben, wie Sie mit dem AWS bereitgestellten Client für macOS eine VPN-Verbindung herstellen. Sie können den Client unter AWS Client VPN-Download herunterladen und installieren. Der AWS bereitgestellte Client unterstützt keine automatischen Updates.

Voraussetzungen

Um den AWS bereitgestellten Client für macOS verwenden zu können, ist Folgendes erforderlich:

- macOS Sonoma (14.0), Sequoia (15.0) oder Tahoe (26.0)
- ARM64 x86_64 oder prozessorkompatibel.
- Für Client VPN, Endpunkte, die SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client die TCP-Ports 8096-8115 auf Ihrem Computer.

Themen

Connect to (Verbinden mit) AWS Client VPN mit einem AWS bereitgestellter Client für macOS

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie eine Verbindung zu mehreren Profilen gleichzeitig herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Stellen Sie außerdem sicher, dass Sie die Anforderungen gelesen haben. Der AWS bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN-Client bezeichnet.

Um eine Verbindung mit dem herzustellen AWS bereitgestellter Client für macOS

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.
3. Wählen Sie Add Profile (Profil hinzufügen) aus.
4. Geben Sie für Display name (Anzeigelname) einen Namen für das Profil ein.
5. Wählen Sie unter VPN Configuration File (VPN-Konfigurationsdatei) die Konfigurationsdatei aus, die Sie von Ihrem Client VPN-Administrator erhalten haben. Wählen Sie dann Add Profile (Profil hinzufügen) aus.
6. Wenn Sie mehrere Verbindungen erstellen möchten, wiederholen Sie die Schritte zum Hinzufügen von Profilen für jede Konfigurationsdatei, die Sie hinzufügen möchten. Sie können so viele Profile hinzufügen, wie Sie möchten, aber Sie können nur bis zu fünf offene Verbindungen haben.
7. Wählen Sie im AWS VPN-Client-Fenster das Profil aus, mit dem Sie Connect möchten, und wählen Sie dann Verbinden aus. Wenn der Client VPN-Endpunkt für die Verwendung der auf Anmeldeinformationen basierenden Authentifizierung konfiguriert wurde, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wiederholen Sie diesen Schritt für jede Profilverbindung, die Sie initiieren möchten, und verbinden Sie bis zu fünf Endpunkte gleichzeitig.

> **Note**
>
> Wenn ein Profil, mit dem Sie eine Verbindung herstellen, Konflikte mit einer aktuell geöffneten Sitzung aufweist, können Sie die Verbindung nicht herstellen. Wählen Sie

entweder eine neue Verbindung oder trennen Sie die Verbindung zu der Sitzung, die den Konflikt verursacht hat.

8. Um Statistiken für eine Verbindung anzuzeigen, wählen Sie im AWS VPN-Client-Fenster Verbindung aus, wählen Sie Details anzeigen und wählen Sie dann die Verbindung aus, zu der Sie Details sehen möchten.
9. Um eine Verbindung zu trennen, wählen Sie im AWS VPN-Client-Fenster eine Verbindung aus und klicken Sie dann auf Trennen. Wenn Sie mehrere offene Verbindungen haben, müssen Sie jede Verbindung einzeln schließen.

AWS Client VPN Versionshinweise für macOS

Die folgende Tabelle enthält die Versionshinweise und Download-Links für die aktuelle und frühere Version von AWS Client VPN für macOS.

Note

Wir bieten weiterhin mit jeder Version Verbesserungen in Bezug auf Benutzerfreundlichkeit und Sicherheit. Wir empfehlen dringend, für jede Plattform die neueste Version zu verwenden. Frühere Versionen können von Benutzerfreundlichkeits and/or - und Sicherheitsproblemen betroffen sein. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Datum	Download-Link
5.3.5	• Kleinere Fehlerbehebungen und Verbesserungen • Verbesserter Sicherheitsstatus • In future Updates wurde das automatische Upgrade auf den nativen ARM64-Client für ARM-based Mac-Benutzer aktiviert, sodass keine manuelle Migration vom Intel-bas ed Client erforderlich ist, der unter	14. Mai 2026	• Laden Sie macOS ARM64 Version 5.3.5 herunter sha256:048c9011b7c ea43720cb92d7c2fe0 64c8d853b391ee4994 08736cba5d9111652

Version	Änderungen	Datum	Download-Link
	der Rosetta-Übersetzungsebene ausgeführt wird		• Laden Sie macOS x64 Version 5.3.5 herunter sha256:64a84f529a09b2ee9756dd8f5e193b9624b3239bcd76d9f20411a72d1f93887c
5.3.4	• Die Anforderung für die Intel Compatibility Layer (Rosetta) wurde auf ARM-Maschinen entfernt • Kleinere Fehlerbehebungen und Verbesserungen	17. Februar 2026	Nicht mehr unterstützt.
5.3.3	• Kleinere Fehlerbehebungen und Verbesserungen. • Verbesserter Sicherheitsstatus.	26. Dezember 2025	Nicht mehr unterstützt.
5.3.2	• Native Unterstützung für die Apple Silicon-Architektur und ein neues macOS ARM64-Installation sprogramm hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	27. Oktober 2025	Nicht mehr unterstützt.
5.3.1	• Kleinere Fehlerbehebungen und Verbesserungen.	9. September 2	Nicht mehr unterstützt.
5.3.0	• Kleinere Verbesserungen. • Unterstützung für IPv6-Verbindungen hinzugefügt.	14. August 202	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
5.2.1	• Unterstützung für das Ping-Exit-OpenVPN-Flag hinzugefügt. • Die OpenSSL-Bibliothek wurde aktualisiert. • Verbesserter Sicherheitsstatus. • Kleinere Fehlerbehebungen und Verbesserungen.	18. Juni 2025	Nicht mehr unterstützt.
5.2.0	• Kleinere Verbesserungen. • Unterstützung für Client Route Enforcement hinzugefügt.	8. April 2025	Nicht mehr unterstützt.
5.1.0	• Es wurde ein Problem behoben, das dazu führte, dass AWS Client VPN Version 5.0.x nach einer Unterbrechung des Inaktivitäts-Timeouts automatisch wieder eine Verbindung zum VPN herstellte. • Es wurde ein Problem behoben, das den Aufbau AWS Client VPN einer VPN-Verbindung für Konfigurationsdateien mit Zeilenenden verhinderte. Windows-style • Kleinere Fehlerbehebungen und Verbesserungen.	17. März 2025	Nicht mehr unterstützt.
5.0.3	Kleinere Fehlerbehebungen und Verbesserungen.	6. März 2025	Nicht mehr unterstützt.
5.0.2	Es wurde ein Problem behoben, das zu sporadischen Fehlern bei der Auswahl von Connect führte.	17. Februar 20	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
5.0.1	Es wurde ein Problem behoben, das die Client-Version 5.0.0 daran hinderte, eine VPN-Verbindung für Profilnamen herzustellen, die Leerzeichen enthielten.	22. Januar 2025	Nicht mehr unterstützt.
5.0.0	• Unterstützung für gleichzeitige Verbindungen hinzugefügt. • Die grafische Benutzeroberfläche wurde aktualisiert. • Kleinere Fehlerbehebungen und Verbesserungen.	21. Januar 202	Nicht mehr unterstützt.
4.1.0	Kleinere Fehlerbehebungen und Verbesserungen.	12. November 2024	Nicht mehr unterstützt.
4.0.0	Kleinere Verbesserungen.	25. September 2024	Nicht mehr unterstützt.
3.12.1	Unterstützung für das `mssfix` OpenVPN-Flag hinzugefügt.	4. September 2	Nicht mehr unterstützt.
3.12.0	• Unterstützung für das `tap-sleep` OpenVPN-Flag hinzugefügt. • Die OpenVPN- und OpenSSL-Bibliotheken wurden aktualisiert.	12. August 202	Nicht mehr unterstützt.
3.11.0	• Die OpenVPN- und OpenSSL-Bibliotheken wurden aktualisiert.	29. Juli 2024	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
3.10.0	• Stellt die Verbindung automatisch wieder her, wenn sich die Bereiche des lokalen Netzwerks ändern. • Ein Problem mit der DNS-Wiede rherstellung beim Netzwerkwechsel wurde behoben. • Der automatische Anwendungsfokus bei Verbindung mit SAML-Endpunkten wurde entfernt.	21. Mai 2024	Nicht mehr unterstützt.
3.9.2	• Es wurde ein Problem mit der SAML-Authentifizierung bei Chromium-based Browsern seit Version 123 behoben. • Unterstützung für macOS Sonoma hinzugefügt. Unterstützung für macOS Big Sur wurde eingestellt. • Verbesserter Sicherheitsstatus.	11. April 2024	Nicht mehr unterstützt.
3.9.1	• Es wurde eine Pufferüberlauf-Akt ion behoben, die es einem lokalen Akteur potenziell ermöglichen konnte, beliebige Befehle mit erhöhten Rechten auszuführen. • Die Fortschrittsanzeige beim Herunterl aden von Anwendungsupdates wurde behoben. • Verbesserter Sicherheitsstatus.	16. Februar 20	Nicht mehr unterstützt.
3.9.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
3.8.0	• Es wurde ein Verbindungsproblem behoben, das auftrat, wenn NAT64 im Client-Netzwerk aktiviert war. • Kleinere Fehlerbehebungen und Verbesserungen.	24. August 202	Nicht mehr unterstützt.
3.7.0	• Verbesserter Sicherheitsstatus.	3. August 2023	Nicht mehr unterstützt.
3.6.0	• Verbesserter Sicherheitsstatus.	15. Juli 2023	Nicht mehr unterstützt.
3.5.0	• Die Änderungen von 3.4.0 wurden zurückgenommen.	15. Juli 2023	Nicht mehr unterstützt.
3.4.0	• Verbesserter Sicherheitsstatus.	14. Juli 2023	Nicht mehr unterstützt.
3.3.0	• Unterstützung für macOS Ventura (13.0) wurde hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	27. April 2023	Nicht mehr unterstützt.
3.2.0	• Unterstützung für das OpenVPN-Flag „verify-x509-name“ hinzugefügt. • Automatische Erkennung, wenn aktualisierte Versionen des Clients verfügbar sind. • Möglichkeit zur automatischen Installation neuer Client-Versionen bei Verfügbarkeit hinzugefügt.	23. Januar 202	Nicht mehr unterstützt.
3.1.0	• Unterstützung für macOS Monterey wurde hinzugefügt. • Problem bei der Festplattenerkennung wurde behoben. • Verbesserter Sicherheitsstatus.	23. Mai 2022	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
3.0.0	• Es wurde behoben, dass die Bannermeldung bei Verwendung der Verbundauthentifizierung nicht angezeigt wird. • Bannertextanzeige für längeren Text wurde korrigiert. • Erhöhter Sicherheitsstatus.	3. März 2022	Nicht mehr unterstützt.
2.0.0	• Unterstützung für Bannertext nach dem Herstellen einer neuen Verbindung wurde hinzugefügt. • Die Fähigkeit, pull-filter in Bezug auf Echo zu verwenden, z. B. pull-filter * echo, wurde entfernt. • Kleinere Fehlerbehebungen und Verbesserungen.	20. Januar 202	Nicht mehr unterstützt.
1.4.0	• DNS-Serverüberwachung während der Verbindung hinzugefügt. Die Einstellungen werden neu konfiguriert, wenn sie nicht den VPN-Einstellungen entsprechen. • In einigen Fällen wurde der Verbindungsversuch mit einer Verbundauthentifizierung korrigiert. • Kleinere Fehlerbehebungen und Verbesserungen.	9. November 2021	Nicht mehr unterstützt.
1.3.5	• Unterstützung für OpenVPN Flags hinzugefügt: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • Kleinere Fehlerbehebungen und Verbesserungen.	20. September 2021	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
1.3.4	• Unterstützung für OpenVPN-Flag hinzugefügt: dhcp-Option. • Kleinere Fehlerbehebungen und Verbesserungen.	4. August 2021	Nicht mehr unterstützt.
1.3.3	• Unterstützung für OpenVPN-Flags hinzugefügt: inaktiv, Pull-Filter, Route. • Ein Problem mit Konfigurationsdate inamen mit Leerzeichen oder Unicode wurde behoben. • Es wurde ein Fehler behoben, der beim Trennen oder Beenden der App zu Abstürzen führte. • Es wurde ein Problem mit Active-Di rectory-Benutzernamen mit umgekehrt em Schrägstrich behoben. • Es wurde ein App-Absturz beim Bearbeiten der Profilliste außerhalb der App behoben. • Kleinere Fehlerbehebungen und Verbesserungen.	1. Juli 2021	Nicht mehr unterstützt.
1.3.2	• Fügen Sie IPv6-Leckschutz hinzu, wenn es konfiguriert ist. • Es wurde ein potenzieller Absturz behoben, bei dem Sie die Option Details anzeigen unter Verbindung verwenden. • Fügen Sie Daemon-Log-Rotation hinzu.	12. Mai 2021	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
1.3.1	• Unterstützung für macOS Big Sur (10.16) hinzugefügt. • Behobenes Problem, das die von anderen Anwendungen konfigurierten DNS-Einstellungen entfernte. • Behobenes Problem, bei dem die Verwendung eines ungültigen Zertifikats für die gegenseitige Authentifizierung, das Verbindungsprobleme verursachte. • Support für OpenVPN-Direktive 'route-IPv6' hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	05. April 2021	Nicht mehr unterstützt.
1.3.0	Zusätzliche Supportfunktionen wie Fehlerberichte, Senden von Diagnoseprotokollen und Analysen.	8. März 2021	Nicht mehr unterstützt.
1.2.5	Kleinere Fehlerbehebungen und Verbesserungen.	25. Februar 2021	Nicht mehr unterstützt.
1.2.4	Kleinere Fehlerbehebungen und Verbesserungen.	26. Oktober 20	Nicht mehr unterstützt.
1.2.3	• Unterstützung für Kommentare in der OpenVPN-Konfiguration hinzugefügt. • Fehlermeldung für TLS-Handshake-Fehler hinzugefügt. • Es wurde ein Deinstallationsfehler behoben, der einige Benutzer betraf.	8. Oktober 202	Nicht mehr unterstützt.
1.2.2	Kleinere Fehlerbehebungen und Verbesserungen.	12. August 2020	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
1.2.1	• Unterstützung für die Deinstallation der Anwendung hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	1. Juli 2020	Nicht mehr unterstützt.
1.2.0	• Unterstützung für die SAML 2.0-basierte Verbundauthentifizierung hinzugefügt. • Unterstützung für macOS Catalina (10.15) hinzugefügt.	19. Mai 2020	Nicht mehr unterstützt.
1.1.2	Kleinere Fehlerbehebungen und Verbesserungen.	21. April 2020	Nicht mehr unterstützt.
1.1.1	• Problem behoben, bei dem DNS nicht aufgelöst wurde. • Absturzproblem bei Apps durch längere Verbindungen behoben. • MFA-Problem behoben.	2. April 2020	Nicht mehr unterstützt.
1.1.0	• Unterstützung für macOS-DNS-Konfiguration hinzugefügt. • Unterstützung für die statische OpenVPN-Challenge-Echo-Funktionalität zum Ein- und Ausblenden des in der Benutzeroberfläche angezeigten Textes hinzugefügt. • Kleinere Fehlerbehebungen und Verbesserungen.	9. März 2020	Nicht mehr unterstützt.
1.0.0	Die Erstversion.	4. Februar 2020	Nicht mehr unterstützt.

AWS Client VPN für Linux

In diesen Abschnitten AWS wird die Installation des bereitgestellten Clients für Linux und der anschließende Aufbau einer VPN-Verbindung mithilfe des AWS bereitgestellten Clients beschrieben. Der AWS bereitgestellte Client für Linux unterstützt keine automatischen Updates. Die neuesten Updates und Downloads finden Sie unterthe section called “Versionshinweise”.

Voraussetzungen für die Verbindung zum Client VPN mit einem AWS bereitgestellter Client für Linux

Um den AWS bereitgestellten Client für Linux zu verwenden, ist Folgendes erforderlich:

- Ubuntu 22.04 LTS (AMD64), Ubuntu 24.04 LTS (nur AMD64) oder Ubuntu 26.04 LTS (nur AMD64)

Für Client-VPN-Endpunkte, die SAML-based Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client die TCP-Ports 8096-8115 auf Ihrem Computer.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie eine Verbindung zu mehreren Profilen gleichzeitig herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Themen

- Installieren Sie das AWS Client VPN für Linux bereitgestellte
- Connect zum bereitgestellten her AWS Client VPN für Linux
- AWS Client VPN für Linux-Versionshinweise

Installieren Sie das AWS Client VPN für Linux bereitgestellte

Es gibt mehrere Methoden, mit denen der AWS bereitgestellte Client für Linux installiert werden kann. Verwenden Sie eine der in den folgenden Optionen bereitgestellten Methoden. Bevor Sie beginnen, stellen Sie sicher, dass Sie die Anforderungen gelesen haben.

Option 1: Installation über das Paket-Repository

1. Fügen Sie den öffentlichen Schlüssel des AWS VPN-Clients zu Ihrem Ubuntu-Betriebssystem hinzu.

```
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. Verwenden Sie den folgenden Befehl, um das Repository zu Ihrem Ubuntu-Betriebssystem (Version 22.04 und höher) hinzuzufügen:

```
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. Verwenden Sie den folgenden Befehl, um die Repositories auf Ihrem System zu aktualisieren.

```
sudo apt-get update
```

4. Verwenden Sie den folgenden Befehl, um den AWS bereitgestellten Client für Linux zu installieren.

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

Option 2: Installation mithilfe der .deb-Paketdatei

1. Laden Sie die DEB-Datei von AWS Client VPN herunterladen oder mithilfe des folgenden Befehls herunter.

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

2. Installieren Sie den AWS bereitgestellten Client für Linux mit dem `dpkg` Hilfsprogramm.

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

Option 3 – Installation über das DEB-Paket mit dem Ubuntu Software Center

1. Laden Sie die DEB-Paketdatei von AWS Client VPN herunterladen herunter.
2. Verwenden Sie nach dem Herunterladen der DEB-Paketdatei das Ubuntu Software Center, um das Paket zu installieren. Befolgen Sie die Schritte für die Installation von einem eigenständigen DEB-Paket mit dem Ubuntu Software Center von der Ubuntu Wiki.

Connect zum bereitgestellten her AWS Client VPN für Linux

Der AWS bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN-Client bezeichnet.

Um eine Verbindung mit dem herzustellen AWS bereitgestellter Client für Linux

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.
3. Wählen Sie Add Profile (Profil hinzufügen) aus.
4. Geben Sie für Display name (Anzeigelname) einen Namen für das Profil ein.
5. Suchen Sie unter VPN Configuration File (VPN-Konfigurationsdatei) nach der Konfigurationsdatei, die Sie von Ihrem Client-VPN-Administrator erhalten haben. Klicken Sie auf Open.
6. Wählen Sie Add Profile (Profil hinzufügen) aus.
7. Wenn Sie mehrere Verbindungen erstellen möchten, wiederholen Sie die Schritte zum Hinzufügen von Profilen für jede Konfigurationsdatei, die Sie hinzufügen möchten. Sie können so viele Profile hinzufügen, wie Sie möchten, aber Sie können nur bis zu fünf offene Verbindungen haben.
8. Wählen Sie im AWS VPN-Client-Fenster das Profil aus, mit dem Sie Connect möchten, und wählen Sie dann Verbinden aus. Wenn der Client VPN-Endpunkt für die Verwendung der auf Anmeldeinformationen basierenden Authentifizierung konfiguriert wurde, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wiederholen Sie diesen Schritt für jede Profilverbindung, die Sie initiieren möchten, und verbinden Sie bis zu fünf Endpunkte gleichzeitig.

   > **Note**
   >
   > Wenn ein Profil, mit dem Sie eine Verbindung herstellen, Konflikte mit einer aktuell geöffneten Sitzung aufweist, können Sie die Verbindung nicht herstellen. Wählen Sie entweder eine neue Verbindung oder trennen Sie die Verbindung zu der Sitzung, die den Konflikt verursacht hat.

9. Um Statistiken für eine Verbindung anzuzeigen, wählen Sie im AWS VPN-Client-Fenster Verbindung aus, wählen Sie Details anzeigen und wählen Sie dann die Verbindung aus, zu der Sie Details sehen möchten.

10. Um eine Verbindung zu trennen, wählen Sie im AWS VPN-Client-Fenster eine Verbindung aus und klicken Sie dann auf Trennen. Wenn Sie mehrere offene Verbindungen haben, müssen Sie jede Verbindung einzeln schließen.

AWS Client VPN für Linux-Versionshinweise

Die folgende Tabelle enthält die Versionshinweise und Download-Links für die aktuelle und frühere Version von AWS Client VPN für Linux.

> **Note**
>
> Wir bieten weiterhin mit jeder Version Verbesserungen in Bezug auf Benutzerfreundlichkeit und Sicherheit. Wir empfehlen dringend, für jede Plattform die neueste Version zu verwenden. Frühere Versionen können von Benutzerfreundlichkeits and/or - und Sicherheitsproblemen betroffen sein. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Datum	Download-Link
5.3.3	• Kleinere Fehlerbehebungen und Verbesserungen • Verbesserter Sicherheitsstatus	18. Mai 2026	Version 5.3.3 herunterladen sha256: d0096c934 b36122c24 5d8c2243d 4146cdac6 7125c7421 c4e1e6ad4 30eb3adfcf
5.3.2	• Kleinere Fehlerbehebungen und Verbesserungen. • Verbesserter Sicherheitsstatus.	17. Dezember 2025	Version 5.3.2 herunterladen sha256:89 e4b9f2c9f 7def37167

Version	Änderungen	Datum	Download-Link
			f5f137f4ff9c6c5246fd6e0a7244b70c196a17683569
5.3.1	• Kleinere Verbesserungen.	25. September 2025	Version 5.3.1 herunterladen sha256:4a426cc226382748d683a4946340447dab87ec42583977d9488ee45d11cdcec0
5.3.0	• Kleinere Verbesserungen. • Unterstützung für IPv6-Verbindungen hinzugefügt.	14. August 2025	Laden Sie Version 5.3.0 herunter sha256:31edb55f12dcd68a7a4ca9b6233ddbeebcd37e01f87655a520cc7e7542bbfcb4

Version	Änderungen	Datum	Download-Link
5.2.0	• Kleinere Verbesserungen. • Unterstützung für Client Route Enforce hinzugefügt.	8. April 2025	Version 5.2.0 herunterladen sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• Es wurde ein Problem behoben, das dazu führte, dass Version 5.0.x nach einer Unterbrechung des Inaktivitäts-Timeouts automatisch wieder eine Verbindung zum VPN herstellte. AWS Client VPN • Kleinere Fehlerbehebungen und Verbesserungen.	17. März 2025	Version 5.1.0 herunterladen sha256:14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba
5.0.0	• Unterstützung für mehrere gleichzeitige Verbindungen hinzugefügt. • Die grafische Benutzeroberfläche wurde aktualisiert. • Kleinere Fehlerbehebungen und Verbesserungen.	21. Januar 2025	Version 5.0.0 herunterladen sha256:645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c

Version	Änderungen	Datum	Download-Link
4.1.0	• Unterstützung für Ubuntu 22.04 und 24.04 hinzugefügt. • Fehlerbehebungen	12. November 2024	Laden Sie Version 4.1.0 herunter sha256:33 4d0022245 8fbfe9dad e16c99fe9 7e9ebcbd5 1fff017d0 d6b1d1b76 4e7af472
4.0.0	Kleinere Verbesserungen.	25. September 2024	Version 4.0.0 herunterladen sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3,15,1	Unterstützung für das `mssfix` OpenVPN-Flag hinzugefügt.	4. September 2024	Laden Sie Version 3.15.1 herunter sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2

Version	Änderungen	Datum	Download-Link
3,15.0	• Unterstützung für das `tap-sleep` OpenVPN-Flag hinzugefügt. • Die OpenVPN- und OpenSSL-B ibliotheken wurden aktualisiert.	12. August 2024	Version 3.15.0 herunterladen sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6d89d012
3,14.0	• Die OpenVPN- und OpenSSL-B ibliotheken wurden aktualisiert.	29. Juli 2024	Version 3.14.0 herunterladen sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3,13,0	• Stellt die Verbindung automatisch wieder her, wenn sich die Bereiche des lokalen Netzwerks ändern.	21. Mai 2024	Laden Sie Version 3.13.0 herunter sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1

Version	Änderungen	Datum	Download-Link
3.12,2	• Es wurde ein Problem mit der SAML-Authentifizierung bei Chromium-based Browsern seit Version 123 behoben.	11. April 2024	Laden Sie Version 3.12.2 herunter sha256: f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
3,12,1	• Es wurde eine Pufferüberlauf-Aktion behoben, die es einem lokalen Akteur potenziell ermöglichen konnte, beliebige Befehle mit erhöhten Rechten auszuführen. • Verbesserter Sicherheitsstatus.	16. Februar 2024	Version 3.12.1 herunterladen sha256:547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben.	19. Dezember 2023	Version 3.12.0 herunterladen sha256: 9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1

Version	Änderungen	Datum	Download-Link
3.11.0	• Rollback für „Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben“. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.11.0 herunterladen sha256:86c0fa1bf1c971940828 35a739ec7f1c87e540 194955f414a35c679b 94538970
3.10.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.10.0 herunterladen sha256: e7450b2490f3b96ab7 d589a8000d838d9fd2 adcdd72ae80666c4c0 d900687e51
3.9.0	• Es wurde ein Verbindungsproblem behoben, das auftrat, wenn NAT64 im Client-Netzwerk aktiviert war. • Kleinere Fehlerbehebungen und Verbesserungen.	24. August 2023	Version 3.9.0 herunterladen sha256: 6cde9cfff82754119e 6a68464d4bb350da3c b3e1ebf9140dacf24e 4fd2197454

Version	Änderungen	Datum	Download-Link
3.8.0	• Verbesserter Sicherheitsstatus.	3. August 2023	Version 3.8.0 herunterladen sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• Verbesserter Sicherheitsstatus.	15. Juli 2023	Nicht mehr unterstützt
3.6.0	• Die Änderungen von 3.5.0 wurden zurückgenommen.	15. Juli 2023	Nicht mehr unterstützt
3.5.0	• Verbesserter Sicherheitsstatus.	14. Juli 2023	Nicht mehr unterstützt
3.4.0	• Unterstützung für das OpenVPN-Flag „verify-x509-name“ hinzugefügt.	14. Februar 2023	Nicht mehr unterstützt
3.1.0	• Problem bei der Festplattenerkennung wurde behoben. • Verbesserter Sicherheitsstatus.	23. Mai 2022	Nicht mehr unterstützt
3.0.0	• Es wurde behoben, dass die Bannermeldung bei Verwendung der Verbundauthentifizierung nicht angezeigt wird. • Bannertextanzeige für längeren Text und bestimmte Zeichenfolgen wurde korrigiert. • Erhöhter Sicherheitsstatus.	3. März 2022	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
2.0.0	• Unterstützung für Bannertext nach dem Herstellen einer neuen Verbindung wurde hinzugefügt. • Die Fähigkeit, pull-filter in Bezug auf Echo zu verwenden, z. B. pull-filter * echo, wurde entfernt. • Kleinere Fehlerbehebungen und Verbesserungen.	20. Januar 2022	Nicht mehr unterstützt.
1.0.3	• In einigen Fällen wurde der Verbindungsversuch mit einer Verbundauthentifizierung korrigiert. • Kleinere Fehlerbehebungen und Verbesserungen.	8. November 2021	Nicht mehr unterstützt.
1.0.2	• Unterstützung für OpenVPN Flags hinzugefügt: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • Kleinere Fehlerbehebungen und Verbesserungen.	28. September 2021	Nicht mehr unterstützt.
1.0.1	• Aktivierte Option zum Beenden von Ubuntu-Anwendungsleiste. • Unterstützung für OpenVPN-Flags hinzugefügt: inaktiv, Pull-Filter, Route. • Kleinere Fehlerbehebungen und Verbesserungen.	4. August 2021	Nicht mehr unterstützt.
1.0.0	Die Erstversion.	11. Juni 2021	Nicht mehr unterstützt.

Connect zu einem her AWS Client VPN Endpunkt, der einen OpenVPN-Client verwendet

Sie können mithilfe gängiger Open VPN-Clientanwendungen eine Verbindung zu einem Client-VPN-Endpunkt herstellen. Client VPN wird auf den folgenden Betriebssystemen unterstützt:

- Windows

  Verwenden Sie ein Zertifikat und einen privaten Schlüssel aus dem Windows-Zertifikatsspeicher. Sobald Sie das Zertifikat und den Schlüssel generiert haben, können Sie entweder mit der OpenVPN AWS GUI-Client-Anwendung oder dem OpenVPN GUI Connect Client eine Client-Verbindung herstellen. Die Schritte zum Erstellen des Zertifikats und des Schlüssels finden Sie unter. Stellen Sie unter Windows eine VPN-Verbindung mithilfe eines Zertifikats her
- macOS

  Stellen Sie mithilfe einer Konfigurationsdatei für Mac OS-based Tunnelblick oder für AWS Client VPN eine VPN-Verbindung her. Weitere Informationen finden Sie unter Stellen Sie eine VPN-Verbindung unter macOS her.
- Linux

  Stellen Sie unter Linux entweder über die OpenVPN - Network Manager-Schnittstelle oder die OpenVPN-Anwendung eine VPN-Verbindung her. Um die OpenVPN - Network Manager-Schnittstelle verwenden zu können, müssen Sie zuerst das Netzwerkmanager-Modul installieren, falls es noch nicht installiert ist. Weitere Informationen finden Sie unter Stellen Sie eine VPN-Verbindung unter Linux her.
- Android und iOS

  Stellen Sie mit der OpenVPN-Client-Anwendung auf einem Android- oder iOS-Gerät eine VPN-Verbindung her. Weitere Informationen finden Sie unter Client-VPN-Verbindungen auf Android und iOS.

> **Important**
>
> Wenn der Client-VPN-Endpunkt für die Verwendung der SAML-based Verbundauthentifizierung konfiguriert wurde, können Sie den OpenVPN-based VPN-Client nicht verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Dies

schließt alle ARM-based Architekturen ein. Wenn Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. Apple Silicon Macs oder ARM-based Windows-Geräte), müssen Sie SAML-based VPN-Endpunkte mit dem AWS bereitgestellten Client anstelle von OpenVPN-Clients verwenden.

Clientanwendungen

- Connect zu einem her AWS Client VPN Endpunkt, der eine Windows-Client-Anwendung verwendet
- Connect zu einem her AWS Client VPN Endpunkt mit einer macOS-Client-Anwendung
- Connect zu einem her AWS Client VPN Endpunkt, der eine OpenVPN-Client-Anwendung verwendet
- AWS Client VPN Verbindungen in Android- und iOS-Anwendungen

Connect zu einem her AWS Client VPN Endpunkt, der eine Windows-Client-Anwendung verwendet

In diesen Abschnitten wird beschrieben, wie Sie mithilfe von VPN-Clients eine Windows-based VPN-Verbindung herstellen.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie eine Verbindung zu mehreren Profilen gleichzeitig herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Informationen zur Problembehebung finden Sie unter Fehlerbehebung AWS Client-VPN-Verbindungen mit Windows-based Clients.

Important

Wenn der Client-VPN-Endpunkt für die Verwendung der SAML-based Verbundauthentifizierung konfiguriert wurde, können Sie den OpenVPN-based VPN-Client nicht verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Dies schließt alle ARM-based Architekturen ein. Wenn Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. Apple Silicon Macs oder ARM-based Windows-Geräte), müssen Sie SAML-based VPN-Endpunkte mit dem AWS bereitgestellten Client anstelle von OpenVPN-Clients verwenden.

Aufgaben

- Verwenden Sie ein Zertifikat und richten Sie ein AWS Client-VPN-Verbindung unter Windows

Verwenden Sie ein Zertifikat und richten Sie ein AWS Client-VPN-Verbindung unter Windows

Sie können den OpenVPN-Client so konfigurieren, dass er ein Zertifikat und einen privaten Schlüssel aus dem Windows Certificate System Store verwendet. Diese Option ist nützlich, wenn Sie eine Smartcard als Teil Ihrer Client-VPN-Verbindung verwenden. Informationen zur Cryptoapicert-Option OpenVPN-Client finden Sie unter Referenzhandbuch für OpenVPN auf der OpenVPN-Website.

> **Note**
>
> Das Zertifikat muss auf dem lokalen Computer gespeichert sein.

Um ein Zertifikat zu verwenden und eine Verbindung herzustellen

1. Erstellen Sie eine PFX-Datei, die das Client-Zertifikat und den privaten Schlüssel enthält.
2. Importieren Sie die PFX-Datei in Ihren persönlichen Zertifikatspeicher auf Ihrem lokalen Computer. Weitere Informationen finden Sie unter Gewusst wie: Anzeigen von Zertifikaten mit dem MMC-Snap-In auf der Microsoft-Website.
3. Stellen Sie sicher, dass Ihr Konto über Berechtigungen zum Lesen des lokalen Computerzertifikats verfügt. Sie können die Microsoft-Managementkonsole verwenden, um die Berechtigungen zu ändern. Weitere Informationen finden Sie unter Rechte zum Zugriff auf den lokalen Computerzertifikatspeicher auf der Microsoft-Website.
4. Aktualisieren Sie die OpenVPN-Konfigurationsdatei und geben Sie das Zertifikat an, indem Sie entweder den Zertifikatbetreff oder den Fingerabdruck des Zertifikats verwenden.

   Im Folgenden finden Sie ein Beispiel für die Angabe des Zertifikats mithilfe eines Betreffs.

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

   Im Folgenden finden Sie ein Beispiel für die Angabe des Zertifikats mithilfe eines Fingerabdrucks. Sie finden den Fingerabdruck mithilfe der Microsoft-Managementkonsole.

Weitere Informationen finden Sie auf der Microsoft-Website unter Vorgehensweise: Abrufen des Fingerabdrucks eines Zertifikats.

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

5. Nachdem Sie die Konfiguration abgeschlossen haben, verwenden Sie OpenVPN, um eine VPN-Verbindung herzustellen, indem Sie einen der folgenden Schritte ausführen:

   - Verwenden Sie die OpenVPN GUI-Client-Anwendung
     1. Starten Sie die OpenVPN-Clientanwendung.
     2. Wählen Sie in der Windows-Taskleiste Symbole ausShow/Hide . Right-click OpenVPN GUI und wählen Sie dann Datei importieren.
     3. Wählen Sie im Dialogfeld „Öffnen“ die Konfigurationsdatei aus, die Sie von Ihrem Client VPN-Administrator erhalten haben, und klicken Sie auf Öffnen.
     4. Wählen Sie in der Windows-Taskleiste Symbole ausShow/Hide . Right-click OpenVPN GUI und wählen Sie dann Connect.

   - Verwenden Sie den OpenVPN GUI Connect Client
     1. Starten Sie die OpenVPN-Anwendung und wählen Sie Import, Aus lokaler Datei... .
     2. Navigieren Sie zu der Konfigurationsdatei, die Sie von Ihrem VPN-Administrator erhalten haben, und wählen Sie Open (Öffnen) aus.

Connect zu einem her AWS Client VPN Endpunkt mit einer macOS-Client-Anwendung

In diesen Abschnitten wird beschrieben, wie Sie mit dem Mac VPN-Client, Tunnelblick oder AWS Client OS-based VPN eine VPN-Verbindung herstellen.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie gleichzeitig eine Verbindung zu mehreren Profilen herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Informationen zur Problembehebung finden Sie unter Fehlerbehebung AWS Client-VPN-Verbindungen mit macOS-Clients.

Important

Wenn der Client-VPN-Endpunkt für die Verwendung der SAML-based Verbundauthentifizierung konfiguriert wurde, können Sie den OpenVPN-based VPN-Client nicht verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Dies schließt alle ARM-based Architekturen ein. Wenn Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. Apple Silicon Macs oder ARM-based Windows-Geräte), müssen Sie SAML-based VPN-Endpunkte mit dem AWS bereitgestellten Client anstelle von OpenVPN-Clients verwenden.

Themen

Richten Sie eine ein AWS Client VPN Verbindung unter macOS

Sie können mit der Tunnelblick-Client-Anwendung auf einem macOS-Computer eine VPN-Verbindung herstellen.

Note

Weitere Informationen über die Tunnelblick-Clientanwendung für macOS finden Sie in der Tunnelblick-Dokumentation auf der Tunnelblick-Website.

So stellen Sie mit Tunnelblick eine VPN-Verbindung her

1. Starten Sie die Tunnelblick-Clientanwendung und wählen Sie I have configuration files aus.
2. Ziehen Sie die Konfigurationsdatei, die Sie von Ihrem VPN-Administrator erhalten haben, in den Bereich Configurations (Konfigurationen).
3. Wählen Sie die Konfigurationsdatei im Bereich Configurations und die Option Connect aus.

Um eine VPN-Verbindung herzustellen mit AWS Client VPN.

1. Starten Sie die OpenVPN-Anwendung und wählen Sie Import (Importieren), From local file... (Aus lokaler Datei...) aus.

2. Navigieren Sie zu der Konfigurationsdatei, die Sie von Ihrem VPN-Administrator erhalten haben, und wählen Sie Open (Öffnen) aus.

Connect zu einem her AWS Client VPN Endpunkt, der eine OpenVPN-Client-Anwendung verwendet

In diesen Abschnitten wird beschrieben, wie Sie eine VPN-Verbindung mit OpenVPN - Network Manager oder OpenVPN herstellen.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie eine Verbindung zu mehreren Profilen gleichzeitig herstellen möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Informationen zur Problembehebung finden Sie unter Fehlerbehebung AWS Client-VPN-Verbindungen mit Linux-based Clients.

> **Important**
>
> Wenn der Client-VPN-Endpunkt für die Verwendung der SAML-based Verbundauthentifizierung konfiguriert wurde, können Sie den OpenVPN-based VPN-Client nicht verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Dies schließt alle ARM-based Architekturen ein. Wenn Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. Apple Silicon Macs oder ARM-based Windows-Geräte), müssen Sie SAML-based VPN-Endpunkte mit dem AWS bereitgestellten Client anstelle von OpenVPN-Clients verwenden.

Themen

Richten Sie eine ein AWS Client VPN Verbindung unter Linux

Stellen Sie mithilfe der Network Manager-GUI auf einem Ubuntu-Computer oder der OpenVPN-Anwendung eine VPN-Verbindung her.

So stellen Sie eine VPN-Verbindung mit OpenVPN her - Network Manager

1. Installieren Sie das Netzwerkmanager-Modul mit folgendem Befehl.

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

2. Wechseln Sie zu Settings (Einstellungen), Network (Netzwerk).
3. Wählen Sie das Plus-Symbol (+) neben VPN aus. Wählen Sie dann Import from file... (Importieren aus Datei...) aus.
4. Navigieren Sie zu der Konfigurationsdatei, die Sie von Ihrem VPN-Administrator erhalten haben, und wählen Sie Open (Öffnen) aus.
5. Wählen Sie im Fenster VPN hinzufügen die Option Hinzufügen aus.
6. Starten Sie die Verbindung, indem Sie den Schalter neben dem hinzugefügten VPN-Profil aktivieren.

Um eine VPN-Verbindung mit OpenVPN herzustellen

1. Installieren Sie OpenVPN mit dem folgenden Befehl.

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

2. Starten Sie die Verbindung, indem Sie die Konfigurationsdatei laden, die Sie von Ihrem VPN-Administrator erhalten haben.

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

AWS Client VPN Verbindungen in Android- und iOS-Anwendungen

Important

Wenn der Client-VPN-Endpunkt für die Verwendung der SAML-based Verbundauthentifizierung konfiguriert wurde, können Sie den OpenVPN-based VPN-Client nicht verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen. Dies schließt alle ARM-based Architekturen ein. Wenn Sie ein Gerät mit einem ARM-Prozessor verwenden (z. B. Apple Silicon Macs oder ARM-based Windows-Geräte), müssen Sie SAML-

based VPN-Endpunkte mit dem AWS bereitgestellten Client anstelle von OpenVPN-Clients verwenden.

Die folgenden Informationen zeigen, wie Sie eine VPN-Verbindung mithilfe der OpenVPN-Clientanwendung auf einem Android- oder iOS-Gerät herstellen. Die Schritte für Android und iOS sind identisch.

> **Note**
>
> Weitere Informationen zum Herunterladen und Verwenden der OpenVPN-Client-Anwendung für iOS oder Android finden Sie im OpenVPN Connect-Benutzerhandbuch auf der OpenVPN-Website.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat. Wenn Sie sich mit mehreren Profilen gleichzeitig verbinden möchten, benötigen Sie für jedes Profil eine Konfigurationsdatei.

Um die Verbindung herzustellen, starten Sie die OpenVPN-Client-Anwendung, importieren Sie die Datei, die Sie von Ihrem Client-VPN-Administrator erhalten haben.

Fehlerbehebung AWS Client-VPN-Verbindungen

Nutzen Sie die folgenden Themen zur Behebung von Problemen, die auftreten können, wenn zur Herstellung einer Verbindung mit einem Client VPN-Endpunkt einer Client-Anwendung genutzt wird.

Themen

Client VPN-Endpunkt-Fehlerbehebung für Administratoren

Einige der Schritte in dieser Anleitung können von Ihnen selbst durchgeführt werden. Andere Schritte müssen von Ihrem Client VPN-Administrator auf dem Client-VPN-Endpunkt selbst durchgeführt werden. In den folgenden Abschnitten erfahren Sie, wann Sie sich an Ihren Administrator wenden müssen.

Weitere Informationen zur Behebung von Problemen mit Client VPN-Endpunkten finden Sie unter Fehlerbehebung bei Client VPN im AWS Client VPN -Administratorhandbuch.

Senden Sie Diagnoseprotokolle an AWS Support in der AWS bereitgestellter Client

Wenn Sie Probleme mit dem AWS bereitgestellten Client haben und sich zur Behebung der Probleme AWS Support an den Client wenden müssen, bietet der AWS angegebene Client die Möglichkeit, die Diagnoseprotokolle an diesen zu senden AWS Support. Die Option ist für die Windows-, macOS- und Linux-Client-Anwendungen verfügbar.

Bevor Sie die Dateien senden, müssen Sie dem Zugriff AWS Support auf Ihre Diagnoseprotokolle zustimmen. Nachdem Sie zugestimmt haben, geben wir Ihnen eine Referenznummer, die Sie angeben können, AWS Support damit sie sofort auf die Dateien zugreifen können.

Senden Sie Diagnoseprotokolle

Der AWS bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN-Client bezeichnet.

Um Diagnoseprotokolle mit dem zu senden AWS bereitgestellter Client für Windows

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie Hilfe, Diagnoseprotokolle senden.
3. Wählen Sie im Fenster Diagnoseprotokolle senden Ja.
4. Führen Sie im Fenster Diagnoseprotokolle senden einen der folgenden Vorgänge aus:

   - Um die Referenznummer in die Zwischenablage zu kopieren, wählen Sie Ja und wählen Sie dann OK.
   - Um die Referenznummer manuell zu verfolgen, wählen Sie Nein.

   Wenn Sie Kontakt aufnehmen AWS Support, müssen Sie ihnen die Referenznummer mitteilen.

Um Diagnoseprotokolle mit dem zu senden AWS bereitgestellter Client für macOS

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie Hilfe, Diagnoseprotokolle senden.
3. Wählen Sie im Fenster Diagnoseprotokolle senden Ja.
4. Notieren Sie sich die Referenznummer im Bestätigungsfenster und wählen Sie dann OK.

   Wenn Sie Kontakt aufnehmen AWS Support, müssen Sie ihnen die Referenznummer mitteilen.

Um Diagnoseprotokolle mit dem zu senden AWS bereitgestellter Client für Ubuntu

1. Öffnen Sie die AWS VPN-Client-App.
2. Wählen Sie Hilfe, Diagnoseprotokolle senden.
3. Wählen Sie im Fenster Diagnoseprotokolle senden Senden.
4. Notieren Sie sich die Referenznummer im Bestätigungsfenster. Sie haben die Wahl, die Informationen in Ihre Zwischenablage zu kopieren.

   Wenn Sie Kontakt aufnehmen AWS Support, müssen Sie ihnen die Referenznummer mitteilen.

Fehlerbehebung AWS Client-VPN-Verbindungen mit Windows-based Clients

Die folgenden Abschnitte enthalten Informationen zu Problemen, die auftreten können, wenn Sie Windows-based Clients verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen.

AWS bereitgestellte Client-Ereignisprotokolle

Der AWS bereitgestellte Client erstellt Ereignisprotokolle und speichert sie am folgenden Ort auf Ihrem Computer.

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

Die folgenden Arten von Protokollen sind verfügbar:

- Anwendungsprotokolle: Enthalten Informationen über die Anwendung. Diesen Protokollen wird das Präfix "aws_vpn_client_" vorangestellt.
- OpenVPN-Protokolle: Informationen über OpenVPN-Prozesse. Diesen Protokollen wird das Präfix 'ovpn_aws_vpn_client_' vorangestellt.

Der AWS bereitgestellte Client verwendet den Windows-Dienst, um Root-Operationen auszuführen. Windows-Serviceprotokolle werden an folgendem Ort auf Ihrem Computer gespeichert.

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

Themen zur Fehlerbehebung

- Client-Absturz tritt auf Dell PCs auf, die Windows 10 oder 11 verwenden
- OpenVPN GUI
- OpenVPN Connect-Client
- DNS kann nicht aufgelöst werden
- Fehlender PKI-Alias

Client kann keine Verbindung herstellen

Problem

Der AWS angegebene Client kann keine Verbindung zum Client-VPN-Endpunkt herstellen.

Ursache

Dieses Problem kann folgende Ursachen haben:

- Ein anderer OpenVPN-Prozess wird bereits auf Ihrem Computer ausgeführt, was den Client daran hindert, eine Verbindung herzustellen.
- Ihre Konfigurationsdatei (OVPN) ist ungültig.

Lösung

Überprüfen Sie, ob andere OpenVPN-Anwendungen auf Ihrem Computer ausgeführt werden. Wenn dies der Fall ist, stoppen oder beenden Sie diese Prozesse und versuchen Sie erneut, eine Verbindung mit dem Client VPN-Endpunkt herzustellen. Überprüfen Sie die OpenVPN-Protokolle auf Fehler und bitten Sie Ihren Client VPN-Administrator, die folgenden Informationen zu überprüfen:

- Dass die Konfigurationsdatei den korrekten Client-Schlüssel und das Zertifikat enthält. Weitere Informationen finden Sie unter Exportieren der Client-Konfiguration im AWS Client VPN - Administratorhandbuch.
- Dass die CRL weiterhin gültig ist. Weitere Informationen finden Sie unter Clients können keine Verbindung mit einem Client-VPN-Endpunkt herstellen im AWS Client VPN - Administratorhandbuch.

Der Client kann mit der Protokollmeldung „Keine TAP-Windows Adapter“ keine Verbindung herstellen

Problem

Der AWS angegebene Client kann keine Verbindung zum Client-VPN-Endpunkt herstellen und die folgende Fehlermeldung wird in den Anwendungsprotokollen angezeigt: „Es gibt keine TAP-Windows Adapter auf diesem System. Sie sollten in der Lage sein, einen TAP-Windows Adapter zu erstellen, indem Sie zu Start -> Alle Programme TAP-Windows -> -> Dienstprogramme -> Neuen TAP-Windows virtuellen Ethernet-Adapter hinzufügen gehen.

Lösung

Sie können dieses Problem beheben, indem Sie mindestens eine der folgenden Maßnahmen ergreifen:

- Starten Sie den TAP-Windows Adapter neu.
- Installieren Sie den TAP-Windows Treiber erneut.
- Erstellen Sie einen neuen TAP-Windows Adapter.

Client ist in einem Wiederverbindungszustand blockiert

Problem

Der AWS angegebene Client versucht, eine Verbindung zum Client-VPN-Endpunkt herzustellen, befindet sich jedoch in einem Zustand, in dem die Verbindung erneut hergestellt wird.

Ursache

Dieses Problem kann folgende Ursachen haben:

- Ihr Computer ist nicht mit dem Internet verbunden.
- Der DNS-Hostname wird nicht in eine IP-Adresse aufgelöst.
- Ein OpenVPN-Prozess versucht unbegrenzt, sich mit dem Endpunkt zu verbinden.

Lösung

Überprüfen Sie, ob Ihr Computer mit dem Internet verbunden ist. Bitten Sie Ihren Client VPN-Administrator zu überprüfen, ob die Direktive `remote` in der Konfigurationsdatei in eine gültige IP-

Adresse aufgelöst wird. Sie können die VPN-Sitzung auch trennen, indem Sie im AWS VPN-Client-Fenster auf Trennen klicken und erneut versuchen, eine Verbindung herzustellen.

VPN-Verbindungsprozess wird unerwartet beendet

Problem

Während der Verbindung zu einem Client VPN-Endpunkt wird der Client unerwartet beendet.

Ursache

TAP-Windows ist nicht auf Ihrem Computer installiert. Diese Software ist für die Ausführung des Clients erforderlich.

Lösung

Führen Sie das AWS mitgelieferte Client-Installationsprogramm erneut aus, um alle erforderlichen Abhängigkeiten zu installieren.

Anwendung startet nicht

Problem

Unter Windows 7 AWS wird der bereitgestellte Client nicht gestartet, wenn Sie versuchen, ihn zu öffnen.

Ursache

.NET Framework 4.7.2 oder höher ist nicht auf Ihrem Computer installiert. Dies ist erforderlich, um den Client auszuführen.

Lösung

Führen Sie das AWS bereitgestellte Client-Installationsprogramm erneut aus, um alle erforderlichen Abhängigkeiten zu installieren.

Client kann kein Profil erstellen

Problem

Sie erhalten folgenden Fehler, wenn Sie versuchen, ein Profil mit dem von AWS bereitgestellten Client zu erstellen.

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

Ursache

Wenn der Client VPN-Endpunkt die gegenseitige Authentifizierung verwendet, enthält die Konfigurationsdatei (OVPN) nicht das Client-Zertifikat und den Schlüssel.

Lösung

Stellen Sie sicher, dass Ihr Client VPN-Administrator das Client-Zertifikat und den Schlüssel zur Konfigurationsdatei hinzufügt. Weitere Informationen finden Sie unter Exportieren der Client-Konfiguration im AWS Client VPN -Administratorhandbuch.

VPN trennt die Verbindung mit einer Popup-Meldung

Problem

Das VPN trennt die Verbindung mit einer Popup-Meldung, die besagt: „Die VPN-Verbindung wird beendet, weil sich der Adressraum des lokalen Netzwerks, mit dem Ihr Gerät verbunden ist, geändert hat. Bitte stellen Sie eine neue VPN-Verbindung her.“

Ursache

TAP-Windows Der Adapter enthält nicht die erforderliche Beschreibung.

Lösung

Wenn das `Description` Feld unten nicht übereinstimmt, entfernen Sie zuerst den TAP-Windows Adapter und führen Sie dann das AWS mitgelieferte Client-Installationsprogramm erneut aus, um alle erforderlichen Abhängigkeiten zu installieren.

```
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
```

Client-Absturz tritt auf Dell PCs auf, die Windows 10 oder 11 verwenden

Problem

Auf bestimmten Dell PCs (Desktop und Laptop), auf denen Windows 10 oder 11 ausgeführt wird, kann ein Absturz auftreten, wenn Sie Ihr Dateisystem durchsuchen, um eine VPN-Konfigurationsdatei zu importieren. Wenn dieses Problem auftritt, werden in den Protokollen des AWS bereitgestellten Clients Meldungen wie die folgenden angezeigt:

```
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()
```

Ursache

Das Dell Backup and Recovery System in Windows 10 und 11 kann zu Konflikten mit dem AWS bereitgestellten Client führen, insbesondere mit den folgenden drei DLLs:

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

Lösung

Um dieses Problem zu vermeiden, stellen Sie zunächst sicher, dass Ihr Client über die neueste Version des AWS bereitgestellten Clients verfügt. Wechseln Sie zuAWS Client-VPN-Download und wenn eine neuere Version verfügbar ist, nehmen Sie ein Upgrade auf die neueste Version vor.

Führen Sie außerdem einen der folgenden Schritte aus:

- Wenn Sie die Dell Backup- and Recovery-Anwendung verwenden, stellen Sie sicher, dass sie auf dem neuesten Stand ist. Ein Forenbeitrag von Dell gibt an, dass dieses Problem in neueren Versionen der Anwendung behoben wurde.
- Wenn Sie die Dell Backup- and Recovery-Anwendung nicht verwenden, müssen weiterhin einige Maßnahmen ergriffen werden, wenn dieses Problem auftritt. Wenn Sie die Anwendung nicht aktualisieren möchten, können Sie alternativ die DLL-Dateien löschen oder umbenennen. Beachten Sie jedoch, dass dies verhindert, dass die Dell Backup- and Recovery-Anwendung vollständig funktioniert.

Löschen oder umbenennen der DLL-Dateien

1. Wechseln Sie zum Windows Explorer und navigieren Sie zu dem Speicherort, an dem Dell Backup and Recovery installiert ist. Es wird normalerweise am folgenden Speicherort installiert, aber Sie müssen möglicherweise suchen, um es zu finden.

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

2. Löschen Sie die folgenden DLL-Dateien manuell aus dem Installationsverzeichnis oder benennen Sie sie um. Jede der Aktionen verhindert, dass sie geladen werden.

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

   Sie können die Dateien umbenennen, indem Sie am Ende des Dateinamens „.bak“ hinzufügen, z. B. DBROverlayIconBackuped.dll.bak

OpenVPN GUI

Die folgenden Informationen zur Fehlerbehebung wurden mit den Versionen 11.10.0.0 und 11.11.0.0 der OpenVPN-GUI-Software unter Windows 10 Home (64-Bit) und Windows Server 2016 (64-Bit) getestet.

Die Konfigurationsdatei ist an folgendem Speicherort auf Ihrem Computer gespeichert.

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

Die Verbindungsprotokolle werden an folgendem Ort auf Ihrem Computer gespeichert.

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

OpenVPN Connect-Client

Die folgenden Informationen zur Fehlerbehebung wurden mit den Versionen 2.6.0.100 und 2.7.1.101 der OpenVPN-Connect-Client-Software unter Windows 10 Home (64-Bit) und Windows Server 2016 (64-Bit) getestet.

Die Konfigurationsdatei ist an folgendem Speicherort auf Ihrem Computer gespeichert.

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

Die Verbindungsprotokolle werden an folgendem Ort auf Ihrem Computer gespeichert.

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

DNS kann nicht aufgelöst werden

Problem

Die Verbindung scheitert mit folgendem Fehler.

```
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.
```

Ursache

Der DNS-Name kann nicht aufgelöst werden. Der Client muss dem DNS-Namen eine zufällige Zeichenfolge voranstellen, um das DNS-Caching zu verhindern. Einige Clients tun dies jedoch nicht.

Lösung

Siehe die Lösung für Auflösung des DNS-Namens des Client-VPN-Endpunkts im AWS Client VPN - Administratorhandbuch.

Fehlender PKI-Alias

Problem

Eine Verbindung zu einem Client VPN-Endpunkt, der keine gegenseitige Authentifizierung verwendet, schlägt mit folgendem Fehler fehl.

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

Ursache

Die OpenVPN-Connect-Client-Software hat ein bekanntes Problem, bei dem sie versucht, sich mit gegenseitiger Authentifizierung zu authentifizieren. Wenn die Konfigurationsdatei keinen Client-Schlüssel und kein Zertifikat enthält, schlägt die Authentifizierung fehl.

Lösung

Geben Sie einen zufälligen Clientschlüssel und ein Zertifikat in der Client VPN-Konfigurationsdatei an und importieren Sie die neue Konfiguration in die OpenVPN Connect-Clientsoftware. Verwenden Sie alternativ einen anderen Client, z. B. den OpenVPN-GUI-Client (v11.12.0.0) oder den Viscosity-Client (v.1.7.14).

Fehlerbehebung AWS Client-VPN-Verbindungen mit macOS-Clients

Die folgenden Abschnitte enthalten Informationen zu Protokollierung und Problemen, die bei der Verwendung von macOS-Clients auftreten können. Stellen Sie bitte sicher, dass Sie die neueste Version dieser Clients ausführen.

AWS bereitgestellte Client-Ereignisprotokolle

Der AWS bereitgestellte Client erstellt Ereignisprotokolle und speichert sie am folgenden Ort auf Ihrem Computer.

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

Die folgenden Arten von Protokollen sind verfügbar:

- Anwendungsprotokolle: Enthalten Informationen über die Anwendung. Diesen Protokollen wird das Präfix "aws_vpn_client_" vorangestellt.
- OpenVPN-Protokolle: Informationen über OpenVPN-Prozesse. Diesen Protokollen wird das Präfix 'ovpn_aws_vpn_client_' vorangestellt.

Der AWS bereitgestellte Client verwendet den Client-Daemon, um Root-Operationen durchzuführen. Die Daemon-Protokolle werden an den folgenden Speicherorten auf Ihrem Computer gespeichert: Die CRL ist noch gültig.

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

Der AWS bereitgestellte Client speichert die Konfigurationsdateien im folgenden Verzeichnis auf Ihrem Computer.

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

Themen zur Fehlerbehebung

- Client kann keine Verbindung herstellen
- Client ist in einem Wiederverbindungszustand blockiert
- Client kann kein Profil erstellen
- Hilfstool ist erforderlich (Fehler)
- Tunnelblick
- Der Verschlüsselungsalgorithmus 'AES-256-GCM' wurde nicht gefunden
- Verbindung reagiert nicht mehr und wird zurückgesetzt
- Erweiterte Schlüsselverwendung (Extended Key Usage, EKU)
- Abgelaufenes Zertifikat
- OpenVPN
- DNS kann nicht aufgelöst werden

Client kann keine Verbindung herstellen

Problem

Der AWS angegebene Client kann keine Verbindung zum Client-VPN-Endpunkt herstellen.

Ursache

Dieses Problem kann folgende Ursachen haben:

- Ein anderer OpenVPN-Prozess wird bereits auf Ihrem Computer ausgeführt, was den Client daran hindert, eine Verbindung herzustellen.
- Ihre Konfigurationsdatei (OVPN) ist ungültig.

Lösung

Überprüfen Sie, ob andere OpenVPN-Anwendungen auf Ihrem Computer ausgeführt werden. Wenn dies der Fall ist, stoppen oder beenden Sie diese Prozesse und versuchen Sie erneut, eine Verbindung mit dem Client VPN-Endpunkt herzustellen. Überprüfen Sie die OpenVPN-Protokolle auf Fehler und bitten Sie Ihren Client VPN-Administrator, die folgenden Informationen zu überprüfen:

- Dass die Konfigurationsdatei den korrekten Client-Schlüssel und das Zertifikat enthält. Weitere Informationen finden Sie unter Exportieren der Client-Konfiguration im AWS Client VPN - Administratorhandbuch.
- Dass die CRL weiterhin gültig ist. Weitere Informationen finden Sie unter Clients können keine Verbindung mit einem Client-VPN-Endpunkt herstellen im AWS Client VPN - Administratorhandbuch.

Client ist in einem Wiederverbindungszustand blockiert

Problem

Der AWS angegebene Client versucht, eine Verbindung zum Client-VPN-Endpunkt herzustellen, befindet sich jedoch in einem Zustand, in dem die Verbindung erneut hergestellt wird.

Ursache

Dieses Problem kann folgende Ursachen haben:

- Ihr Computer ist nicht mit dem Internet verbunden.
- Der DNS-Hostname wird nicht in eine IP-Adresse aufgelöst.
- Ein OpenVPN-Prozess versucht unbegrenzt, sich mit dem Endpunkt zu verbinden.

Lösung

Überprüfen Sie, ob Ihr Computer mit dem Internet verbunden ist. Bitten Sie Ihren Client VPN-Administrator zu überprüfen, ob die Direktive `remote` in der Konfigurationsdatei in eine gültige IP-Adresse aufgelöst wird. Sie können die VPN-Sitzung auch trennen, indem Sie im AWS VPN-Client-Fenster auf Trennen klicken und erneut versuchen, eine Verbindung herzustellen.

Client kann kein Profil erstellen

Problem

Sie erhalten folgenden Fehler, wenn Sie versuchen, ein Profil mit dem von AWS bereitgestellten Client zu erstellen.

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

Ursache

Wenn der Client VPN-Endpunkt die gegenseitige Authentifizierung verwendet, enthält die Konfigurationsdatei (OVPN) nicht das Client-Zertifikat und den Schlüssel.

Lösung

Stellen Sie sicher, dass Ihr Client VPN-Administrator das Client-Zertifikat und den Schlüssel zur Konfigurationsdatei hinzufügt. Weitere Informationen finden Sie unter Exportieren der Client-Konfiguration im AWS Client VPN -Administratorhandbuch.

Hilfstool ist erforderlich (Fehler)

Problem

Sie erhalten die folgende Fehlermeldung, wenn Sie versuchen, eine VPN-Verbindung herzustellen.

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

Lösung

Lesen Sie den folgenden Artikel auf AWS re:POST. Fehler „AWS VPN Client — Hilfstool ist erforderlich“

Tunnelblick

Die folgenden Informationen zur Fehlerbehebung wurden mit Version 3.7.8 (Build 5180) der Tunnelblick-Software unter macOS High Sierra 10.13.6 getestet.

Die Konfigurationsdatei für private Konfigurationen wird an folgendem Ort auf Ihrem Computer gespeichert.

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

Die Konfigurationsdatei für gemeinsam genutzte Konfigurationen wird an folgendem Ort auf Ihrem Computer gespeichert.

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

Die Verbindungsprotokolle werden an folgendem Ort auf Ihrem Computer gespeichert.

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

Um den Protokollumfang zu erhöhen, öffnen Sie die Tunnelblick-Anwendung, wählen Sie Settings (Einstellungen) aus und passen Sie den Wert für VPN log level (VPN-Protokollstufe) an.

Der Verschlüsselungsalgorithmus 'AES-256-GCM' wurde nicht gefunden

Problem

Die Verbindung schlägt fehl und gibt in den Protokollen den folgenden Fehler zurück.

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

Ursache

Die Anwendung verwendet eine OpenVPN-Version, die den Verschlüsselungsalgorithmus nicht unterstützt. AES-256-GCM

Lösung

Wählen Sie eine kompatible OpenVPN-Version aus, indem Sie wie folgt vorgehen:

1. Öffnen Sie die Tunnelblick-Anwendung.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie für OpenVPN version (OpenVPN-Version) die Option 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - OpenSSL-Version ist v1.0.2q) aus.

Verbindung reagiert nicht mehr und wird zurückgesetzt

Problem

Die Verbindung schlägt fehl und gibt in den Protokollen den folgenden Fehler zurück.

```
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
```

Ursache

Das Client-Zertifikat wurde widerrufen. Die Verbindung reagiert nach dem Versuch der Authentifizierung nicht mehr und wird schließlich serverseitig zurückgesetzt.

Lösung

Fordern Sie eine neue Konfigurationsdatei von Ihrem Client VPN-Administrator an.

Erweiterte Schlüsselverwendung (Extended Key Usage, EKU)

Problem

Die Verbindung schlägt fehl und gibt in den Protokollen den folgenden Fehler zurück.

```
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,,,,,
```

Ursache

Die Server-Authentifizierung war erfolgreich. Die Client-Authentifizierung schlägt jedoch fehl, weil im Client-Zertifikat das Feld für die erweiterte Schlüsselverwendung (EKU) für die Serverauthentifizierung aktiviert ist.

Lösung

Stellen Sie sicher, dass Sie das richtige Client-Zertifikat und den richtigen Schlüssel verwenden. Falls erforderlich, überprüfen Sie dies bei Ihrem Client VPN-Administrator. Dieser Fehler kann auftreten, wenn Sie das Server-Zertifikat und nicht das Client-Zertifikat für die Verbindung mit dem Client VPN-Endpunkt verwenden.

Abgelaufenes Zertifikat

Problem

Die Server-Authentifizierung ist erfolgreich, aber die Client-Authentifizierung schlägt mit folgendem Fehler fehl.

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

Ursache

Die Gültigkeit des Client-Zertifikats ist abgelaufen.

Lösung

Fordern Sie ein neues Client-Zertifikat von Ihrem Client VPN-Administrator an.

OpenVPN

Die folgenden Informationen zur Fehlerbehebung wurden mit Version 2.7.1.100 der OpenVPN-Connect-Client-Software unter macOS High Sierra 10.13.6 getestet.

Die Konfigurationsdatei ist an folgendem Speicherort auf Ihrem Computer gespeichert.

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

Die Verbindungsprotokolle werden an folgendem Ort auf Ihrem Computer gespeichert.

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

DNS kann nicht aufgelöst werden

Problem

Die Verbindung scheitert mit folgendem Fehler.

```
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
```

Ursache

OpenVPN Connect ist nicht in der Lage, den Client VPN-DNS-Namen aufzulösen.

Lösung

Siehe die Lösung für Auflösung des DNS-Namens des Client-VPN-Endpunkts im AWS Client VPN - Administratorhandbuch.

Fehlerbehebung AWS Client-VPN-Verbindungen mit Linux-based Clients

Die folgenden Abschnitte enthalten Informationen zur Protokollierung und zu Problemen, die bei der Verwendung von Linux-based Clients auftreten können. Stellen Sie bitte sicher, dass Sie die neueste Version dieser Clients ausführen.

Themen

- AWS bereitgestellte Client-Ereignisprotokolle

- DNS-Abfragen werden an einen Standard-Nameserver gesendet
- OpenVPN (Befehlszeile)
- OpenVPN über Network Manager (GUI)

AWS bereitgestellte Client-Ereignisprotokolle

Der AWS bereitgestellte Client speichert Protokolldateien und Konfigurationsdateien am folgenden Speicherort auf Ihrem System:

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

Der AWS bereitgestellte Client-Daemon-Prozess speichert Protokolldateien am folgenden Ort auf Ihrem System:

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

Sie können beispielsweise die folgenden Protokolldateien überprüfen, um Fehler in den up/down DNS-Skripts zu finden, die dazu führen, dass die Verbindung fehlschlägt:

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

DNS-Abfragen werden an einen Standard-Nameserver gesendet

Problem

Unter bestimmten Umständen, nachdem eine VPN-Verbindung hergestellt wurde, werden DNS-Abfragen weiterhin an den Standardsystemnameserver weitergeleitet, anstatt an die für den ClientVPN-Endpunkt konfigurierten Nameserver.

Ursache

Der Client interagiert mit systemd-resolved, einem auf Linux-Systemen verfügbaren Service, der als zentraler Bestandteil der DNS-Verwaltung dient. Der Service wird verwendet, um DNS-Server zu konfigurieren, die vom ClientVPN-Endpunkt übertragen werden. Das Problem tritt auf, wenn systemd-resolved nicht die höchste Priorität für DNS-Server festlegt, die vom ClientVPN-Endpunkt bereitgestellt werden. Stattdessen werden die Server an die vorhandene Liste der DNS-Server

angehängt, die auf dem lokalen System konfiguriert sind. Daher haben die ursprünglichen DNS-Server möglicherweise immer noch die höchste Priorität und werden daher zum Auflösen von DNS-Abfragen verwendet.

Lösung

1. Fügen Sie der OpenVPN-Konfigurationsdatei die folgende Anweisung auf der ersten Zeile hinzu, damit alle DNS-Abfragen an den VPN-Tunnel gesendet werden.

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

2. Verwenden Sie den Stub-Resolver, der von systemd-resolved bereitgestellt wird. Dafür müssen Sie symlink `/etc/resolv.conf` zu `/run/systemd/resolve/stub-resolv.conf` verwenden, indem Sie den folgenden Befehl auf dem System ausführen.

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

3. (Optional) Wenn Sie nicht möchten, dass systemd-resolved Proxy-DNS-Abfragen erstellt, sondern dass die Abfragen direkt an die echten DNS-Nameserver gesendet werden, verwenden Sie stattdessen symlink `/etc/resolv.conf` auf `/run/systemd/resolve/resolv.conf`.

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

   Dies kann sinnvoll sein, um die systemd-resolved-Konfiguration zu umgehen, z. B. für DNS-Antwort-Caching, DNS-Konfiguration pro Schnittstelle, DNSSec-Erzwingung usw. Diese Option ist besonders nützlich, wenn Sie einen öffentlichen DNS-Eintrag mit einem privaten Datensatz überschreiben müssen, wenn Sie mit VPN verbunden sind. Sie haben beispielsweise einen privaten DNS-Resolver in Ihrer privaten VPC mit einem Datensatz für www.beispiel.com, der in eine private IP aufgelöst wird. Diese Option kann verwendet werden, um den öffentlichen Datensatz von www.example.com zu überschreiben, der in eine öffentliche IP aufgelöst wird.

OpenVPN (Befehlszeile)

Problem

Die Verbindung funktioniert nicht ordnungsgemäß, da die DNS-Auflösung nicht funktioniert.

Ursache

Der DNS-Server ist am Client VPN-Endpunkt nicht konfiguriert oder er wird von der Client-Software nicht berücksichtigt.

Lösung

Überprüfen Sie mit den folgenden Schritten, ob der DNS-Server konfiguriert ist und korrekt funktioniert.

1. Stellen Sie sicher, dass ein DNS-Server-Eintrag in den Protokollen vorhanden ist. Im folgenden Beispiel wird in der letzten Zeile der (im Client VPN-Endpunkt konfigurierte) DNS-Server `192.168.0.2` zurückgegeben.

   ```
   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
   ```

   Wenn kein DNS-Server angegeben ist, bitten Sie Ihren Client VPN-Administrator, den Client VPN-Endpunkt zu ändern und sicherzustellen, dass für den Client VPN-Endpunkt ein DNS-Server (z. B. der VPC-DNS-Server) angegeben ist. Weitere Informationen finden Sie unter Client-VPN-Endpunkte im AWS Client VPN -Administratorhandbuch.

2. Stellen Sie sicher, dass das `resolvconf`-Paket installiert ist, indem Sie den folgenden Befehl ausführen.

   ```
   sudo apt list resolvconf
   ```

   Die Ausgabe sollte Folgendes zurückgeben.

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

   Wenn es nicht installiert ist, installieren Sie es mit dem folgenden Befehl.

   ```
   sudo apt install resolvconf
   ```

3. Öffnen Sie die Client VPN-Konfigurationsdatei (die OVPN-Datei) in einem Texteditor und fügen Sie die folgenden Zeilen hinzu.

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

Überprüfen Sie die Protokolle, um sicherzustellen, dass das `resolvconf`-Skript aufgerufen wurde. Die Protokolle sollten eine Zeile ähnlich der folgenden enthalten.

```
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 über Network Manager (GUI)

Problem

Bei Verwendung des Network Manager OpenVPN-Clients schlägt die Verbindung mit folgendem Fehler fehl.

```
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
```

Ursache

Das `remote-random-hostname`-Flag wird nicht beachtet. Der Client kann keine Verbindung mit dem `network-manager-gnome`-Paket herstellen.

Lösung

Siehe die Lösung für Auflösung des DNS-Namens des Client-VPN-Endpunkts im AWS Client VPN - Administratorhandbuch.

Häufig auftretende Problembehebung AWS Client-VPN-Probleme

Die folgenden sind häufige Probleme, die bei der Verwendung eines Clients zur Verbindung mit einem Client VPN-Endpunkt auftreten können.

TLS-Schlüsselaushandlung fehlgeschlagen

Problem

Die TLS-Aushandlung schlägt mit folgendem Fehler fehl.

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

Ursache

Dieses Problem kann folgende Ursachen haben:

- Firewallregeln blockieren UDP- oder TCP-Datenverkehr.
- Sie verwenden den falschen Client-Schlüssel und das falsche Zertifikat in Ihrer Konfigurationsdatei (OVPN).
- Die Client-Zertifikat-Widerrufsliste (CRL) ist abgelaufen.

Lösung

Überprüfen Sie, ob die Firewallregeln auf Ihrem Computer den ein- oder ausgehenden TCP- oder UDP-Datenverkehr über die Ports 443 oder 1194 blockieren. Bitten Sie Ihren Client VPN-Administrator, die folgenden Informationen zu überprüfen:

- Dass die Firewall-Regeln für den Client VPN-Endpunkt keinen TCP- oder UDP-Datenverkehr über die Ports 443 oder 1194 blockieren.
- Dass die Konfigurationsdatei den korrekten Client-Schlüssel und das Zertifikat enthält. Weitere Informationen finden Sie unter Exportieren der Client-Konfiguration im AWS Client VPN - Administratorhandbuch.
- Dass die CRL weiterhin gültig ist. Weitere Informationen finden Sie unter Clients können keine Verbindung mit einem Client-VPN-Endpunkt herstellen im AWS Client VPN - Administratorhandbuch.

Dokumentverlauf

In der folgenden Tabelle werden die Aktualisierungen des AWS Client VPN VPN-Benutzerhandbuchs beschrieben.

Änderung	Beschreibung	Datum
AWS bereitgestellter Client (5.3.3) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	18. Mai 2026
AWS bereitgestellter Client (5.3.5) für macOS ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. Mai 2026
AWS bereitgestellter Client (5.3.4) für Windows ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	26. März 2026
AWS bereitgestellter Client (5.3.3) für Windows ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	28. Februar 2026
AWS bereitgestellter Client (5.3.4) für macOS ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. Februar 2026
AWS bereitgestellter Client (5.3.2) für Windows ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. Februar 2026
AWS bereitgestellter Client (5.3.3) für macOS ARM64 und x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	26. Dezember 2025
AWS bereitgestellter Client (5.3.2) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. Dezember 2025

AWS bereitgestellter Client (5.3.2) für macOS x64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	27. Oktober 2025
AWS bereitgestellter Client (5.3.2) für macOS ARM64-Systeme veröffentlicht	Support für ARM64-based macOS-Betriebssysteme wurde jetzt hinzugefügt. Dies beinhaltet den Download einer neuen AWS Client VPN Version 5.3.2 speziell für macOS ARM64-Systeme. Weitere Informationen finden Sie unter Anforderungen für Client VPN für macOS und den AWS Client VPN Download-Link in den Versionshinweisen für macOS.	27. Oktober 2025
AWS bereitgestellter Client (5.3.1) für Windows x64 und Arm64 veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	30. September 2025
AWS der bereitgestellte Client für macOS unterstützt jetzt Tahoe (26.0)	Einzelheiten finden Sie unter Anforderungen.	25. September 2025
AWS bereitgestellter Client (5.3.1) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	25. September 2025
AWS bereitgestellter Client (5.3.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	9. September 2025

AWS bereitgestellter Client (5.3.0) für Windows Arm64-Systeme veröffentlicht	Support für Arm64-based Windows-Betriebssysteme wurde jetzt hinzugefügt. Dies beinhaltet einen Download der neuen AWS Client VPN Version 5.3.0 speziell für Windows Arm64-Systeme. Weitere Informationen finden Sie unter Anforderungen für Client VPN AWS Client VPN für Windows und den Download-Link in den Versionshinweisen für Windows.	26. August 2025
AWS bereitgestellter Client (5.3.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. August 2025
AWS bereitgestellter Client (5.3.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. August 2025
AWS bereitgestellter Client (5.3.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. August 2025
AWS bereitgestellter Client (5.2.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	18. Juni 2025
AWS bereitgestellter Client (5.2.2) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	2. Juni 2025
AWS bereitgestellter Client (5.2.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. April 2025

AWS bereitgestellter Client (5.2.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. April 2025
AWS bereitgestellter Client (5.2.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. April 2025
AWS bereitgestellter Client (5.2.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. April 2025
AWS bereitgestellter Client (5.1.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. März 2025
AWS bereitgestellter Client (5.1.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. März 2025
AWS bereitgestellter Client (5.1.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. März 2025
Unterstützung für macOS Monterey wurde entfernt und Unterstützung für macOS Sonoma (14.0) hinzugefügt	Einzelheiten finden Sie unter Anforderungen für Client VPN für macOS.	12. März 2025
Die Unterstützung für Ubuntu 18.0.4 (LTS) und Ubuntu 20.04 LTS (nur AMD64) wurde entfernt	Einzelheiten finden Sie unter Anforderungen für Client VPN für Linux.	12. März 2025
AWS bereitgestellter Client (5.0.3) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. März 2025

AWS bereitgestellter Client (5.0.2) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	24. Februar 2025
AWS bereitgestellter Client (5.0.2) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. Februar 2025
AWS bereitgestellter Client (5.0.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	30. Januar 2025
AWS bereitgestellter Client (5.0.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	22. Januar 2025
Der AWS bereitgestellte Client unterstützt jetzt bis zu fünf gleichzeitige Verbindungen	Einzelheiten finden Sie unter Support für gleichzeitige Verbindungen mit einem AWS bereitgestellten Client.	21. Januar 2025
AWS bereitgestellter Client (5.0.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. Januar 2025
AWS bereitgestellter Client (5.0.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. Januar 2025
AWS bereitgestellter Client (5.0.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. November 2024
AWS bereitgestellter Client (4.1.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. November 2024

AWS bereitgestellter Client (4.1.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. November 2024
AWS bereitgestellter Client (4.1.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. November 2024
AWS bereitgestellter Client (4.0.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	25. September 2024
AWS bereitgestellter Client (4.0.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	25. September 2024
AWS bereitgestellter Client (4.0.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	25. September 2024
AWS bereitgestellter Client (3.15.1) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	4. September 2024
AWS bereitgestellter Client (3.14.2) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	4. September 2024
AWS bereitgestellter Client (3.12.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	4. September 2024
AWS bereitgestellter Client (3.14.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	22. August 2024
AWS bereitgestellter Client (3.15.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. August 2024

AWS bereitgestellter Client (3.14.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. August 2024
AWS bereitgestellter Client (3.12.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	12. August 2024
AWS bereitgestellter Client (3.14.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	29. Juli 2024
AWS bereitgestellter Client (3.13.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	29. Juli 2024
AWS bereitgestellter Client (3.11.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	29. Juli 2024
AWS bereitgestellter Client (3.12.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	18. Juli 2024
AWS bereitgestellter Client (3.13.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. Mai 2024
AWS bereitgestellter Client (3.12.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. Mai 2024
AWS bereitgestellter Client (3.10.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	21. Mai 2024
AWS bereitgestellter Client (3.9.2) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	11. April 2024

AWS bereitgestellter Client (3.12.2) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	11. April 2024
AWS bereitgestellter Client (3.11.2) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	11. April 2024
AWS bereitgestellter Client (3.9.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS bereitgestellter Client (3.12.1) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS bereitgestellter Client (3.11.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS bereitgestellter Client (3.12.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	19. Dezember 2023
AWS bereitgestellter Client (3.9.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS bereitgestellter Client (3.11.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS bereitgestellter Client (3.11.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS bereitgestellter Client (3.10.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023

AWS bereitgestellter Client (3.9.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	24. August 2023
AWS bereitgestellter Client (3.8.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	24. August 2023
AWS bereitgestellter Client (3.10.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	24. August 2023
AWS bereitgestellter Client (3.9.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. August 2023
AWS bereitgestellter Client (3.8.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. August 2023
AWS bereitgestellter Client (3.7.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. August 2023
AWS bereitgestellter Client (3.8.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023
AWS bereitgestellter Client (3.7.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023
AWS bereitgestellter Client (3.7.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023
AWS bereitgestellter Client (3.6.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023

AWS bereitgestellter Client (3.6.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023
AWS bereitgestellter Client (3.5.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	15. Juli 2023
AWS bereitgestellter Client (3.6.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. Juli 2023
AWS bereitgestellter Client (3.5.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. Juli 2023
AWS bereitgestellter Client (3.4.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. Juli 2023
AWS bereitgestellter Client (3.3.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	27. April 2023
AWS bereitgestellter Client (3.5.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	03. April 2023
AWS bereitgestellter Client (3.4.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	28. März 2023
AWS bereitgestellter Client (3.3.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	17. März 2023
AWS bereitgestellter Client (3.4.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	14. Februar 2023

AWS bereitgestellter Client (3.2.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	23. Januar 2023
AWS bereitgestellter Client (3.2.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	23. Januar 2023
AWS bereitgestellter Client (3.1.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	23. Mai 2022
AWS bereitgestellter Client (3.1.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	23. Mai 2022
AWS bereitgestellter Client (3.1.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	23. Mai 2022
AWS bereitgestellter Client (3.0.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. März 2022
AWS bereitgestellter Client (3.0.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. März 2022
AWS bereitgestellter Client (3.0.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	3. März 2022
AWS bereitgestellter Client (2.0.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. Januar 2022
AWS bereitgestellter Client (2.0.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. Januar 2022

AWS bereitgestellter Client (2.0.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. Januar 2022
AWS bereitgestellter Client (1.4.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	9. November 2021
AWS bereitgestellter Client für Windows (1.3.7) veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. November 2021
AWS bereitgestellter Client (1.0.3) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. November 2021
AWS bereitgestellter Client (1.0.2) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	28. September 2021
AWS bereitgestellter Client für Windows (1.3.6) und macOS (1.3.5) veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. September 2021
AWS bereitgestellter Client für Ubuntu 18.04 LTS und Ubuntu 20.04 LTS veröffentlicht	Sie können den von AWS-bereitgestellten Client auf Ubuntu 18.04 LTS und Ubuntu 20.04 LTS verwenden.	11. Juni 2021
Unterstützung von OpenVPN mithilfe eines Zertifikats aus dem Windows Certificate System Store	Sie können OpenVPN mithilfe eines Zertifikats aus dem Windows Certificate System Store verwenden.	25. Februar 2021
Self-service Portal	Sie können auf ein Self-Service-Portal zugreifen, um die neueste AWS bereitgestellte Client- und Konfigurationsdatei abzurufen.	29. Oktober 2020

AWS bereitgestellter Kunde	Sie können den AWS bereitgestellten Client verwenden, um eine Verbindung zu einem Client-VPN-Endpunkt herzustellen.	4. Februar 2020
Erstversion	In dieser Version wird AWS Client VPN eingeführt.	18. Dezember 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.