Benutzerhandbuch

AWS Client VPN

AWS Client VPN: Benutzerhandbuch

Table of Contents

Was ist AWS Client-VPN?

AWS Client-VPN ist ein verwalteter clientbasierter VPN-Service, der es Ihnen ermöglicht, im On-Premise-Netzwerk auf Ihre AWS-Ressourcen zuzugreifen.

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

Komponenten

Nachfolgend finden Sie 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 sowie die Zertifikate, die für das Einrichten einer VPN-Verbindung erforderlich sind. Sie laden diese Datei in die von Ihnen gewählte VPN-Client-Anwendung.

Weitere Ressourcen

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

Erste Schritte mit 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.

Themen

Prerequisites

Zum Herstellen einer VPN-Verbindung ist Folgendes erforderlich:

- Zugriff auf das Internet
- Ein unterstütztes Gerät
- 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.

Der von AWS bereitgestellte Client wird für Windows, macOS, Ubuntu 18.04 LTS und Ubuntu 20.04 LTS unterstützt. Sie können den Client unter AWS Client VPN Download herunterladen.

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 Client VPN-Endpunkt-Konfigurationsdatei 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 von AWS bereitgestellten Clients und die neueste Version der Client VPN-Endpunkt-Konfigurationsdatei selbst herunterladen. Weitere Informationen finden Sie unter Verwendung des Self-Service-Portals.

Schritt 3: Verbinden mit dem VPN

Importieren Sie die Client VPN-Endpunkt-Konfigurationsdatei in den von AWS bereitgestellten Client oder in Ihre OpenVPN-Client-Anwendung und verbinden Sie sich mit dem VPN. Schritte zum Herstellen einer Verbindung zu einem VPN finden Sie unter den folgenden Themen:

- Verbinden mit einem von AWS bereitgestellten Client
- Verbindung mit einem OpenVPN-Client herstellen

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.

Bei Client VPN-Endpunkten, die SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, öffnet der von 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.

Verwendung des Self-Service-Portals

Ihr Client-VPN-Endpunkt-Administrator kann ein Self-Service-Portal für den Client-VPN-Endpunkt konfigurieren. Das Self-Service-Portal ist eine Webseite, auf der Sie die neueste Version des von AWS bereitgestellten Clients und die neueste Version der Client-VPN-Endpunkt-Konfigurationsdatei herunterladen können. Weitere Informationen zur Konfiguration des Self-Service-Portals finden Sie unter Client-VPN-Endpunkte im AWS Client VPN-Administratorhandbuch.

Bevor Sie beginnen, müssen Sie die ID des Client-VPN-Endpunkts haben. Ihr Client-VPN-Endpunkt-Administrator kann Ihnen die ID oder eine Self-Service-Portal-URL zur Verfügung stellen, die die ID enthält.

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 Ihnen von Ihrem Administrator bereitgestellt wurde.
2. Geben Sie bei Bedarf die ID des Client-VPN-Endpunkts ein, z. B, `cvpn-endpoint-0123456abcd123456`. Wählen Sie Next.
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.
   - Laden Sie die neueste Version des von AWS bereitgestellten Clients für Ihre Plattform herunter.

Verbinden mit einem von AWS bereitgestellten Client

Sie können über den von AWS bereitgestellten Client eine Verbindung zu einem Client-VPN-Endpunkt herstellen. Der von AWS bereitgestellte Client wird für Windows, macOS, Ubuntu 18.04 LTS und Ubuntu 20.04 LTS unterstützt.

Clients

- AWS Client VPN für Windows
- AWS Client VPN für macOS
- AWS Client VPN für Linux

OpenVPN-Richtlinien

Der von AWS bereitgestellte Client unterstützt die folgenden OpenVPN-Richtlinien:

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

- Schlüssel
- nobind
- persist-key
- persist-tun
- ping
- 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
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN für Windows

Das folgende Verfahren zeigt, wie Sie eine VPN-Verbindung mit dem von AWS bereitgestellten Client für Windows herstellen. Sie können den Client unter AWS Client VPN-Download herunterladen und installieren. Der AWS von bereitgestellte Client unterstützt keine automatischen Updates.

Inhalt

Voraussetzungen

Um den von AWS bereitgestellten Client für Windows verwenden zu können, sind folgende Schritte erforderlich:

- Windows 10-64-Bit-Betriebssystem, x64-Prozessor
- .NET Framework 4.7.2 oder höher

Der Client reserviert den TCP-Port 8096 auf Ihrem Computer. Für Client VPN-Endpunkte, die eine SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client TCP-Port 35001.

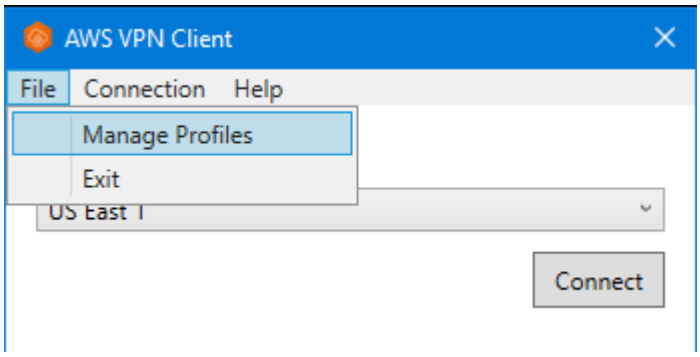
Bevor Sie beginnen, stellen Sie sicher, dass Ihr Client VPN-Administrator einen Client VPN-Endpunkt erstellt und Ihnen die Client VPN-Endpunkt-Konfigurationsdatei zur Verfügung gestellt hat.

Herstellen von Verbindungen

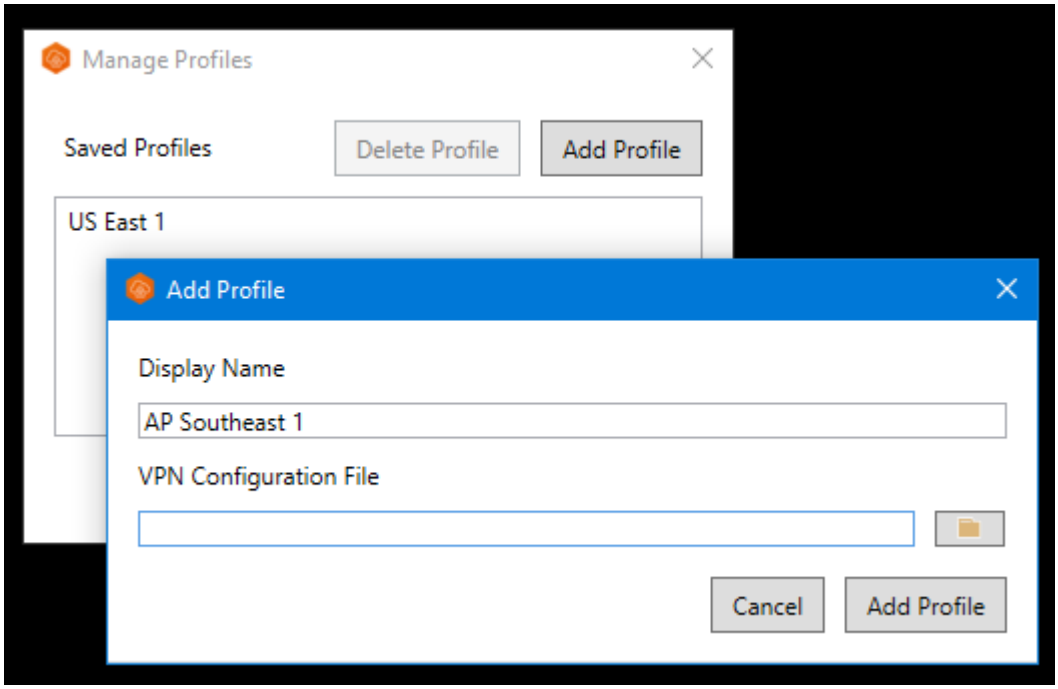
Bevor Sie beginnen, stellen Sie sicher, dass Sie die Anforderungen gelesen haben. Der AWS von bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN Client bezeichnet.

So stellen Sie eine Verbindung mit dem von AWS bereitgestellten Client für Windows her

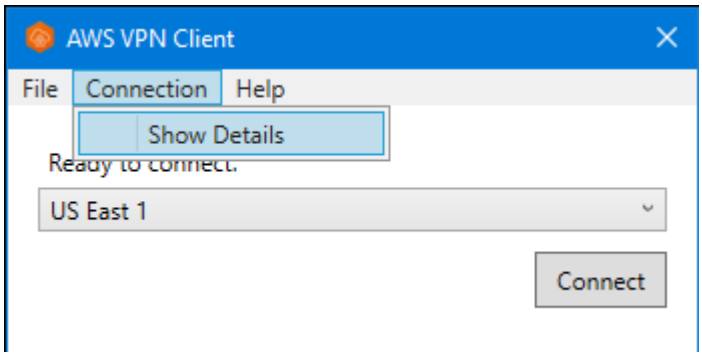
1. Öffnen Sie die AWS VPN Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.



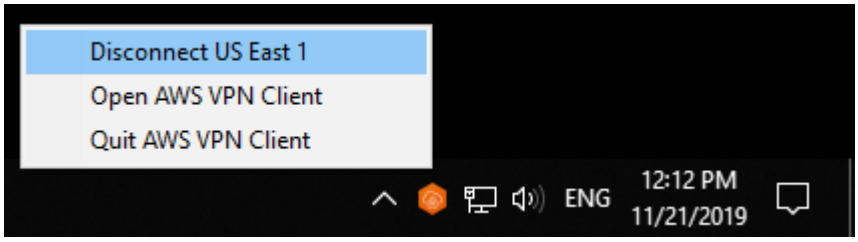
3. Wählen Sie Add Profile (Profil hinzufügen) aus.



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. Vergewissern Sie sich im Fenster AWS VPN -Client, dass Ihr Profil ausgewählt ist, und wählen Sie dann Connect (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.
7. Um Statistiken für Ihre Verbindung anzuzeigen, wählen Sie Connections (Verbindung), Show details (Details anzeigen) aus.



8. Um die Verbindung zu trennen, wählen Sie im Fenster AWS VPN Client die Option Disconnect (Trennen) aus. Alternativ wählen Sie das Client-Symbol in der Windows-Taskleiste und dann Disconnect (Trennen) aus.



Versionshinweise

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

Version	Änderungen	Datum	Link und SHA256 herunterladen
3.11.1	• Verbesserter Sicherheitsstatus.	16. Februar 2024	Version 3.11.1 herunterladen sha256: fb67b60aa837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Es wurde ein Verbindungsproblem behoben, das durch Windows-VMs verursacht wurde. • 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	Datum	Link und SHA256 herunterladen
3.10.0	• Es wurde ein Verbindungsproblem behoben, das auftrat, wenn NAT64 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	Datum	Link und SHA256 herunterladen
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	Datum	Link und SHA256 herunterladen
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	Datum	Link und SHA256 herunterladen
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 IPv6-Leckschutz hinzu, wenn es konfiguriert ist. • 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	Datum	Link und SHA256 herunterladen
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	Datum	Link und SHA256 herunterladen
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

Das folgende Verfahren zeigt, wie Sie eine VPN-Verbindung mit dem von AWS bereitgestellten Client für macOS herstellen. Sie können den Client unter AWS Client VPN-Download herunterladen und installieren. Der AWS von bereitgestellte Client unterstützt keine automatischen Updates.

Inhalt

Voraussetzungen

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

- macOS Big Sur (11.0), Monterey (12.0) oder Ventura (13.0).
- Mit x86_64-Prozessor kompatibel.
- Der Client reserviert den TCP-Port 8096 auf Ihrem Computer.

- Für Client VPN-Endpunkte, die eine SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client TCP-Port 35001.

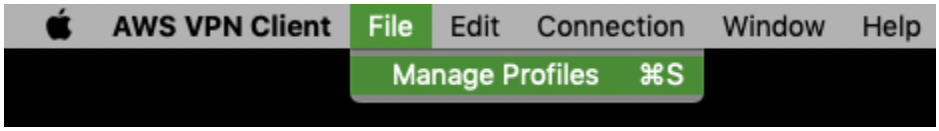
Herstellen von Verbindungen

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.

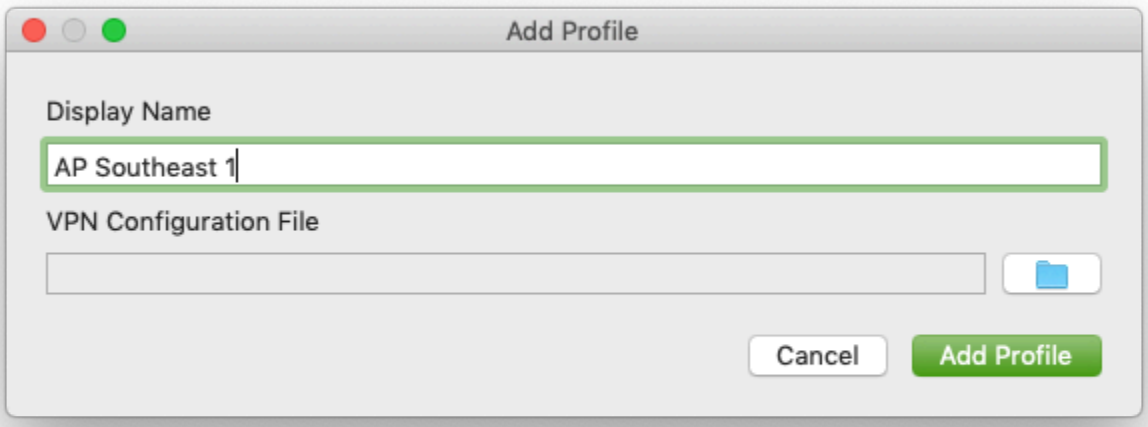
Stellen Sie außerdem sicher, dass Sie die Anforderungen gelesen haben. Der AWS von bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN Client bezeichnet.

So stellen Sie eine Verbindung mit dem von AWS bereitgestellten Client für macOS her

1. Öffnen Sie die AWS VPN Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.



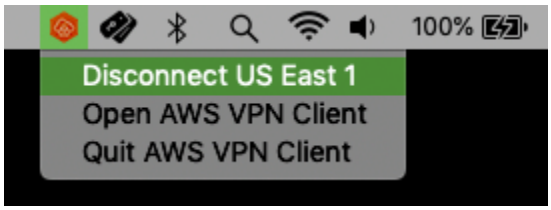
3. Wählen Sie Add Profile (Profil hinzufügen) aus.
4. Geben Sie für Display name (Anzeigelname) einen Namen für das Profil ein.



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. Vergewissern Sie sich im Fenster AWS VPN Client, dass Ihr Profil ausgewählt ist, und wählen Sie dann Connect (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.
8. Um Statistiken für Ihre Verbindung anzuzeigen, wählen Sie Connections (Verbindung), Show details (Details anzeigen) aus.

9. Um die Verbindung zu trennen, wählen Sie im Fenster AWS VPN Client die Option Disconnect (Trennen) aus. Wählen Sie alternativ das Client-Symbol in der Menüleiste und dann Trennen <your-profile-name> aus.



Versionshinweise

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

Version	Änderungen	Datum	Download-Link
3.9.1	• Fortschrittsleiste für das Herunterladen von Anwendungsaktualisierungen behoben. • Verbesserter Sicherheitsstatus.	16. Februar 2024	Version 3.9.1 herunterladen sha256: 9bba4b27a635e75038703e2cf4cd814aa75306179fac8

Version	Änderungen	Datum	Download-Link
			e500e2c7a f4e899e971
3.9.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.9.0 herunterladen sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8
3.8.0	• Es wurde ein Verbindungsproblem behoben, das auftrat, wenn NAT64 im Client-Netzwerk aktiviert war. • Kleinere Fehlerbehebungen und Verbesserungen.	24. August 2023	Version 3.8.0 herunterladen sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461

Version	Änderungen	Datum	Download-Link
3.7.0	• Verbesserter Sicherheitsstatus.	3. August 2023	Version 3.7.0 herunterladen sha256: 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a
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 Installat ion neuer Client-Versionen bei Verfügbarkeit hinzugefügt.	23. Januar 2023	Nicht mehr unterstützt

Version	Änderungen	Datum	Download-Link
3.1.0	• Unterstützung für macOS Monterey wurde hinzugefügt. • 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 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 2022	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.

Version	Änderungen	Datum	Download-Link
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.
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.

Version	Änderungen	Datum	Download-Link
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.
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 2020	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
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 2020	Nicht mehr unterstützt.
1.2.2	Kleinere Fehlerbehebungen und Verbesserungen.	12. August 2020	Nicht mehr unterstützt.
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.

Version	Änderungen	Datum	Download-Link
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

Die folgenden Verfahren zeigen, wie Sie den von AWS bereitgestellten Client für Linux installieren und eine VPN-Verbindung mit dem von AWS bereitgestellten Client herstellen. Der AWS von bereitgestellte Client für Linux unterstützt keine automatischen Updates.

Inhalt

Voraussetzungen

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

- Ubuntu 18.04 LTS oder Ubuntu 20.04 LTS (nur AMD64)

Der Client reserviert den TCP-Port 8096 auf Ihrem Computer. Für Client VPN-Endpunkte, die eine SAML-basierte Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client TCP-Port 35001.

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.

Installation

Es gibt mehrere Methoden, mit denen der von 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 Paket-Repository

1. Fügen Sie dem Betriebssystem Ubuntu den öffentlichen Schlüssel des AWS VPN Clients 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 entsprechenden Befehl, um das Repository Ihrem Ubuntu-Betriebssystem hinzuzufügen, abhängig von Ihrer Ubuntu-Version:

   Ubuntu 18.04

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

   Ubuntu 20.04

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

3. 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 von AWS bereitgestellten Client für Linux zu installieren.

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

Option 2 – Installation über die 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 von AWS bereitgestellten Client für Linux mit dem `dpkg` Dienstprogramm .

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

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

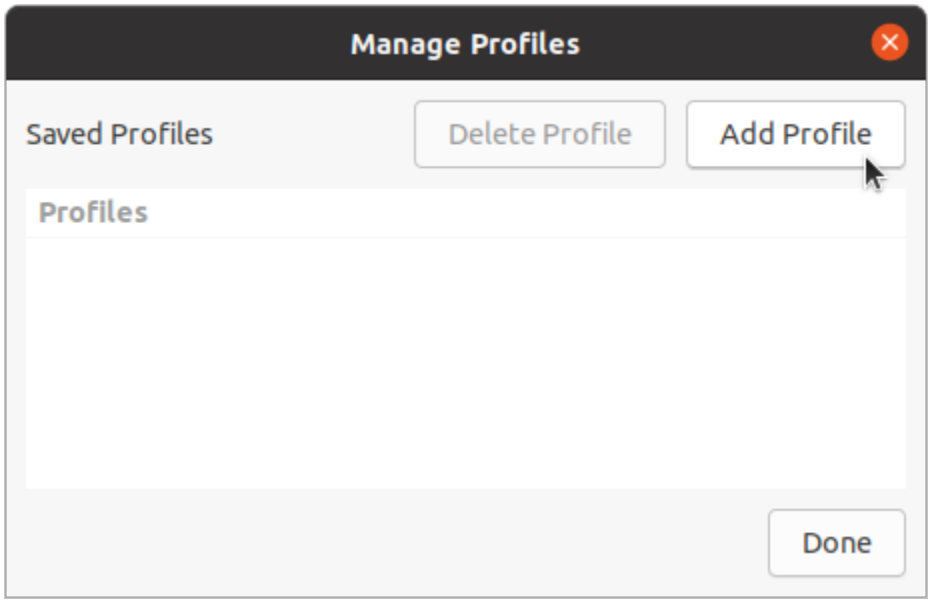
1. Laden Sie die DEB-Paketdatei von AWS Client VPN herunterladen herunter.
2. Verwenden Sie nach dem Herunterladen der DEB-Paketdatei das Ubuntu Software Center, um das Paket zu installieren. Befolgen Sie die Schritte für die Installation von einem eigenständigen DEB-Paket mit dem Ubuntu Software Center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

Herstellen von Verbindungen

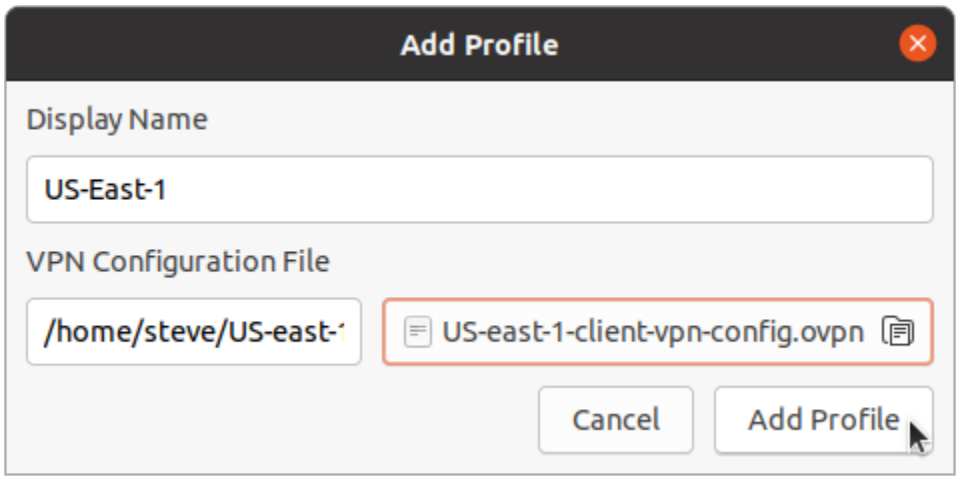
Der AWS von bereitgestellte Client wird in den folgenden Schritten auch als AWS VPN Client bezeichnet.

So stellen Sie eine Verbindung mit dem von AWS bereitgestellten Client für Linux her

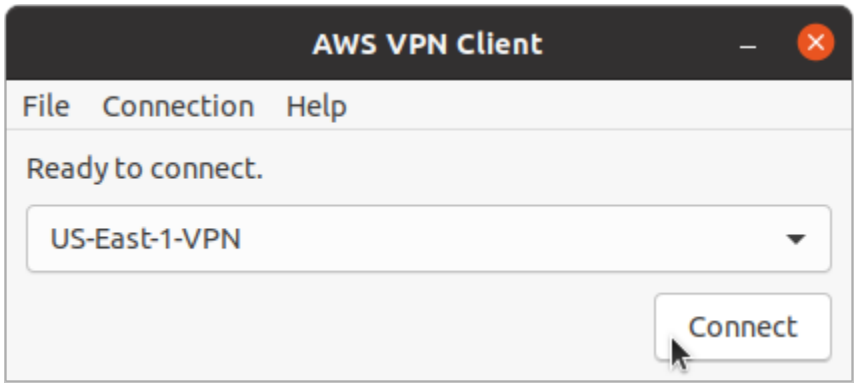
1. Öffnen Sie die AWS VPN Client-App.
2. Wählen Sie File (Datei), Manage Profiles (Profile verwalten) aus.
3. Wählen Sie Add Profile (Profil hinzufügen) aus.



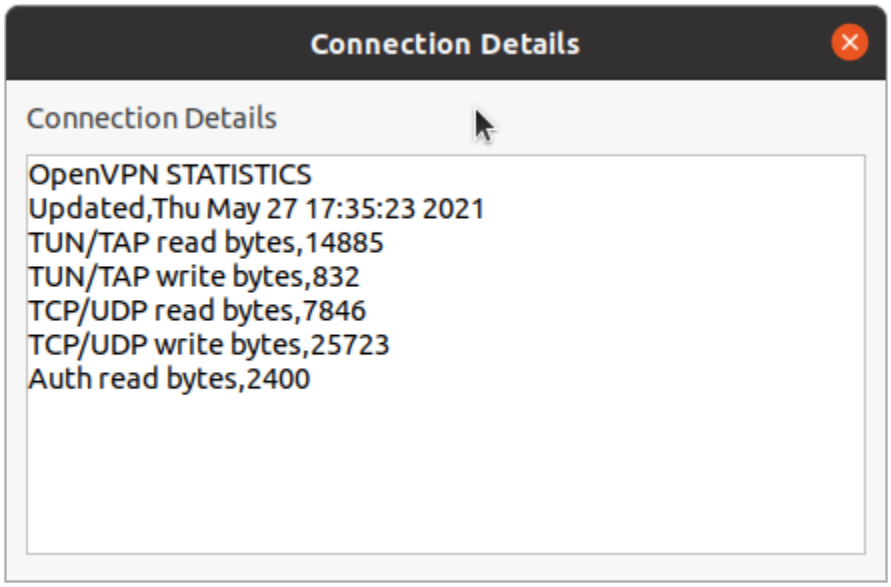
4. Geben Sie für Display name (Anzeigelname) einen Namen für das Profil ein.
5. Suchen Sie unter VPN Configuration File (VPN-Konfigurationsdatei) nach der Konfigurationsdatei, die Sie von Ihrem Client-VPN-Administrator erhalten haben. Klicken Sie auf Open.
6. Wählen Sie Add Profile (Profil hinzufügen) aus.



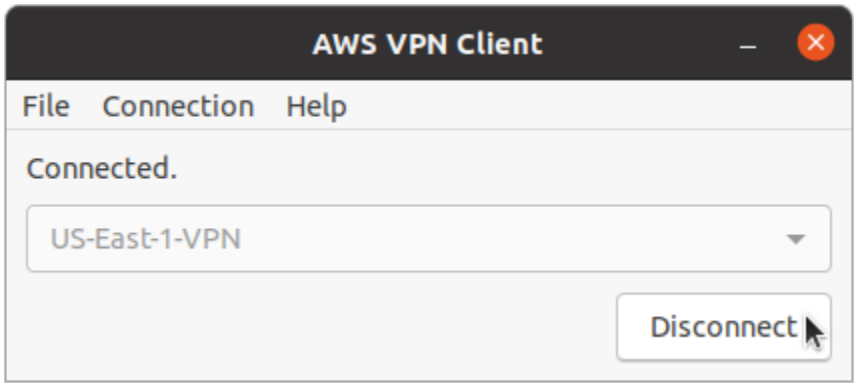
7. Vergewissern Sie sich im Fenster AWS VPN -Client, dass Ihr Profil ausgewählt ist, und wählen Sie dann Connect (Verbinden) aus. Wenn der Client VPN-Endpunkt für die Verwendung der auf Anmeldeinformationen basierenden Authentifizierung konfiguriert wurde, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben.



8. Um Statistiken für Ihre Verbindung anzuzeigen, wählen Sie Connections (Verbindung), Show details (Details anzeigen) aus.



9. Um die Verbindung zu trennen, wählen Sie im Fenster AWS VPN Client die Option Disconnect (Trennen) aus.



Versionshinweise

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

Version	Änderungen	Datum	Download-Link
3.12.1	• Verbesserter Sicherheitsstatus.	16. Februar 2024	Version 3.12.1 herunterladen sha256: 547c4ffd3 e35c54db8 e0b792aed 9de1510f6 f31a6009e 55b8af4f0 c2f5cf31d0
3.12.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben.	19. Dezember 2023	Version 3.12.0 herunterladen sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Rollback für „Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben“. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.11.0 herunterladen sha256:86 c0fa1bf1c 971940828 35a739ec7 f1c87e540

Version	Änderungen	Datum	Download-Link
			194955f41 4a35c679b 94538970
3.10.0	• Es wurden Verbindungsprobleme bei einigen LAN-Konfigurationen behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.10.0 herunterladen sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 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: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 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.

Verbindung mit einem OpenVPN-Client herstellen

Sie können mithilfe allgemeiner Open-VPN-Client-Anwendungen eine Verbindung zu einem Client-VPN-Endpunkt herstellen.

> **Note**
>
> Für eine SAML-basierte Verbundauthentifizierung müssen Sie den von AWS bereitgestellten Client verwenden, um eine Verbindung mit einem Client-VPN-Endpunkt herzustellen. Weitere Informationen finden Sie unter Verbinden mit einem von AWS bereitgestellten Client, oder wenden Sie sich an Ihren VPN-Administrator.

Clientanwendungen

- Herstellen einer Verbindung mit einer Windows-Client-Anwendung
- Verbinden Sie sich mit einer Android- oder iOS-VPN-Client-Anwendung
- Verbinden mit einer macOS-Client-Anwendung
- Herstellen einer Verbindung mit einer OpenVPN-Client-Anwendung

Herstellen einer Verbindung mit einer Windows-Client-Anwendung

Die folgenden Prozeduren zeigen, wie eine VPN-Verbindung mit Windows-basierten VPN-Clients hergestellt wird.

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.

Informationen zur Problembehebung finden Sie unter Windows-Fehlerbehebung.

OpenVPN verwendet ein Zertifikat aus dem Windows Certificate System Store

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.

Verwenden der Cryptoapicert-Option mit OpenVPN

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 Berechtigungen zum Anzeigen des Speichers für lokale Computerzertifikate auf der Microsoft-Technet-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 unter Gewusst wie: Abrufen des Fingerabdrucks eines Zertifikats auf der Microsoft-Technet-Website.

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

Nachdem Sie die Konfiguration abgeschlossen haben, verwenden Sie OpenVPN, um eine Verbindung herzustellen.

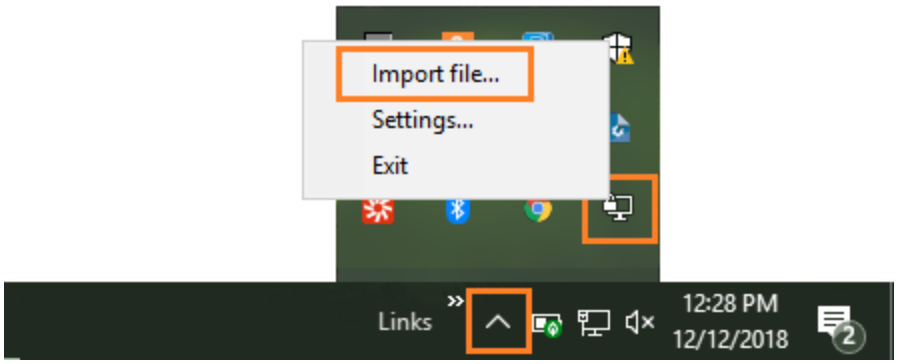
OpenVPN GUI

Das folgende Verfahren zeigt, wie Sie eine VPN-Verbindung mithilfe der OpenVPN-GUI-Clientanwendung auf einem Windows-Computer herstellen.

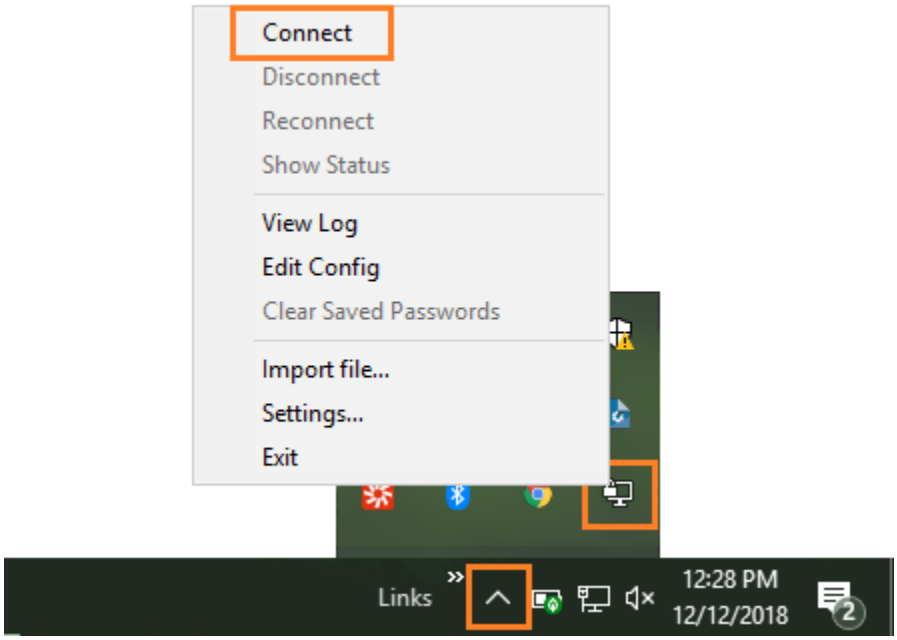
> **Note**
>
> Informationen über die OpenVPN-Client-Anwendung finden Sie unter Community-Downloads auf der OpenVPN-Website.

So stellen Sie eine VPN-Verbindung her

1. Starten Sie die OpenVPN-Clientanwendung.
2. Klicken Sie in der Windows-Taskleiste auf die Option für Show/Hide icons (Symbole anzeigen/ausblenden), klicken Sie mit der rechten Maustaste auf OpenVPN GUI und wählen Sie Import file (Datei importieren) aus.



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 auf die Option für Show/Hide icons (Symbole anzeigen/ausblenden), klicken Sie mit der rechten Maustaste auf OpenVPN GUI und wählen Sie Connect (Verbinden) aus.



OpenVPN Connect-Client

Das folgende Verfahren zeigt, wie Sie eine VPN-Verbindung mithilfe der OpenVPN-Clientanwendung auf einem Windows-Computer herstellen.

> **Note**
>
> Weitere Informationen finden Sie unter Verbindung zum Zugriffsserver mit Windows auf der OpenVPN-Website.

So stellen Sie eine VPN-Verbindung her

1. Starten Sie die OpenVPN Connect Client-Anwendung.
2. Wählen Sie in der Windows-Taskleiste Show/Hide icons (Symbole ein-/ausblenden) aus, klicken Sie mit der rechten Maustaste auf OpenVPN und wählen Sie Import profile (Profil importieren) aus.
3. Wählen Sie Aus Datei importieren aus. Wählen Sie die Konfigurationsdatei aus, die Sie von Ihrem Client VPN-Administrator erhalten haben.
4. Wählen Sie das Verbindungsprofil aus, um die Verbindung zu beginnen.

Verbinden Sie sich mit einer Android- oder iOS-VPN-Client-Anwendung

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 zu den OpenVPN-Clientanwendungen für Android finden Sie in den häufig gestellten Fragen in Bezug auf OpenVPN Connect Android 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.

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

Verbinden mit einer macOS-Client-Anwendung

Die folgenden Prozeduren zeigen, wie eine VPN-Verbindung unter Verwendung von macOS-basierten VPN-Clients hergestellt wird.

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.

Informationen zur Problembehebung finden Sie unter macOS-Fehlerbehebung.

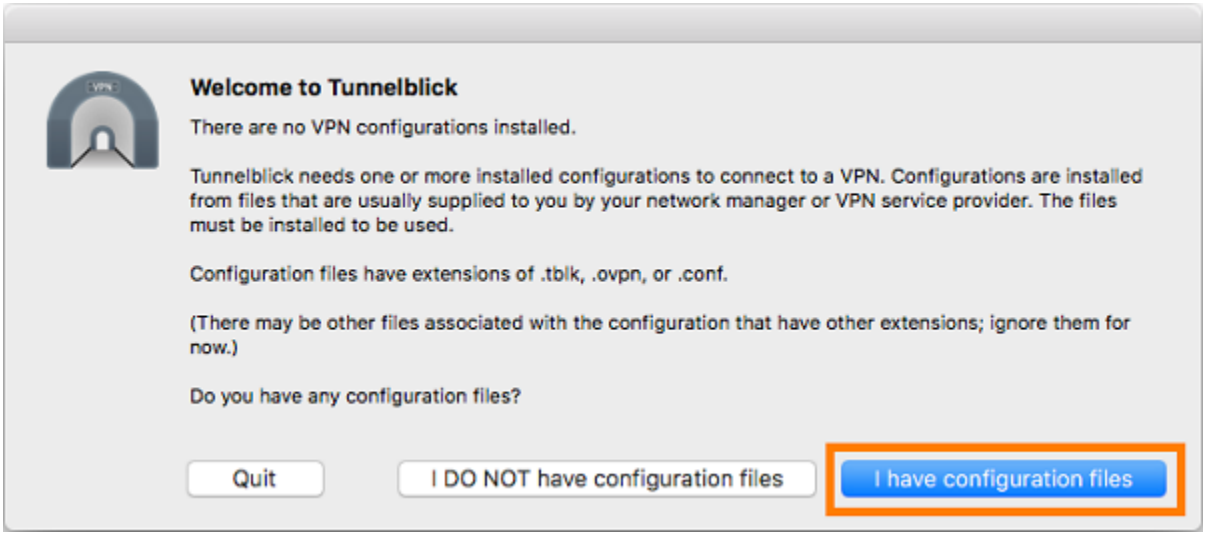
Tunnelblick

Das folgende Verfahren zeigt, wie Sie eine VPN-Verbindung mithilfe der Tunnelblick-Clientanwendung auf einem macOS-Computer herstellen.

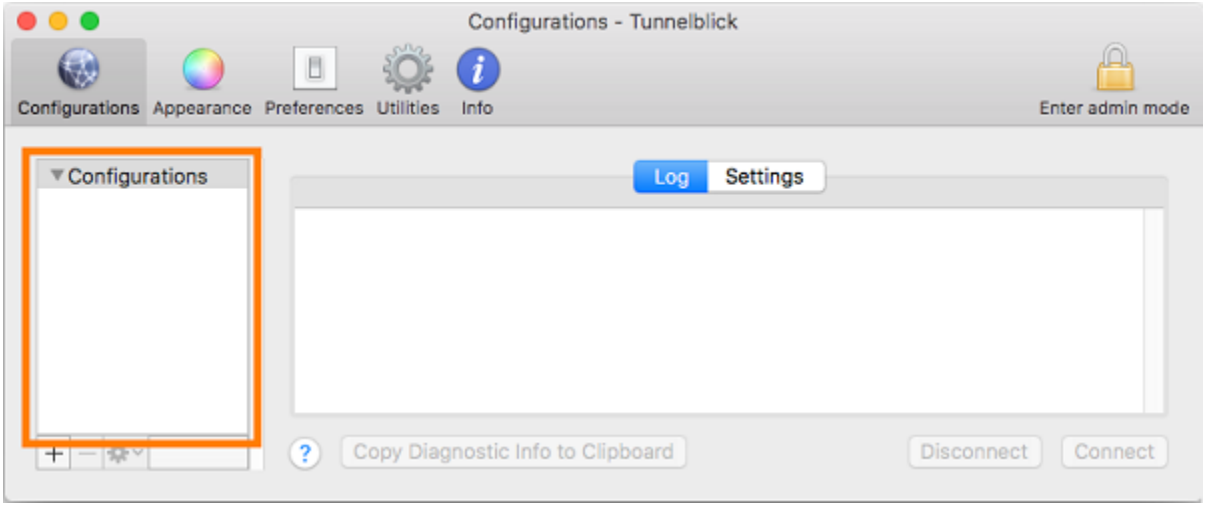
> **Note**
>
> Weitere Informationen über die Tunnelblick-Clientanwendung für macOS finden Sie in der Tunnelblick-Dokumentation auf der Tunnelblick-Website.

So stellen Sie eine VPN-Verbindung her

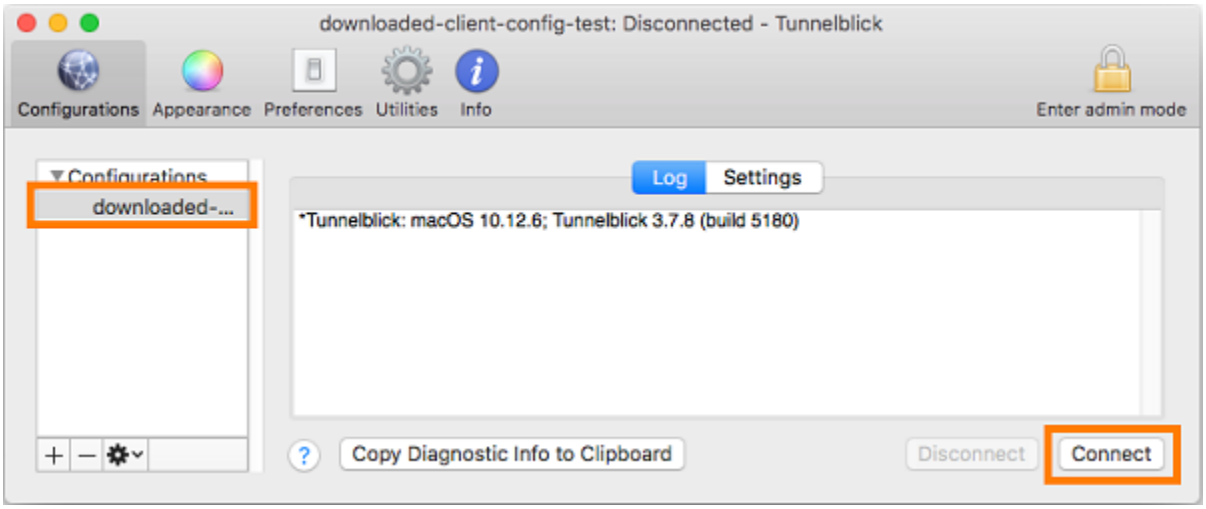
1. Starten Sie die Tunnelblick-Clientanwendung und wählen Sie I have configuration files aus.



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.



OpenVPN Connect-Client

Die folgende Prozedur zeigt, wie eine VPN-Verbindung mit der OpenVPN-Client-Anwendung auf einem MacOS-Computer hergestellt wird.

> **Note**
>
> Weitere Informationen finden Sie unter Verbindung zum Zugriffsserver mit macOS auf der OpenVPN-Website.

So stellen Sie eine VPN-Verbindung her

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.

Herstellen einer Verbindung mit einer OpenVPN-Client-Anwendung

Die folgenden Prozeduren zeigen, wie eine VPN-Verbindung unter Verwendung von OpenVPN-basierten VPN-Clients hergestellt wird.

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.

Informationen zur Problembehebung finden Sie unter Linux-Fehlerbehebung.

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

OpenVPN - Network Manager

Die folgende Prozedur zeigt, wie eine VPN-Verbindung mit der OpenVPN-Anwendung über die Network Manager-Benutzeroberfläche auf einem Ubuntu-Computer hergestellt wird.

So stellen Sie eine VPN-Verbindung her

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.

OpenVPN

Die folgende Prozedur zeigt, wie eine VPN-Verbindung mit der OpenVPN-Anwendung auf einem Ubuntu-Computer hergestellt wird.

So stellen Sie eine VPN-Verbindung her

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
```

Fehlerbehebung bei Ihrer Client VPN-Verbindung

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.

Sendet Diagnoseprotokolle AWS Support an den AWS bereitgestellten Client

Wenn Sie Probleme mit dem AWS bereitgestellten Client haben und Sie sich mit der Problembehebung in Verbindung setzen AWS Support müssen, hat der 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, stellen wir Ihnen eine Referenznummer zur Verfügung, die Sie angeben können, AWS Support damit sie sofort auf die Dateien zugreifen können.

Senden von Diagnoseprotokollen

Der AWS angegebene Client wird in den folgenden Schritten auch als AWS VPN Kunde bezeichnet.

Um Diagnoseprotokolle mit dem AWS bereitgestellten Client für Windows zu senden

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 AWS bereitgestellten Client für macOS zu senden

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 AWS bereitgestellten Client für Ubuntu zu senden

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 möchten.

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

Windows-Fehlerbehebung

Die folgenden Abschnitte enthalten Informationen zu Problemen, die bei der Verwendung von Windows-basierten Clients zur Herstellung einer Verbindung zu einem Client VPN-Endpunkt auftreten können.

Themen

AWS bereitgestellter Kunde

AWS bereitgestellter Kunde

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

- Client ist in einem Wiederverbindungszustand blockiert
- VPN-Verbindungsprozess wird unerwartet beendet
- Anwendung startet nicht
- Client kann kein Profil erstellen
- Client-Absturz tritt auf Dell PCs auf, die Windows 10 oder 11 verwenden
- VPN trennt die Verbindung mit einer Popup-Meldung

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 keine Verbindung mit der Protokollmeldung „Keine TAP-Windows-Adapter“ 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 einen TAP-Windows-Adapter erstellen können, indem Sie zu „Start -> Alle Programme -> TAP-Windows -> Dienstprogramme -> Neuen virtuellen TAP-Windows-Ethernet-Adapter hinzufügen“ navigieren.

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.

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:

- DBR .dll ShellExtension
- DBR.dll OverlayIconBackuped
- DBR.dll OverlayIconNotBackuped

Lösung

Um dieses Problem zu vermeiden, stellen Sie zunächst sicher, dass Ihr Client mit der neuesten Version des AWS bereitgestellten Clients auf dem neuesten Stand ist. 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.

   - DBR.dll ShellExtension
   - DBR.dll OverlayIconBackuped
   - DBR.dll OverlayIconNotBackuped

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

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

Der TAP-Windows-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
```

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).

macOS-Fehlerbehebung

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.

Themen

AWS bereitgestellter Client

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.

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

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

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

Themen

- Client kann keine Verbindung herstellen
- Client ist in einem Wiederverbindungszustand blockiert
- Client kann kein Profil erstellen

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.

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.

Verschlüsselungsalgorithmus "AES-256-GCM" 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 AES-256-GCM nicht unterstützt.

Lösung

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

1. Öffnen Sie die Tunnelblick-Anwendung.
2. Wählen Sie Settings (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.

Linux-Fehlerbehebung

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

Themen

- AWS bereitgestellter Client
- OpenVPN (Befehlszeile)
- OpenVPN über Network Manager (GUI)

AWS bereitgestellter Client

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/username/
```

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.

Allgemeine 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-Benutzerhandbuchs beschrieben.

Änderung	Beschreibung	Datum
AWS Von bereitgestellter Client (3.9.1) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS Von bereitgestellter Client (3.12.1) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS Von bereitgestellter Client (3.11.1) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	16. Februar 2024
AWS Von bereitgestellter Client (3.12.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	19. Dezember 2023
AWS Von bereitgestellter Client (3.9.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS Von bereitgestellter Client (3.11.0) für Windows veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS Von bereitgestellter Client (3.11.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023
AWS Von bereitgestellter Client (3.10.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	6. Dezember 2023

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

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

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

AWS Von bereitgestellter Client (2.0.0) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. Januar 2022
AWS Von bereitgestellter Client (1.4.0) für macOS veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	9. November 2021
AWS Von bereitgestellter Client für Windows (1.3.7) veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. November 2021
AWS Von bereitgestellter Client (1.0.3) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	8. November 2021
AWS Von bereitgestellter Client (1.0.2) für Ubuntu veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	28. September 2021
AWS Von bereitgestellter Client für Windows (1.3.6) und macOS (1.3.5) veröffentlicht	Weitere Informationen finden Sie unter Versionshinweise.	20. September 2021
AWS Von bereitgestellter Client für Ubuntu 18.04 LTS und Ubuntu 20.04 LTS veröffentlicht	Sie können den AWSvon 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 zu erhalten.	29. Oktober 2020
AWS Von bereitgestellter Client	Sie können den von 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.