Benutzerhandbuch

AWS Kunde VPN

AWS Kunde VPN: Benutzerhandbuch

Table of Contents

Was ist AWS KundeVPN?

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

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

VPNClient-Komponenten

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

- VPNClient-Endpunkt — Ihr VPN Client-Administrator erstellt und konfiguriert einen VPN Client-Endpunkt in AWS. Ihr Administrator kontrolliert, auf welche Netzwerke und Ressourcen Sie zugreifen können, wenn Sie eine VPN Verbindung herstellen.
- VPNClient-Anwendung — Die Softwareanwendung, mit der Sie eine Verbindung zum VPN Client-Endpunkt herstellen und eine sichere VPN Verbindung herstellen.
- Konfigurationsdatei für den VPN Client-Endpunkt — Eine Konfigurationsdatei, die Ihnen von Ihrem VPN Client-Administrator zur Verfügung gestellt wird. Die Datei enthält Informationen über den VPN Client-Endpunkt und die Zertifikate, die für den VPN Verbindungsaufbau erforderlich sind. Sie laden diese Datei in die von Ihnen gewählte VPN Client-Anwendung.

Zusätzliche Ressourcen für die Konfiguration des Clients VPN

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

Fangen Sie an mit AWS Client VPN

Bevor Sie eine VPN Sitzung einrichten können, muss Ihr VPN Client-Administrator einen VPN Client-Endpunkt erstellen und konfigurieren. Ihr Administrator steuert, auf welche Netzwerke und Ressourcen Sie zugreifen können, wenn Sie eine VPN Sitzung einrichten. Anschließend verwenden Sie eine VPN Client-Anwendung, um eine Verbindung zu einem VPN Client-Endpunkt herzustellen und eine sichere VPN Verbindung herzustellen.

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

Themen

Voraussetzungen für die Verwendung des Clients VPN

Um eine VPN Verbindung herzustellen, müssen Sie über Folgendes verfügen:

- Zugriff auf das Internet
- Ein unterstütztes Gerät
- Für VPN Client-Endgeräte, die die SAML basierte Verbundauthentifizierung (Single Sign-On) verwenden, einen der folgenden Browser:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Schritt 1: Besorgen Sie sich eine Client-Anwendung VPN

Sie können eine Verbindung zu einem VPN Client-Endpunkt herstellen und mithilfe des AWS bereitgestellten Clients oder einer anderen VPN Open-basierten Client-Anwendung eine VPN Verbindung herstellen.

Der AWS bereitgestellte Client wird unter Windows, macOS, Ubuntu 18.04 und Ubuntu 20.04 LTS unterstützt. LTS

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

- Wenn Ihr Administrator die Endpunktkonfigurationsdatei nicht eingerichtet hat, laden Sie den Client über den Client-Download herunter und installieren VPNSie ihn.AWS Nachdem Sie die Anwendung heruntergeladen und installiert haben, fahren Sie mit the section called “Schritt 2: Holen Sie sich die Konfigurationsdatei für den VPN Client-Endpunkt” dem Abrufen der Endpunktkonfigurationsdatei von Ihrem Administrator fort.
- Wenn Ihr Administrator die Endpunkt-Konfigurationsdatei bereits vorkonfiguriert hat, können Sie die VPN Client-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 “Laden Sie den Client herunter VPN” Nachdem Sie die Anwendung und Datei heruntergeladen und installiert haben, gehen Sie zuthe section called “Schritt 3: Stellen Sie eine Verbindung zum her VPN”.

Sie können auch eine Open VPN Client-Anwendung herunterladen und auf dem Gerät installieren, von dem aus Sie die VPN Verbindung herstellen möchten.

Schritt 2: Holen Sie sich die Konfigurationsdatei für den VPN Client-Endpunkt

Sie erhalten die Konfigurationsdatei für den VPN Client-Endpunkt von Ihrem Administrator. Die Konfigurationsdatei enthält die Informationen über den VPN Client-Endpunkt und die Zertifikate, die für den VPN Verbindungsaufbau erforderlich sind.

Wenn Ihr VPN Client-Administrator ein Self-Service-Portal für den VPN Client-Endpunkt konfiguriert hat, können Sie alternativ die neueste Version des AWS bereitgestellten Clients und die neueste

Version der VPN Client-Endpunkt-Konfigurationsdatei selbst herunterladen. Weitere Informationen finden Sie unter Laden Sie das AWS Client VPN vom Self-Service-Portal herunter.

Schritt 3: Stellen Sie eine Verbindung zum her VPN

Importieren Sie die Konfigurationsdatei für den VPN Client-Endpunkt in den AWS bereitgestellten Client oder in Ihre VPN Open-Client-Anwendung und stellen Sie eine Verbindung zum herVPN. Anweisungen zum Herstellen einer Verbindung zu einerVPN, einschließlich des Imports der Endpunkt-Konfigurationsdatei, finden Sie in den folgenden Themen:

- Stellen Sie mithilfe eines AWS bereitgestellten Clients eine Verbindung zu einem VPN Client-Endpunkt her
- Stellen Sie mit einem Open Client eine Connect zu einem VPN VPN Client-Endpunkt her

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

Bei VPN Client-Endpunkten, die eine SAML basierte Verbundauthentifizierung (Single Sign-On) verwenden, öffnet der AWS bereitgestellte Client ein Browserfenster auf Ihrem Computer. Sie werden aufgefordert, Ihre Unternehmensanmeldedaten einzugeben, bevor Sie eine Verbindung zum Client-Endpunkt herstellen können. VPN

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 neueste Version der VPN Client-Endpunkt-Konfigurationsdatei herunterladen können. Wenn Ihr VPN Client-Endpunktadministrator die Konfigurationsdatei für den VPN Client-Client vorkonfiguriert hat, können Sie diese VPN Client-Anwendung zusammen mit der Konfigurationsdatei von diesem Portal herunterladen und installieren.

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

Bevor Sie beginnen, benötigen Sie die ID des VPN Client-Endpunkts. Ihr VPN Client-Endpunktadministrator kann Ihnen die ID zur Verfügung stellen oder Ihnen ein Self-Service-Portal zur Verfügung stellenURL, das 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 das, URL das Ihnen von Ihrem Administrator zur Verfügung gestellt wurde.
2. Geben Sie bei Bedarf die ID des VPN Client-Endpunkts ein, `cvpn-endpoint-0123456abcd123456` z. B. Wählen Sie Weiter.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und wählen Sie Sign In (Anmelden). Dies ist derselbe Benutzername und das gleiche Passwort, die Sie für die Verbindung zum VPN Client-Endpunkt verwenden.
4. Im Self-Service-Portal haben Sie folgende Möglichkeiten:
   - Laden Sie die neueste Version der Client-Konfigurationsdatei für den VPN Client-Endpunkt herunter.
   - Laden Sie die neueste Version des AWS bereitgestellten Clients für Ihre Plattform herunter.

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

Sie können mit dem AWS bereitgestellten Client eine Verbindung zu einem VPN Client-Endpunkt herstellen. Der AWS bereitgestellte Client wird unter Windows, macOS, Ubuntu 18.04 und Ubuntu 20.04 LTS unterstützt. LTS

Clients

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

Direktiven öffnen VPN

Der AWS bereitgestellte Client unterstützt die folgenden VPN Open-Direktiven:

- 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

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

Voraussetzungen

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

- Windows 10 oder Windows 11 (64-Bit-Betriebssystem, x64-Prozessor)
- . NETFramework 4.7.2 oder höher

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

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

Themen

Stellen Sie VPN mit einem AWS bereitgestellten Client für Windows eine Connect zum Client her

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 AWS bereitgestellten Client für Windows herzustellen

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 VPNunter Konfigurationsdatei nach der Konfigurationsdatei, die Sie von Ihrem VPN Client-Administrator erhalten haben, wählen Sie sie aus und wählen Sie 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 VPN Client-Endpunkt für die Authentifizierung auf der Grundlage von Anmeldeinformationen 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.

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.

> **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 durch Benutzerfreundlichkeits- und/oder Sicherheitsprobleme beeinträchtigt werden. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Datum	Link herunterladen und SHA256
3.14.0	• Unterstützung für das `tap-sleep` VPN Open-Flag wurde hinzugefügt. • Die SSL Bibliotheken „Öffnen“ VPN und „Öffnen“ wurden aktualisiert.	12. August 2024	Version 3.14.0 herunterladen sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516
3,13,0	Die Bibliotheken Open VPN und Open SSL wurden aktualisiert.	29. Juli 2024	Version 3.13.0 herunterladen

Version	Änderungen	Datum	Link herunterladen und SHA256
			sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12,1	Es wurde ein Problem behoben, das verhindert, dass die Windows-Client-Ver sion 3.12.0 für einige Benutzer VPN eine Verbindung herstellen konnte.	18. Juli 2024	Version 3.12.1 herunterladen 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	Datum	Link herunterladen und SHA256
3.11.2	Ein SAML Authentifizierungsproblem mit Chromium-basierten Browsern seit Version 123 wurde behoben.	11. April 2024	Version 3.11.2 herunterladen 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 • Verbindungsprobleme für einige LAN Konfigurationen wurden behoben. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.11.0 herunterladen sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version	Änderungen	Datum	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	Datum	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 Open-Flag „verify-x509-name“ hinzugefügt. VPN • 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
3.1.0	Verbesserter Sicherheitsstatus.	23. Mai 2022	Nicht mehr unterstützt
3.0.0	• Zusätzlicher Windows 11 Support. • Die Benennung von TAP Windows-Treibern wurde behoben, wodurch andere Treibernamen betroffen waren. • 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 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 Open VPN 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 Open flag: dhcp-option hinzugefügt. VPN • Kleinere Fehlerbehebungen und Verbesserungen.	4. August 2021	Nicht mehr unterstützt

Version	Änderungen	Datum	Link herunterladen und SHA256
1.3.3	• Unterstützung für VPN Open-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 IPv6 Leckschutz hinzu, wenn er 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. • Unterstützung für die Open-Direktive „route-ipv6“ hinzugefügt. VPN • Kleinere Fehlerbehebungen und Verbesserungen.	05. April 2021	Nicht mehr unterstützt

Version	Änderungen	Datum	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 Cryptoapicert Open-Direktive hinzugefügt. VPN • 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 Open-Konfiguration hinzugefügt. VPN • Es wurde eine 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 SAML2.0-basierte Verbundauthentifizierung hinzugefügt. • Unterstützung für die Windows 7-Plattfo rm eingestellt.	19. Mai 2020	Nicht mehr unterstützt
1.1.1	Kleinere Fehlerbehebungen und Verbesserungen.	21. April 2020	Nicht mehr unterstützt

Version	Änderungen	Datum	Link herunterladen und SHA256
1.1.0	• Es wurde Unterstützung für die Funktion Open VPN static challenge echo hinzugefügt, mit der der auf der Benutzeroberfläche angezeigte Text ein- oder ausgeblendet werden kann. • 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 VPNClient-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 Monterey (12.0), Ventura (13.0) oder Sonoma (14.0).
- Mit x86_64-Prozessor kompatibel.
- Der Client reserviert TCP Port 8096 auf Ihrem Computer.
- Für VPN Client-Endpunkte, die die SAML basierte Verbundauthentifizierung (Single Sign-On) verwenden, reserviert der Client Port 35001. TCP

> **Note**
>
> Wenn Sie einen Mac mit einem Apple-Silicon-Prozessor verwenden, müssen Sie Rosetta 2 installieren, um die Client-Software auszuführen. Weitere Informationen finden Sie auf der Apple-Website unter Über die Rosetta Translation Environment.

Themen

Stellen Sie VPN mit einem AWS bereitgestellten Client für macOS eine Connect zum Client her

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

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 AWS bereitgestellten Client für macOS herzustellen

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 Konfigurationsdatei nach der Konfigurationsdatei, die Sie von Ihrem VPN Client-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 VPN Client-Endpunkt für die Authentifizierung auf der Grundlage von Anmeldeinformationen 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 wählen Sie dann Disconnect < > your-profile-name.

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 durch Benutzerfreundlichkeits- und/oder Sicherheitsprobleme beeinträchtigt werden. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Datum	Download-Link
3.12.0	• Unterstützung für das `tap-sleep` VPN Open-Flag wurde hinzugefügt. • Die SSL Bibliotheken „Öffnen“ VPN und „Öffnen“ wurden aktualisiert.	12. August 2024	Version 3.12.0 herunterladen sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13
3.11.0	• Die Bibliotheken „Öffnen“ und „Öffnen“ wurden aktualisiert. VPN SSL	29. Juli 2024	Version 3.11.0 herunterladen sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062

Version	Änderungen	Datum	Download-Link
			21b8caea8 1732848f
3.10.0	• Stellt die Verbindung automatisch wieder her, wenn sich die Bereiche des lokalen Netzwerks ändern. • Ein DNS Wiederherstellungsproblem beim Netzwerkwechsel wurde behoben. • Der automatische Anwendungsfokus bei einer Verbindung mit SAML Endpunkten wurde entfernt.	21. Mai 2024	Version 3.10.0 herunterladen sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3,9.2	• Ein SAML Authentifizierungsproblem mit Chromium-basierten Browsern seit Version 123 wurde behoben. • Unterstützung für macOS Sonoma hinzugefügt. Unterstützung für macOS Big Sur wurde eingestellt. • Verbesserter Sicherheitsstatus.	11. April 2024	Version 3.9.2 herunterladen sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480

Version	Änderungen	Datum	Download-Link
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 2024	Version 3.9.1 herunterladen sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e899e971
3.9.0	• Verbindungsprobleme für einige Konfigurationen wurden behoben. LAN • 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, wenn NAT64 es im Client-Ne tzwerk 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 Open-Flag „verify-x509-name“ hinzugefügt. VPN • 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	• Serverüberwachung während der Verbindung hinzugefügt. DNS Die Einstellungen werden neu konfiguriert, wenn sie nicht mit den VPN Einstellungen übereinstimmen. • 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 Open VPN flags: connect-retry-max, dev-type, keepalive , ping, ping-restart, pull, rcvbuf, hinzugefügt. server-poll-timeout • Kleinere Fehlerbehebungen und Verbesserungen.	20. September 2021	Nicht mehr unterstützt.
1.3.4	• Unterstützung für Open flag: dhcp-opti on hinzugefügt. VPN • Kleinere Fehlerbehebungen und Verbesserungen.	4. August 2021	Nicht mehr unterstützt.
1.3.3	• Unterstützung für VPN Open-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 den IPv6 Leckschutz hinzu, wenn er 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. • Das Problem, dass DNS Einstellu ngen entfernt wurden, die von anderen Anwendungen konfiguriert wurden, wurde behoben. • Behobenes Problem, bei dem die Verwendung eines ungültigen Zertifika ts für die gegenseitige Authentif izierung, das Verbindungsprobleme verursachte. • Unterstützung für die Open-Direktive „route-ipv6“ hinzugefügt. VPN • Kleinere Fehlerbehebungen und Verbesserungen.	05. April 2021	Nicht mehr unterstützt.
1.3.0	Zusätzliche Supportfunktionen wie Fehlerberichte, Senden von Diagnosep rotokollen 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 Open-Konfiguration hinzugefügt. VPN • Es wurde eine 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 SAML2.0-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	• Es wurde ein Problem behoben, bei dem DNS es nicht behoben wurde. • Absturzproblem bei Apps durch längere Verbindungen behoben. • Ein MFA Problem wurde behoben.	2. April 2020	Nicht mehr unterstützt.

Version	Änderungen	Datum	Download-Link
1.1.0	• Unterstützung für die DNS macOS-Konfiguration hinzugefügt. • Es wurde Unterstützung für die Funktion Open VPN static challenge echo hinzugefügt, mit der der auf der Benutzeroberfläche angezeigte Text ein- oder ausgeblendet werden kann. • 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 das anschließende Herstellen 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”.

Anforderungen für die Verbindung zum Client VPN mit einem AWS bereitgestellten Client für Linux

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

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

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

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

Themen

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

Installieren Sie den AWS bereitgestellten Client für Linux

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 AWS VPN Client-Schlüssel 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 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 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 vom AWS VPNClient-Download herunter oder verwenden Sie den folgenden Befehl.

```
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 vom AWS VPNClient-Download 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 AWS bereitgestellten Client für Linux her

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

Um eine Verbindung mit dem AWS bereitgestellten Client für Linux herzustellen

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 Konfigurationsdatei nach der Konfigurationsdatei, die Sie von Ihrem VPN Client-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 VPN Client-Endpunkt für die Authentifizierung auf der Grundlage von Anmeldeinformationen 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.

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 durch Benutzerfreundlichkeits- und/oder Sicherheitsprobleme beeinträchtigt werden. Weitere Informationen finden Sie unter Versionshinweise.

Version	Änderungen	Datum	Download-Link
3.15.0	• Unterstützung für das `tap-sleep` VPN Open-Flag wurde hinzugefügt. • Die SSL Bibliotheken „Öffnen“ VPN und „Öffnen“ wurden aktualisiert.	12. August 2024	Version 3.15.0 herunterladen sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6d89d012
3,14.0	• Die Bibliotheken Open VPN und Open SSL wurden aktualisiert.	29. Juli 2024	Version 3.14.0 herunterladen

Version	Änderungen	Datum	Download-Link
			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
3.12,2	• Ein SAML Authentifizierungsproblem mit Chromium-basierten Browsern seit Version 123 wurde behoben.	11. April 2024	Version 3.12.2 herunterladen sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d

Version	Änderungen	Datum	Download-Link
3,12,1	• 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 3.12.1 herunterladen sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0
3.12.0	• Verbindungsprobleme für einige Konfigurationen wurden behoben. LAN	19. Dezember 2023	Version 3.12.0 herunterladen sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Rollback für „Verbindungsprobleme für einige LAN Konfigurationen behoben“. • Verbesserte Barrierefreiheit.	6. Dezember 2023	Version 3.11.0 herunterladen sha256:86 c0fa1bf1c 971940828 35a739ec7 f1c87e540 194955f41 4a35c679b 94538970

Version	Änderungen	Datum	Download-Link
3.10.0	• Verbindungsprobleme für einige LAN Konfigurationen wurden 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, wenn NAT64 es im Client-Ne tzwerk aktiviert war. • Kleinere Fehlerbehebungen und Verbesserungen.	24. August 2023	Version 3.9.0 herunterladen sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454
3.8.0	• Verbesserter Sicherheitsstatus.	3. August 2023	Version 3.8.0 herunterladen sha256: 5fe479236 cc0a1940b a37fe168e 551096f8d ae4c68d45 560a164e4 1edea3e5bd
3.7.0	• Verbesserter Sicherheitsstatus.	15. Juli 2023	Nicht mehr unterstützt

Version	Änderungen	Datum	Download-Link
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 Open-Flag „verify-x509-name“ hinzugefügt. VPN	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.
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.

Version	Änderungen	Datum	Download-Link
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 VPN Open-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 VPN Open-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.

Stellen Sie mit einem Open Client eine Connect zu einem VPN VPN Client-Endpunkt her

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

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

Clientanwendungen

- Stellen Sie mithilfe einer Windows-Client-Anwendung eine Connect zu einem VPN Client-Endpunkt her
- Stellen Sie mithilfe einer Android- oder iOS-Client-Anwendung eine Connect zu einem VPN VPN Client-Endpunkt her
- Stellen Sie mithilfe einer macOS-Client-Anwendung eine Connect zu einem VPN Client-Endpunkt her
- Stellen Sie mithilfe einer Open Client-Anwendung eine Connect zu einem VPN VPN Client-Endpunkt her

Stellen Sie mithilfe einer Windows-Client-Anwendung eine Connect zu einem VPN Client-Endpunkt her

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

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

Informationen zur Problembehebung finden Sie unter Problembehandlung bei VPN Client-Verbindungen mit Windows-basierten Clients.

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

Aufgaben

- Verwenden Sie mit Open ein Zertifikat aus dem Windows Certificate System Store VPN
- Verwenden Sie die Option Öffnen VPN GUI
- Verwenden Sie den Open VPN Connect Client

Verwenden Sie mit Open ein Zertifikat aus dem Windows Certificate System Store VPN

Sie können den VPN Open-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 VPN Client-Verbindung verwenden. Informationen zur Cryptoapicert-Option Open VPN client finden Sie im Referenzhandbuch für Open VPN auf der Open-Website. VPN

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

So verwenden Sie die Cryptoapicert-Option mit Open VPN

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 Vorgehensweise: 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 VPN Open-Konfigurationsdatei und geben Sie das Zertifikat an, indem Sie entweder den Zertifikatsantrag oder den Fingerabdruck des Zertifikats angeben.

   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 Open, VPN um eine Verbindung herzustellen.

Verwenden Sie die Option Öffnen VPN GUI

Das folgende Verfahren zeigt, wie Sie mit der Open VPN GUI Client-Anwendung auf einem Windows-Computer eine VPN Verbindung herstellen.

> **Note**
>
> Informationen zur Open VPN Client-Anwendung finden Sie unter Community-Downloads auf der VPN Open-Website.

Um eine VPN Verbindung herzustellen

1. Starten Sie die Open VPN Client-Anwendung.
2. Wählen Sie in der Windows-Taskleiste die Option „Symbole ein-/ausblenden“. Klicken Sie mit der rechten Maustaste auf Öffnen VPN GUI und wählen Sie dann Datei importieren.
3. Wählen Sie im Dialogfeld Öffnen die Konfigurationsdatei aus, die Sie von Ihrem VPN Client-Administrator erhalten haben, und klicken Sie auf Öffnen.
4. Wählen Sie in der Windows-Taskleiste die Option „Symbole ein-/ausblenden“. Klicken Sie mit der rechten Maustaste auf Öffnen VPN GUI und wählen Sie dann Connect.

Verwenden Sie den Open VPN Connect Client

Das folgende Verfahren zeigt, wie Sie mit der Open VPN Connect Client-Anwendung auf einem Windows-Computer eine VPN Verbindung herstellen.

> **Note**
>
> Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Access Server mit Windows auf der VPN Open-Website.

So stellen Sie eine VPN Verbindung her

1. Starten Sie die Open VPN Connect Client-Anwendung.
2. Wählen Sie in der Windows-Taskleiste die Option „Symbole ein-/ausblenden“. Klicken Sie mit der rechten Maustaste auf Öffnen VPN und wählen Sie dann Profil importieren.
3. Wählen Sie Aus Datei importieren und wählen Sie die Konfigurationsdatei aus, die Sie von Ihrem VPN Client-Administrator erhalten haben.
4. Wählen Sie das Verbindungsprofil aus, um die Verbindung zu beginnen.

Stellen Sie mithilfe einer Android- oder iOS-Client-Anwendung eine Connect zu einem VPN VPN Client-Endpunkt her

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

Die folgenden Informationen zeigen, wie Sie mit der Open VPN Client-Anwendung auf einem Android- oder iOS-Mobilgerät eine VPN Verbindung herstellen. Die Schritte für Android und iOS sind identisch.

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

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

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

Stellen Sie mithilfe einer macOS-Client-Anwendung eine Connect zu einem VPN Client-Endpunkt her

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

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

Informationen zur Problembehebung finden Sie unter Problembehandlung bei VPN Client-Verbindungen mit macOS-Clients.

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

Themen

Starten Sie Tunnelblick, um eine Verbindung herzustellen AWS Client VPN

Das folgende Verfahren zeigt, wie Sie mit der Tunnelblick-Clientanwendung 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.

Um eine Verbindung herzustellen VPN

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, per Drag-and-Drop in das Konfigurationsfenster.
3. Wählen Sie die Konfigurationsdatei im Bereich Configurations und die Option Connect aus.

Stellen Sie mit dem Open VPN Connect Client eine Verbindung zu einem AWS Client VPN Endpunkt her

Das folgende Verfahren zeigt, wie Sie mit der Open VPN Connect Client-Anwendung auf einem macOS-Computer eine VPN Verbindung herstellen.

> **Note**
>
> Weitere Informationen finden Sie unter Herstellen einer Verbindung zum Access Server mit macOS auf der VPN Open-Website.

So stellen Sie eine VPN Verbindung her

1. Starten Sie die VPN Anwendung „Öffnen“ und wählen Sie „Importieren“, „Aus lokaler Datei...“ .
2. Navigieren Sie zu der Konfigurationsdatei, die Sie von Ihrem VPN Administrator erhalten haben, und wählen Sie Öffnen.

Stellen Sie mithilfe einer Open Client-Anwendung eine Connect zu einem VPN VPN Client-Endpunkt her

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

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

Informationen zur Problembehebung finden Sie unter Problembehandlung bei VPN Client-Verbindungen mit Linux-basierten Clients.

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

Themen

- Stellen Sie eine Verbindung zur AWS Client VPN Verwendung von Open VPN — Network Manager her
- Stellen Sie eine Verbindung zur AWS Client VPN Verwendung von Open her VPN

Stellen Sie eine Verbindung zur AWS Client VPN Verwendung von Open VPN — Network Manager her

Das folgende Verfahren zeigt, wie Sie mithilfe der VPN Open-Anwendung über den Network Manager GUI auf einem Ubuntu-Computer eine VPN Verbindung herstellen.

Um eine VPN Verbindung herzustellen

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 Pluszeichen (+) neben VPNund wählen Sie dann Aus Datei importieren... .
4. Navigieren Sie zu der Konfigurationsdatei, die Sie von Ihrem VPN Administrator erhalten haben, und wählen Sie Öffnen.
5. Wählen Sie im VPN Fenster Hinzufügen die Option Hinzufügen aus.
6. Starten Sie die Verbindung, indem Sie den Schalter neben dem VPN Profil aktivieren, das Sie hinzugefügt haben.

Stellen Sie eine Verbindung zur AWS Client VPN Verwendung von Open her VPN

Das folgende Verfahren zeigt, wie Sie mit der VPN Open-Anwendung auf einem Ubuntu-Computer eine VPN Verbindung herstellen.

Um eine VPN Verbindung herzustellen

1. Installieren Sie Open VPN 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
```

Problembehandlung bei Ihrer VPN Client-Verbindung

Verwenden Sie die folgenden Themen, um Probleme zu beheben, die auftreten können, wenn Sie eine Client-Anwendung verwenden, um eine Verbindung zu einem VPN Client-Endpunkt herzustellen.

Themen

Fehlerbehebung bei VPN Client-Endpunkten für Administratoren

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

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

Senden Sie Diagnoseprotokolle AWS Support an den AWS bereitgestellten Client

Wenn Sie Probleme mit dem AWS bereitgestellten Client haben und sich an ihn wenden müssen, AWS Support um Hilfe bei der Fehlerbehebung zu erhalten, 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, 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 Kontakt aufnehmen AWS Support, müssen Sie ihnen die Referenznummer mitteilen.

Problembehandlung bei VPN Client-Verbindungen mit Windows-basierten Clients

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

Themen

AWS bereitgestellter Client

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.
- Offene VPN Protokolle: Enthalten Informationen über offene VPN 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
- VPNDer Verbindungsvorgang wird unerwartet beendet
- Anwendung startet nicht
- Client kann kein Profil erstellen
- Auf Dell, die Windows 10 oder 11 PCs verwenden, tritt ein Client-Absturz auf
- VPNDie Verbindung wird mit einer Popup-Meldung getrennt

Client kann keine Verbindung herstellen

Problem

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

Ursache

Dieses Problem kann folgende Ursachen haben:

- Auf Ihrem Computer läuft bereits ein anderer VPN Open-Prozess, der verhindert, dass der Client eine Verbindung herstellen kann.
- Ihre Konfigurationsdatei (OVPN) ist ungültig.

Lösung

Prüfen Sie, ob auf Ihrem Computer noch andere VPN Open-Anwendungen ausgeführt werden. Falls ja, beenden Sie diese Prozesse oder beenden Sie sie und versuchen Sie erneut, eine Verbindung zum VPN Client-Endpunkt herzustellen. Überprüfen Sie die geöffneten VPN Protokolle auf Fehler und bitten Sie Ihren VPN Client-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 das immer noch gültig CRL ist. Weitere Informationen finden Sie im AWS Client VPN Administratorhandbuch unter Clients, die keine Connect zu einem VPN Client-Endpunkt herstellen können.

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

Problem

Der AWS angegebene Client kann keine Verbindung zum VPN Client-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 virtuellen TAP Windows-Ethernet-Adapter hinzufügen gehen.

Lösung

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

- Starten Sie den -Windows-Adapter neu. TAP
- 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 VPN Client-Endpunkt herzustellen, steckt aber in einem Zustand fest, in dem die Verbindung wiederhergestellt 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 offener VPN Prozess versucht auf unbestimmte Zeit, eine Verbindung zum Endpunkt herzustellen.

Lösung

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

VPNDer Verbindungsvorgang wird unerwartet beendet

Problem

Beim Herstellen einer Verbindung zu einem VPN Client-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

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

Lösung

Führen Sie das AWS mitgelieferte 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 VPN Client-Endpunkt die gegenseitige Authentifizierung verwendet, enthält die Konfigurationsdatei (.ovpn) weder das Client-Zertifikat noch den Schlüssel.

Lösung

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

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

Problem

Bei bestimmten Dell PCs (Desktop und Laptop), auf denen Windows 10 oder 11 ausgeführt wird, kann es zu einem Absturz kommen, 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 dreiDLLs:

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll

- DBROverlayIconNotBackuped.dll

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. Gehen Sie zum AWS VPNClient-Download und wenn eine neuere Version verfügbar ist, führen Sie ein Upgrade auf die neueste Version durch.

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 die DLL Dateien alternativ löschen oder umbenennen. Beachten Sie jedoch, dass dies verhindert, dass die Dell Backup- and Recovery-Anwendung vollständig funktioniert.

Löschen Sie die DLL Dateien oder benennen Sie sie um

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.

VPNDie Verbindung wird mit einer Popup-Meldung getrennt

Problem

Die VPN Verbindung wird mit einer Popup-Meldung getrennt, 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-Der 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
```

Öffnen VPN GUI

Die folgenden Informationen zur Fehlerbehebung wurden mit den Versionen 11.10.0.0 und 11.11.0.0 der VPN GUI Open-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
```

Öffnen Sie den Connect-Client VPN

Die folgenden Informationen zur Fehlerbehebung wurden mit den Versionen 2.6.0.100 und 2.7.1.101 der Open VPN 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
```

Das Problem konnte nicht behoben werden DNS

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 Zwischenspeichern zu verhindern. Einige Clients tun dies jedoch nicht.

Lösung

Informationen zur Lösung für Unable to Resolve Client VPN Endpoint DNS Name finden Sie im AWS Client VPN Administratorhandbuch.

PKIAlias fehlt

Problem

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

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

Ursache

Bei der Open VPN Connect Client-Software gibt es ein bekanntes Problem, bei dem versucht wird, sich mit gegenseitiger Authentifizierung zu authentifizieren. Wenn die Konfigurationsdatei keinen Client-Schlüssel und kein Zertifikat enthält, schlägt die Authentifizierung fehl.

Lösung

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

Problembehandlung bei VPN Client-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.

Themen

- AWS bereitgestellter Client
- Tunnelblick
- Öffnen VPN

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.
- Offene VPN Protokolle: Enthalten Informationen über offene VPN 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

Problem

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

Ursache

Dieses Problem kann folgende Ursachen haben:

- Auf Ihrem Computer läuft bereits ein anderer VPN Open-Prozess, der verhindert, dass der Client eine Verbindung herstellen kann.

- Ihre Konfigurationsdatei (OVPN) ist ungültig.

Lösung

Prüfen Sie, ob auf Ihrem Computer noch andere VPN Open-Anwendungen ausgeführt werden. Falls ja, beenden Sie diese Prozesse oder beenden Sie sie und versuchen Sie erneut, eine Verbindung zum VPN Client-Endpunkt herzustellen. Überprüfen Sie die geöffneten VPN Protokolle auf Fehler und bitten Sie Ihren VPN Client-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 das immer noch gültig CRL ist. Weitere Informationen finden Sie im AWS Client VPN Administratorhandbuch unter Clients, die keine Connect zu einem VPN Client-Endpunkt herstellen können.

Client ist in einem Wiederverbindungszustand blockiert

Problem

Der AWS angegebene Client versucht, eine Verbindung zum VPN Client-Endpunkt herzustellen, steckt aber in einem Zustand fest, in dem die Verbindung wiederhergestellt 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 offener VPN Prozess versucht auf unbestimmte Zeit, eine Verbindung zum Endpunkt herzustellen.

Lösung

Überprüfen Sie, ob Ihr Computer mit dem Internet verbunden ist. Bitten Sie Ihren VPN Client-Administrator, zu überprüfen, ob die `remote` Anweisung in der Konfigurationsdatei zu einer gültigen IP-Adresse aufgelöst wird. Sie können die VPN Sitzung auch trennen, indem Sie im AWS VPN Client-Fenster auf Trennen klicken und erneut versuchen, die 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 VPN Client-Endpunkt die gegenseitige Authentifizierung verwendet, enthält die Konfigurationsdatei (.ovpn) weder das Client-Zertifikat noch den Schlüssel.

Lösung

Stellen Sie sicher, dass Ihr VPN Client-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

Beim Versuch, eine Verbindung herzustellen, wird die folgende Fehlermeldung angezeigtVPN.

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

Lösung

Lesen Sie den folgenden Artikel auf AWS re:POST. AWSVPNFehler „Client — Helper-Tool 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 die Log-Ausführlichkeit zu erhöhen, öffnen Sie die Tunnelblick-Anwendung, wählen Sie Einstellungen und passen Sie den Wert für die Protokollebene an. VPN

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

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 VPN Open-Version, die den Verschlüsselungsalgorithmus -256- nicht unterstützt. AES GCM

Lösung

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

1. Öffnen Sie die Tunnelblick-Anwendung.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie für VPNVersion öffnen die Option 2.4.6 — Die offene SSL Version ist v1.0.2q.

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 von Ihrem Client-Administrator eine neue Konfigurationsdatei an. VPN

Erweiterte Schlüsselnutzung (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, da 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. Erkundigen Sie sich gegebenenfalls bei Ihrem VPN Client-Administrator. Dieser Fehler kann auftreten, wenn Sie das Serverzertifikat und nicht das Client-Zertifikat verwenden, um eine Verbindung zum VPN Client-Endpunkt herzustellen.

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

Öffnen VPN

Die folgenden Informationen zur Fehlerbehebung wurden mit Version 2.7.1.100 der Open VPN Connect Client-Software auf 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
```

Kann nicht gelöst werden DNS

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

Open VPN Connect kann den VPN DNS Clientnamen nicht auflösen.

Lösung

Informationen zur Lösung für den VPNDNSClient-Endpunktnamen konnte nicht aufgelöst werden finden Sie im AWS Client VPN Administratorhandbuch.

Problembehandlung bei VPN Client-Verbindungen mit Linux-basierten Clients

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
- Öffnen VPN (Befehlszeile)
- VPNÜber den Netzwerkmanager öffnen () GUI

AWS bereitgestellter Client

Der AWS bereitgestellte Client speichert Protokolldateien und Konfigurationsdateien am folgenden Ort 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 werden DNS Abfragen nach dem Herstellen einer VPN Verbindung immer noch an den Standardsystem-Nameserver weitergeleitet, anstatt an die Nameserver, die für den Client-Endpunkt konfiguriert sind. VPN

Ursache

Der Client interagiert mit systemd-resolved, einem auf Linux-Systemen verfügbaren Dienst, der als zentrale Verwaltungseinheit dient. DNS Er wird verwendet, um DNS Server zu konfigurieren, die vom Client-Endpunkt aus per Push übertragen werden. VPN Das Problem tritt auf, weil systemd-resolved DNS Servern, die vom VPN Client-Endpunkt bereitgestellt werden, nicht die höchste Priorität einräumt. Stattdessen fügt es die Server an die bestehende Liste der DNS Server an, die auf dem lokalen System konfiguriert sind. Daher haben die ursprünglichen DNS Server möglicherweise immer noch die höchste Priorität und werden daher zur Lösung von DNS Abfragen verwendet.

Lösung

1. Fügen Sie die folgende Direktive in der ersten Zeile der VPN Open-Konfigurationsdatei hinzu, um sicherzustellen, dass alle DNS Anfragen 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 in DNS Proxy-Abfragen aufgelöst wird, sondern die Abfragen stattdessen direkt an die echten DNS Nameserver gesendet werden sollen, verwenden Sie stattdessen einen Symlink zu. `/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

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

   Möglicherweise möchten Sie dieses Verfahren durchführen, um die von Systemd aufgelöste Konfiguration zu umgehen, zum Beispiel für das Zwischenspeichern von DNS Antworten, die Konfiguration pro DNS Schnittstelle, die Durchsetzung usw. DNSSec Diese Option ist besonders nützlich, wenn Sie einen öffentlichen DNS Datensatz durch einen privaten Datensatz überschreiben müssen, wenn Sie mit diesem verbunden sind. VPN Sie könnten zum Beispiel einen privaten DNS Resolver VPC mit einem Eintrag für www.example.com haben, 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.

Öffnen VPN (Befehlszeile)

Problem

Die Verbindung funktioniert nicht richtig, da die DNS Auflösung nicht funktioniert.

Ursache

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

Lösung

Verwenden Sie die folgenden Schritte, um zu überprüfen, ob der DNS Server konfiguriert ist und ordnungsgemäß funktioniert.

1. Stellen Sie sicher, dass ein DNS Servereintrag in den Protokollen vorhanden ist. Im folgenden Beispiel wird der DNS Server `192.168.0.2` (konfiguriert im VPN Client-Endpunkt) in der letzten Zeile 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 VPN Client-Administrator, den VPN Client-Endpunkt zu ändern und sicherzustellen, dass ein DNS Server (z. B. der VPC DNS Server) für den VPN Client-Endpunkt angegeben wurde. Weitere Informationen finden Sie im AWS Client VPN Administratorhandbuch unter VPNClient-Endpunkte.

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 VPN Client-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
```

VPNÜber den Netzwerkmanager öffnen () GUI

Problem

Bei Verwendung des Network Manager VPN Open-Clients schlägt die Verbindung mit dem folgenden 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

Informationen zur Lösung für Unable to Resolve Client VPN Endpoint DNS Name finden Sie im AWS Client VPN Administratorhandbuch.

Behebung häufig auftretender VPN Client-Probleme

Im Folgenden sind häufig auftretende Probleme aufgeführt, die auftreten können, wenn Sie einen Client verwenden, um eine Verbindung zu einem VPN Client-Endpunkt herzustellen.

TLSDie Schlüsselaushandlung ist fehlgeschlagen

Problem

Die TLS Verhandlung schlägt mit dem folgenden 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 TCP den Datenverkehr.
- Sie verwenden den falschen Client-Schlüssel und das falsche Zertifikat in Ihrer Konfigurationsdatei (OVPN).
- Die Sperrliste für Client-Zertifikate (CRL) ist abgelaufen.

Lösung

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

- Dass die Firewallregeln für den VPN Client-Endpunkt den UDP Verkehr auf den Ports 443 oder 1194 nicht blockierenTCP.
- 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 das immer noch gültig CRL ist. Weitere Informationen finden Sie im AWS Client VPN Administratorhandbuch unter Clients, die keine Connect zu einem VPN Client-Endpunkt herstellen können.

Dokumentverlauf

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

Änderung	Beschreibung	Datum
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 und Ubuntu 20.04 veröffentlicht LTS LTS	Sie können den AWS bereitgestellten Client auf Ubuntu 18.04 und Ubuntu 20.04 verwenden. LTS LTS	11. Juni 2021

Support für Open VPN mit einem Zertifikat aus dem Windows Certificate System Store	Sie können Open VPN mit einem Zertifikat aus dem Windows Certificate System Store verwenden.	25. Februar 2021
Self-Service-Portal	Sie können auf ein Self-Service-Portal zugreifen, um die zuletzt AWS bereitgestellte Client- und Konfigurationsdatei abzurufen.	29. Oktober 2020
AWS bereitgestellter Kunde	Sie können den AWS bereitgestellten Client verwenden, um eine Verbindung zu einem VPN Client-Endpunkt herzustellen.	4. Februar 2020
Erstversion	In dieser Version wird der AWS Client eingeführtVPN.	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.