ユーザーガイド

AWS クライアント VPN

AWS クライアント VPN: ユーザーガイド

Table of Contents

AWS クライアントとは VPN

AWS クライアントVPNは、オンプレミスネットワーク内のリソースとリソースに安全にアクセスできる AWS マネージドクライアントベースのVPNサービスです。

このガイドでは、デバイス上のクライアントアプリケーションを使用してクライアントVPNエンドポイントVPNへの接続を確立する手順について説明します。

クライアントVPNコンポーネント

AWS クライアント を使用するための主要なコンポーネントを次に示しますVPN。

- クライアントVPNエンドポイント — クライアントVPN管理者は、 でクライアントVPNエンドポイントを作成して設定します AWS。管理者は、VPN接続を確立するときにアクセスできるネットワークとリソースを制御します。
- VPN クライアントアプリケーション — クライアントVPNエンドポイントに接続し、安全なVPN接続を確立するために使用するソフトウェアアプリケーション。
- クライアントVPNエンドポイント設定ファイル — クライアントVPN管理者から提供される設定ファイル。ファイルには、クライアントVPNエンドポイントに関する情報と、VPN接続を確立するために必要な証明書が含まれています。このファイルを選択したVPNクライアントアプリケーションにロードします。

クライアントを設定するための追加リソース VPN

クライアントVPN管理者の場合、クライアントVPNエンドポイントの作成と設定の詳細については、AWS Client VPN 「 管理者ガイド」を参照してください。

の使用を開始する AWS Client VPN

VPN セッションを確立する前に、クライアントVPN管理者はクライアントVPNエンドポイントを作成して設定する必要があります。管理者は、VPNセッションの確立時にアクセスできるネットワークとリソースを制御します。次に、VPNクライアントアプリケーションを使用してクライアントVPNエンドポイントに接続し、安全なVPN接続を確立します。

クライアントVPNエンドポイントを作成する必要がある管理者の場合は、AWS Client VPN 「 管理者ガイド」を参照してください。

トピック

クライアントを使用するための前提条件 VPN

VPN 接続を確立するには、以下が必要です。

- インターネットへのアクセス
- サポートされているデバイス
- SAMLベースのフェデレーション認証 (シングルサインオン) を使用するクライアントVPNエンドポイントの場合、次のいずれかのブラウザ。
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

ステップ 1: VPNクライアントアプリケーションを取得する

クライアントVPNエンドポイントに接続し、 AWS 提供されたクライアントまたは別の Open VPN ベースのクライアントアプリケーションを使用してVPN接続を確立できます。

AWS が提供するクライアントは、Windows、macOS、Ubuntu 18.04LTS、および Ubuntu 20.04 でサポートされていますLTS。

クライアントVPNアプリケーションは、管理者がアプリケーションのエンドポイント設定ファイルを作成したかどうかに応じて、次の 2 つの方法のいずれかでダウンロードできます。

- 管理者がエンドポイント設定ファイルを設定していない場合は、クライアントのダウンロードからAWS クライアントVPNをダウンロードしてインストールします。アプリケーションをダウンロードしてインストールしたら、 the section called “ステップ 2: クライアントVPNエンドポイント設定ファイルを取得する”に進み、管理者からエンドポイント設定ファイルを取得します。
- 管理者がエンドポイント設定ファイルを既に事前設定している場合は、セルフサービスポータルからクライアントVPNアプリケーションを設定ファイルとともにダウンロードできます。セルフサービスポータルからクライアントと設定ファイルをダウンロードする手順については、「」を参照してくださいthe section called “クライアントをダウンロードする VPN”。アプリケーションとファイルをダウンロードしてインストールしたら、 に移動しますthe section called “ステップ 3: に接続する VPN”。

または、VPN接続を確立する予定のデバイスに Open VPNクライアントアプリケーションをダウンロードしてインストールします。

ステップ 2: クライアントVPNエンドポイント設定ファイルを取得する

管理者からクライアントVPNエンドポイント設定ファイルを取得します。設定ファイルには、クライアントVPNエンドポイントに関する情報と、VPN接続を確立するために必要な証明書が含まれています。

または、クライアントVPN管理者がクライアントVPNエンドポイントのセルフサービスポータルを設定している場合は、 AWS 提供されているクライアントの最新バージョンとクライアントVPNエンドポイント設定ファイルの最新バージョンを自分でダウンロードできます。詳細については、「セルフサービスポータル AWS Client VPN から をダウンロードする」を参照してください。

ステップ 3: に接続する VPN

クライアントVPNエンドポイント設定ファイルを AWS 、提供されたクライアントまたは Open VPN クライアントアプリケーションにインポートし、 に接続しますVPN。エンドポイント設定ファイルのインポートなどVPN、 に接続する手順については、以下のトピックを参照してください。

- AWS が提供するクライアントを使用してクライアントVPNエンドポイントに接続する
- OpenVPN クライアントを使用してクライアントVPNエンドポイントに接続する

Active Directory 認証を使用するクライアントVPNエンドポイントの場合、ユーザー名とパスワードの入力を求められます。ディレクトリで多要素認証 (MFA) が有効になっている場合は、MFAコードの入力も求められます。

SAMLベースのフェデレーティッド認証 (シングルサインオン) を使用するクライアントVPNエンドポイントの場合、 AWS 提供されたクライアントはコンピュータでブラウザウィンドウを開きます。クライアントVPNエンドポイントに接続する前に、会社の認証情報を入力するように求められます。

セルフサービスポータル AWS Client VPN から をダウンロードする

セルフサービスポータルは、 AWS 提供されているクライアントの最新バージョンとクライアントVPNエンドポイント設定ファイルの最新バージョンをダウンロードできるウェブページです。クライアントVPNエンドポイント管理者がクライアントクライアントの設定ファイルを事前に設定している場合はVPN、このポータルからそのクライアントVPNアプリケーションを設定ファイルとともにダウンロードしてインストールできます。

> **Note**
>
> 管理者がセルフサービスポータルを設定する場合は、「 管理者ガイド」の「クライアントVPNエンドポイント」を参照してください。 AWS Client VPN

開始する前に、クライアントVPNエンドポイントの ID が必要です。クライアントVPNエンドポイントの管理者は、ID を提供するか、ID URLを含むセルフサービスポータルを提供できます。

セルフサービスポータルにアクセスするには

1. https://self-service.clientvpn.amazonaws.com/ のセルフサービスポータルにアクセスするか、管理者からURL提供された を使用します。
2. 必要に応じて、 など、クライアントVPNエンドポイントの ID を入力しますcvpn-endpoint-0123456abcd123456。[Next (次へ)] を選択します。
3. ユーザー名とパスワードを入力し、[サインイン] を選択します。これは、クライアントVPNエンドポイントへの接続に使用するユーザー名とパスワードと同じです。

4. セルフサービスポータルでは、以下の操作を行うことができます。

   - クライアントVPNエンドポイントのクライアント設定ファイルの最新バージョンをダウンロードします。
   - プラットフォーム用に AWS 提供されているクライアントの最新バージョンをダウンロードします。

AWS が提供するクライアントを使用してクライアントVPNエンドポイントに接続する

AWS 提供されたクライアントを使用して、クライアントVPNエンドポイントに接続できます。AWS が提供するクライアントは、Windows、macOSUbuntu 18.04LTS、および Ubuntu 20.04 でサポートされています。 LTS

クライアント

- AWS Client VPN for Windows
- AWS Client VPN macOS 用
- AWS Client VPN Linux 用

オープンVPNディレクティブ

AWS が提供するクライアントは、次の OpenVPN ディレクティブをサポートしています。

- 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
- キー
- 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 for Windows

このセクションでは、Windows 用の AWS が提供するクライアントを使用してVPN接続を確立する方法について説明します。クライアントは、クライアントダウンロード AWS でVPNダウンロードしてインストールできます。 AWS が提供するクライアントは、自動更新をサポートしていません。

要件

AWS が提供する Windows 用クライアントを使用するには、以下が必要です。

- Windows 10 または Windows 11 (64 ビットオペレーティングシステム、x64 プロセッサ)
- 。NET フレームワーク 4.7.2 以降

クライアントはコンピュータのTCPポート 8096 を予約します。SAMLベースのフェデレーション認証 (シングルサインオン) を使用するクライアントVPNエンドポイントの場合、クライアントはTCPポート 35001 を予約します。

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

トピック

- Windows 用の AWS 提供のクライアントVPNを使用してクライアントに接続する
- AWS Client VPN for Windows リリースノート

Windows 用の AWS 提供のクライアントVPNを使用してクライアントに接続する

開始する前に、必ず「要件」を参照してください。 AWS 提供されたクライアントは、次のステップではAWS VPN クライアントとも呼ばれます。

AWS が提供する Windows 用クライアントを使用して接続するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [File (ファイル)]、[Manage Profiles (プロファイルの管理)] の順に選択します。
3. [Add Profile (プロファイルの追加)] を選択します。
4. [Display Name (表示名)] に、プロファイルの名前を入力します。
5. VPN 設定ファイル で、クライアントVPN管理者から受け取った設定ファイルを参照して選択し、プロファイルの追加 を選択します。
6. [AWS VPN クライアント] ウィンドウで、プロファイルが選択されていることを確認し、[接続] を選択します。クライアントVPNエンドポイントが認証情報ベースの認証を使用するように設定されている場合は、ユーザー名とパスワードの入力を求められます。

7. 接続の統計を表示するには、[Connection (接続)]、[Show Details (詳細を表示)] の順に選択します。
8. 切断するには、[AWS VPN クライアント] ウィンドウで、[切断] を選択します。または、Windows タスクバーでクライアントアイコンを選択し、[Disconnect (切断)] を選択します。

AWS Client VPN for Windows リリースノート

次の表に、 for AWS Client VPN Windows の現在および以前のバージョンのリリースノートとダウンロードリンクを示します。

> **Note**
>
> リリースのたびに、使いやすさとセキュリティの修正が引き続き提供されます。すべてのプラットフォームで最新バージョンを使用することを強くお勧めします。以前のバージョンは、ユーザビリティやセキュリティの問題の影響を受ける可能性があります。詳細については、リリースノートを参照してください。

Version	変更	日付	ダウンロードリンクと SHA256
3.14.0	• `tap-sleep` Open VPNフラグのサポートが追加されました。 • Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 8 月 12 日	ダウンロードバージョン 3.14.0 sha256: 812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516
3.13.0	Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 7 月 29 日	ダウンロードバージョン 3.13.0

Version	変更	日付	ダウンロードリンクと SHA256
			sha256: c9cc896e81a7441184 0951e349eed9384507 c53337fb703c5ec64d 522c29388b
3.12.1	Windows クライアントバージョン 3.12.0 が一部のユーザーに対してVPN接続を確立できない問題を修正しました。	2024 年 7 月 18 日	ダウンロードバージョン 3.12.1 sha256: 5ed34aee6c03aa281e 625acdbed272896c67 046364a9e5846ca697 e05dbfec08
3.12.0	• ローカルエリアのネットワーク範囲が変更されると、自動的に再接続します。 • SAML エンドポイントに接続するときの自動アプリケーションフォーカスを削除しました。	2024 年 5 月 21 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
3.11.2	バージョン 123 以降の Chromium ベースのブラウザのSAML認証の問題を解決しました。	2024 年 4 月 11 日	ダウンロードバージョン 3.11.2 sha256: 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc
3.11.1	• ローカルアクターが昇格されたアクセス許可を持つ任意のコマンドを実行できるようにする可能性のあるバッファオーバーフローアクションを修正しました。 • セキュリティ体制を強化しました。	2024 年 2 月 16 日	ダウンロードバージョン 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Windows による接続の問題を修正しましたVMs。 • 一部のLAN設定の接続の問題を修正しました。 • アクセシビリティを改善しました。	2023 年 12 月 6 日	ダウンロードバージョン 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version	変更	日付	ダウンロードリンクと SHA256
3.10.0	• クライアントネットワークで NAT64が有効になっている場合の接続の問題を修正しました。 • Hyper-V ネットワークアダプターがクライアントマシンにインストールされている場合の接続に関する問題を修正しました。 • 軽微なバグの修正と機能強化。	2023 年 8 月 24 日	ダウンロードバージョン 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	セキュリティ体制を強化しました。	2023 年 8 月 3 日	ダウンロードバージョン 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	セキュリティ体制を強化しました。	2023 年 7 月 15 日	サポートは終了しました
3.7.0	バージョン 3.6.0 からの変更をロールバック。	2023 年 7 月 15 日	サポートは終了しました
3.6.0	セキュリティ体制を強化しました。	2023 年 7 月 14 日	サポートは終了しました
3.5.0	軽微なバグの修正と機能強化。	2023 年 4 月 3 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
3.4.0	バージョン 3.3.0 からの変更をロールバック。	2023 年 3 月 28 日	サポートは終了しました
3.3.0	軽微なバグの修正と機能強化。	2023 年 3 月 17 日	サポートは終了しました
3.2.0	• 「verify-x509-name」オープンVPNフラグのサポートが追加されました。 • 更新されたバージョンが利用可能になると自動的に検出します。 • 新しいクライアントバージョンが利用可能になると、自動的にインストールする機能が追加されました。	2023 年 1 月 23 日	サポートは終了しました
3.1.0	セキュリティ体制を強化しました。	2022 年 5 月 23 日	サポートは終了しました
3.0.0	• Windows 11 のサポートが追加されました。 • 他のドライバー名に影響する TAP Windows ドライバーの名前を修正しました。 • フェデレーション認証を使用しているときにバナーメッセージが表示されない問題を修正しました。 • 長いテキストのバナーテキスト表示を修正しました。 • セキュリティ体制を強化しました。	2022 年 3 月 3 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
2.0.0	• 新規接続確立後のバナーテキストのサポートが追加されました。 • echo に関連して pull-filter を使用する機能 pull-filter * echo を削除しました。 • 軽微なバグの修正と機能強化。	2022 年 1 月 20 日	サポートは終了しました
1.3.7	• 場合によって、フェデレーション認証接続の試行が修正されました。 • 軽微なバグの修正と機能強化。	2021 年 11 月 8 日	サポートは終了しました
1.3.6	• Open VPNフラグのサポートが追加されました： connect-retry-max、dev-type、 keepalive、ping、ping-restart、pul、rcvbuf、 server-poll-timeout。 • 軽微なバグの修正と機能強化。	2021 年 9 月 20 日	サポートは終了しました
1.3.5	大きな Windows ログファイルを削除するためのパッチ。	2021 年 8 月 16 日	サポートは終了しました
1.3.4	• Open VPNフラグのサポートが追加されました: dhcp-option。 • 軽微なバグの修正と機能強化。	2021 年 8 月 4 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
1.3.3	• Open VPNフラグのサポートが追加されました: 非アクティブ、プルフィルター、ルート。 • 切断時または終了時にアプリがクラッシュするという問題を修正しました。 • バックスラッシュを使用した Active Directory ユーザー名の問題を修正しました。 • アプリの外部でプロファイルリストを操作するときのアプリのクラッシュが修正されました。 • 軽微なバグの修正と機能強化。	2021 年 7 月 1 日	サポートは終了しました
1.3.2	• IPv6 リーク防止は、設定時に追加します。 • [接続] の [詳細を表示] オプションを使用する際に発生する可能性のあるクラッシュが修正されました。	2021 年 5 月 12 日	サポートは終了しました
1.3.1	• 同じサブジェクトを持つ複数のクライアント証明書のサポートが追加されました。期限切れの証明書は無視されます。 • ディスク使用量を減らすために、ローカルログ保持が修正されました。 • 「route-ipv6」Open VPNディレクティブのサポートを追加しました。 • 軽微なバグの修正と機能強化。	2021 年 4 月 5 日	サポートは終了しました
1.3.0	エラー報告、診断ログの送信、分析などのサポート機能が追加されました。	2021 年 3 月 8 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
1.2.7	• cryptoapicert OpenVPN ディレクティブのサポートが追加されました。 • 接続間の古いルートを修正しました。 • 軽微なバグの修正と機能強化。	2021 年 2 月 25 日	サポートは終了しました
1.2.6	軽微なバグの修正と機能強化。	2020 年 10 月 26 日	サポートは終了しました
1.2.5	• Open VPN設定でコメントのサポートが追加されました。 • TLS ハンドシェイクエラーのエラーメッセージを追加しました。	2020 年 10 月 8 日	サポートは終了しました
1.2.4	軽微なバグの修正と機能強化。	2020 年 9 月 1 日	サポートは終了しました
1.2.3	バージョン 1.2.2 での変更をロールバックします。	2020 年 8 月 20 日	サポートは終了しました
1.2.1	軽微なバグの修正と機能強化。	2020 年 7 月 1 日	サポートは終了しました
1.2.0	• SAML 2.0 ベースのフェデレーション認証 のサポートが追加されました。 • Windows 7 プラットフォームのサポートを廃止。	2020 年 5 月 19 日	サポートは終了しました
1.1.1	軽微なバグの修正と機能強化。	2020 年 4 月 21 日	サポートは終了しました
1.1.0	• ユーザーインターフェイスに表示されるテキストを非表示または表示するための OpenVPN static challenge echo 機能のサポートが追加されました。 • 軽微なバグの修正と機能強化。	2020 年 3 月 9 日	サポートは終了しました

Version	変更	日付	ダウンロードリンクと SHA256
1.0.0	初回リリース。	2020 年 2 月 4 日	サポートは終了しました

AWS Client VPN macOS 用

このセクションでは、macOS 用に AWS 提供されたクライアントを使用してVPN接続を確立する方法について説明します。クライアントは、クライアントダウンロード でAWS VPNダウンロードしてインストールできます。 AWS が提供するクライアントは、自動更新をサポートしていません。

要件

AWS が提供するクライアントを macOS に使用するには、以下が必要です。

- macOS Monterey (12.0)、Ventura (13.0)、または Sonoma (14.0)。
- x86_64 プロセッサ互換。
- クライアントはコンピュータのTCPポート 8096 を予約します。
- SAMLベースのフェデレーション認証 (シングルサインオン) を使用するクライアントVPNエンドポイントの場合、クライアントはTCPポート 35001 を予約します。

> **Note**
>
> Apple シリコンプロセッサで Mac を使用している場合は、クライアントソフトウェアを実行するために、Rosetta 2 をインストールする必要があります。詳細については、Apple のウェブサイトの「ロゼッタ変換環境について」を参照してください。

トピック

- macOS 用の AWS が提供するクライアントVPNを使用してクライアントに接続する
- AWS Client VPN for macOS リリースノート

macOS 用の AWS が提供するクライアントVPNを使用してクライアントに接続する

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

また、必ず「要件」を参照してください。 AWS 提供されたクライアントは、次のステップではAWS VPN クライアントとも呼ばれます。

AWS 提供された macOS 用クライアントを使用して接続するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [File (ファイル)]、[Manage Profiles (プロファイルの管理)] の順に選択します。
3. [Add Profile (プロファイルの追加)] を選択します。
4. [Display Name (表示名)] に、プロファイルの名前を入力します。
5. VPN 設定ファイル で、クライアントVPN管理者から受け取った設定ファイルを参照します。[Open (開く)] を選択します。
6. [Add Profile (プロファイルの追加)] を選択します。
7. [AWS VPN クライアント] ウィンドウで、プロファイルが選択されていることを確認し、[接続] を選択します。クライアントVPNエンドポイントが認証情報ベースの認証を使用するように設定されている場合は、ユーザー名とパスワードの入力を求められます。
8. 接続の統計を表示するには、[Connection (接続)]、[Show Details (詳細を表示)] の順に選択します。
9. 切断するには、[AWS VPN クライアント] ウィンドウで、[切断] を選択します。または、メニューバーのクライアントアイコンを選択し、切断 < your-profile-name > を選択します。

AWS Client VPN for macOS リリースノート

次の表に、macOS 用 AWS Client VPN の現在および以前のバージョンのリリースノートとダウンロードリンクを示します。

> **Note**
>
> リリースのたびに、使いやすさとセキュリティの修正が引き続き提供されます。すべてのプラットフォームで最新バージョンを使用することを強くお勧めします。以前のバージョン

は、ユーザビリティやセキュリティの問題の影響を受ける可能性があります。詳細については、リリースノートを参照してください。

Version	変更	日付	ダウンロードリンク
3.12.0	• `tap-sleep` Open VPNフラグのサポートが追加されました。 • Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 8 月 12 日	ダウンロードバージョン 3.12.0 sha256: 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 7 月 29 日	ダウンロードバージョン 3.11.0 sha256: 44b5e6f84 788bf45dd b77871d74 3e09007e1 597555850 6221b8cae a81732848f
3.10.0	• ローカルエリアのネットワーク範囲が変更されると、自動的に再接続します。 • ネットワークスイッチ中のDNS復元の問題を修正しました。	2024 年 5 月 21 日	ダウンロードバージョン 3.10.0 sha256: 28bf26fa1 34b01ff12703cf59ff fa4adba7c 44ceb793d

Version	変更	日付	ダウンロードリンク
	• SAML エンドポイントに接続するときの自動アプリケーションフォーカスを削除しました。		ce4addd44 04e84287dd
3.9.2	• バージョン 123 以降の Chromium ベースのブラウザのSAML認証の問題を解決しました。 • macOS Sonoma のサポートを追加しました。macOS Big Sur のサポートを廃止します。 • セキュリティ体制を強化しました。	2024 年 4 月 11 日	ダウンロードバージョン 3.9.2 sha256: 374467d99 1e8953b50 32e5b985c da80a0ea2 7fb5d5f23 cf16c556a 1568b0d480
3.9.1	• ローカルアクターが昇格されたアクセス許可を持つ任意のコマンドを実行できるようにする可能性のあるバッファオーバーフローアクションを修正しました。 • アプリケーション更新のダウンロードの進行状況バーを修正しました。 • セキュリティ体制を強化しました。	2024 年 2 月 16 日	ダウンロードバージョン 3.9.1 sha256: 9bba4b27a 635e75038 703e2cf4c d814aa753 06179fac8 e500e2c7a f4e899e971

Version	変更	日付	ダウンロードリンク
3.9.0	• 一部のLAN設定の接続の問題を修正しました。 • アクセシビリティを改善しました。	2023 年 12 月 6 日	ダウンロードバージョン 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• クライアントネットワークで NAT64が有効になっている場合の接続の問題を修正しました。 • 軽微なバグの修正と機能強化。	2023 年 8 月 24 日	ダウンロードバージョン 3.8.0 sha256: d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• セキュリティ体制を強化しました。	2023 年 8 月 3 日	ダウンロードバージョン 3.7.0 sha256: 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a

Version	変更	日付	ダウンロードリンク
3.6.0	• セキュリティ体制を強化しました。	2023 年 7 月 15 日	サポートは終了しました
3.5.0	• バージョン 3.4.0 からの変更をロールバック。	2023 年 7 月 15 日	サポートは終了しました
3.4.0	• セキュリティ体制を強化しました。	2023 年 7 月 14 日	サポートは終了しました
3.3.0	• macOS Ventura (13.0) のサポートを追加。 • 軽微なバグの修正と機能強化。	2023 年 4 月 27 日	サポートは終了しました
3.2.0	• 「verify-x509-name」オープンVPNフラグのサポートを追加しました。 • 更新されたバージョンが利用可能になると自動的に検出します。 • 新しいクライアントバージョンが利用可能になると、自動的にインストールする機能が追加されました。	2023 年 1 月 23 日	サポートは終了しました
3.1.0	• macOS Monterey のサポートを追加しました。 • ドライブの種類検出の問題を修正しました。 • セキュリティ体制を強化しました。	2022 年 5 月 23 日	サポートは終了しました
3.0.0	• フェデレーション認証を使用しているときにバナーメッセージが表示されない問題を修正しました。 • 長いテキストのバナーテキスト表示を修正しました。 • セキュリティ体制を強化しました。	2022 年 3 月 3 日	サポートは終了しました。

Version	変更	日付	ダウンロードリンク
2.0.0	• 新規接続確立後のバナーテキストのサポートが追加されました。 • echo に関連して pull-filter を使用する機能 pull-filter * echo を削除しました。 • 軽微なバグの修正と機能強化。	2022 年 1 月 20 日	サポートは終了しました。
1.4.0	• 接続中のDNSサーバーモニタリングを追加しました。設定が一致しない場合、VPN設定は再設定されます。 • 場合によって、フェデレーション認証接続の試行が修正されました。 • 軽微なバグの修正と機能強化。	2021 年 11 月 9 日	サポートは終了しました。
1.3.5	• Open VPNフラグのサポートが追加されました： connect-retry-max、dev-type、 keepalive、ping、ping-restart、pul、rcvbuf、 server-poll-timeout。 • 軽微なバグの修正と機能強化。	2021 年 9 月 20 日	サポートは終了しました。
1.3.4	• Open VPNフラグのサポートが追加されました: dhcp-option。 • 軽微なバグの修正と機能強化。	2021 年 8 月 4 日	サポートは終了しました。

Version	変更	日付	ダウンロードリンク
1.3.3	• Open VPNフラグのサポートが追加されました: 非アクティブ、プルフィルター、ルート。 • スペースまたは Unicode を含む設定ファイル名に関する問題を修正しました。 • 切断時または終了時にアプリがクラッシュするという問題を修正しました。 • バックスラッシュを使用した Active Directory ユーザー名の問題を修正しました。 • アプリの外部でプロファイルリストを操作するときのアプリのクラッシュが修正されました。 • 軽微なバグの修正と機能強化。	2021 年 7 月 1 日	サポートは終了しました。
1.3.2	• IPv6 リーク防止は、設定時に追加します。 • [接続] の [詳細を表示] オプションを使用する際に発生する可能性のあるクラッシュが修正されました。 • デーモンのログローテーションを追加します。	2021 年 5 月 12 日	サポートは終了しました。

Version	変更	日付	ダウンロードリンク
1.3.1	• macOS Big Sur (10.16) のサポートを追加。 • 他のアプリケーションによって設定されたDNS設定を削除する問題を修正しました。 • 相互認証に有効でない証明書を使用して接続の問題が発生する問題を修正しました。 • 「route-ipv6」Open VPNディレクティブのサポートが追加されました。 • 軽微なバグの修正と機能強化。	2021 年 4 月 5 日	サポートは終了しました。
1.3.0	エラー報告、診断ログの送信、分析などのサポート機能が追加されました。	2021 年 3 月 8 日	サポートは終了しました。
1.2.5	軽微なバグの修正と機能強化。	2021 年 2 月 25 日	サポートは終了しました。
1.2.4	軽微なバグの修正と機能強化。	2020 年 10 月 26 日	サポートは終了しました。
1.2.3	• Open VPN設定でコメントのサポートを追加しました。 • TLS ハンドシェイクエラーのエラーメッセージを追加しました。 • 一部のユーザーに影響を与えていたアンインストールのバグを修正。	2020 年 10 月 8 日	サポートは終了しました。
1.2.2	軽微なバグの修正と機能強化。	2020 年 8 月 12 日	サポートは終了しました。
1.2.1	• アプリケーションのアンインストールのサポートを追加。 • 軽微なバグの修正と機能強化。	2020 年 7 月 1 日	サポートは終了しました。

Version	変更	日付	ダウンロードリンク
1.2.0	• SAML 2.0 ベースのフェデレーション認証 のサポートが追加されました。 • macOS Catalina (10.15) のサポートを追加。	2020 年 5 月 19 日	サポートは終了しました。
1.1.2	軽微なバグの修正と機能強化。	2020 年 4 月 21 日	サポートは終了しました。
1.1.1	• が解決されない問題を修正DNSしました。 • 長時間の接続によるアプリのクラッシュの問題を修正。 • MFA 問題を修正しました。	2020 年 4 月 2 日	サポートは終了しました。
1.1.0	• macOS DNS設定のサポートが追加されました。 • ユーザーインターフェイスに表示されるテキストを非表示または表示するための OpenVPN static challenge echo 機能のサポートが追加されました。 • 軽微なバグの修正と機能強化。	2020 年 3 月 9 日	サポートは終了しました。
1.0.0	初回リリース。	2020 年 2 月 4 日	サポートは終了しました。

AWS Client VPN Linux 用

このセクションでは、Linux 用に AWS が提供するクライアントをインストールし、提供された AWS クライアントを使用してVPN接続を確立する方法について説明します。 AWS が提供する Linux 用クライアントは、自動更新をサポートしていません。最新の更新とダウンロードについては、「」を参照してくださいthe section called “リリースノート”。

Linux 用の AWS 提供のクライアントVPNでクライアントに接続するための要件

AWS が提供する Linux 用クライアントを使用するには、以下が必要です。

- Ubuntu 18.04 LTSまたは Ubuntu 20.04 LTS (AMD64 のみ)

クライアントはコンピュータのTCPポート 8096 を予約します。SAMLベースのフェデレーション認証 (シングルサインオン) を使用するクライアントVPNエンドポイントの場合、クライアントはTCPポート 35001 を予約します。

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

トピック

- Linux 用の AWS 提供のクライアントをインストールする
- Linux 用の AWS 提供のクライアントに接続する
- AWS Client VPN for Linux リリースノート

Linux 用の AWS 提供のクライアントをインストールする

Linux 用の AWS 提供のクライアントをインストールするために使用できる方法は複数あります。次のオプションのどれか 1 つを使用します。開始する前に、必ず「要件」を参照してください。

オプション 1: パッケージリポジトリ経由で をインストールする

1. AWS VPN クライアントパブリックキーを Ubuntu OS に追加します。

```
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. Ubuntu のバージョンに応じて、適切なコマンドを使用して Ubuntu OS にリポジトリを追加します。

   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. 次のコマンドを使用して、システム上のリポジトリを更新します。

```
sudo apt-get update
```

4. 次のコマンドを使用して、Linux 用の AWS が提供するクライアントをインストールします。

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

オプション 2: .deb パッケージファイルを使用して をインストールする

1. AWS クライアントのダウンロードから、または次のコマンドを使用して、.deb ファイルVPNをダウンロードします。

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

2. dpkg ユーティリティを使用して、Linux 用に AWS 提供されているクライアントをインストールします。

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

オプション 3 — Ubuntu ソフトウェアセンターを使用して .deb パッケージをインストールする

1. クライアントダウンロード から AWS .deb パッケージファイルVPNをダウンロードします。
2. .deb パッケージファイルをダウンロードしたら、Ubuntu ソフトウェアセンターを使用してパッケージをインストールします。Ubuntu ソフトウェアセンターを使用してスタンドアロンの .deb パッケージからインストールする手順に従います。詳細については、Ubuntu Wiki を参照してください。

Linux 用の AWS 提供のクライアントに接続する

AWS 提供されたクライアントは、次のステップではAWS VPN クライアントとも呼ばれます。

Linux 用の AWS が提供するクライアントを使用して接続するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [File (ファイル)]、[Manage Profiles (プロファイルの管理)] の順に選択します。
3. [Add Profile (プロファイルの追加)] を選択します。
4. [Display Name (表示名)] に、プロファイルの名前を入力します。
5. VPN 設定ファイル で、クライアントVPN管理者から受け取った設定ファイルを参照します。[Open (開く)] を選択します。
6. [Add Profile (プロファイルの追加)] を選択します。
7. [AWS VPN クライアント] ウィンドウで、プロファイルが選択されていることを確認し、[接続] を選択します。クライアントVPNエンドポイントが認証情報ベースの認証を使用するように設定されている場合は、ユーザー名とパスワードの入力を求められます。
8. 接続の統計を表示するには、[Connection (接続)]、[Show Details (詳細を表示)] の順に選択します。
9. 切断するには、[AWS VPN クライアント] ウィンドウで、[切断] を選択します。

AWS Client VPN for Linux リリースノート

次の表に、 AWS Client VPN Linux 用 の現在および以前のバージョンのリリースノートとダウンロードリンクを示します。

> **Note**
>
> リリースのたびに、使いやすさとセキュリティの修正が引き続き提供されます。すべてのプラットフォームで最新バージョンを使用することを強くお勧めします。以前のバージョンは、ユーザビリティやセキュリティの問題の影響を受ける可能性があります。詳細については、リリースノートを参照してください。

Version	変更	日付	ダウンロードリンク
3.15.0	• `tap-sleep` Open VPNフラグのサポートが追加されました。 • Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 8 月 12 日	ダウンロードバージョン 3.15.0 sha256: 5cf3eb08de96821b0ad3d0c93174b2e308041d5490a3edb772dfd89a6d89d012
3.14.0	• Open VPNライブラリと Open SSLライブラリを更新しました。	2024 年 7 月 29 日	ダウンロードバージョン 3.14.0 sha256: bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60
3.13.0	• ローカルエリアのネットワーク範囲が変更されると、自動的に再接続します。	2024 年 5 月 21 日	ダウンロードバージョン 3.13.0 sha256: e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1

Version	変更	日付	ダウンロードリンク
3.12.2	• バージョン 123 以降の Chromium ベースのブラウザのSAML認証の問題を解決しました。	2024 年 4 月 11 日	ダウンロードバージョン 3.12.2 sha256: f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
3.12.1	• ローカルアクターが昇格されたアクセス許可を持つ任意のコマンドを実行できるようにする可能性のあるバッファオーバーフローアクションを修正しました。 • セキュリティ体制を強化しました。	2024 年 2 月 16 日	ダウンロードバージョン 3.12.1 sha256: 547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• 一部のLAN設定の接続の問題を修正しました。	2023 年 12 月 19 日	ダウンロードバージョン 3.12.0 sha256: 9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1

Version	変更	日付	ダウンロードリンク
3.11.0	• 「一部のLAN設定の接続の問題を修正しました」のロールバック。 • アクセシビリティを改善しました。	2023 年 12 月 6 日	ダウンロードバージョン 3.11.0 sha256: 86c0fa1bf1c97194082835a739ec7f1c87e540194955f414a35c679b94538970
3.10.0	• 一部のLAN設定の接続の問題を修正しました。 • アクセシビリティを改善しました。	2023 年 12 月 6 日	ダウンロードバージョン 3.10.0 sha256: e7450b2490f3b96ab7d589a8000d838d9fd2adcdd72ae80666c4c0d900687e51
3.9.0	• クライアントネットワークで NAT64が有効になっている場合の接続の問題を修正しました。 • 軽微なバグの修正と機能強化。	2023 年 8 月 24 日	ダウンロードバージョン 3.9.0 sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454

Version	変更	日付	ダウンロードリンク
3.8.0	• セキュリティ体制を強化しました。	2023 年 8 月 3 日	ダウンロードバージョン 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• セキュリティ体制を強化しました。	2023 年 7 月 15 日	サポートは終了しました
3.6.0	• バージョン 3.5.0 からの変更をロールバック。	2023 年 7 月 15 日	サポートは終了しました
3.5.0	• セキュリティ体制を強化しました。	2023 年 7 月 14 日	サポートは終了しました
3.4.0	• 「verify-x509-name」オープンVPNフラグのサポートが追加されました。	2023 年 2 月 14 日	サポートは終了しました
3.1.0	• ドライブの種類検出の問題を修正しました。 • セキュリティ体制を強化しました。	2022 年 5 月 23 日	サポートは終了しました
3.0.0	• フェデレーション認証を使用しているときにバナーメッセージが表示されない問題を修正しました。 • 長いテキストと特定の文字シーケンスのバナーテキスト表示を修正しました。 • セキュリティ体制を強化しました。	2022 年 3 月 3 日	サポートは終了しました。

Version	変更	日付	ダウンロードリンク
2.0.0	• 新規接続確立後のバナーテキストのサポートが追加されました。 • echo に関連して pull-filter を使用する機能 pull-filter * echo を削除しました。 • 軽微なバグの修正と機能強化。	2022 年 1 月 20 日	サポートは終了しました。
1.0.3	• 場合によって、フェデレーション認証接続の試行が修正されました。 • 軽微なバグの修正と機能強化。	2021 年 11 月 8 日	サポートは終了しました。
1.0.2	• Open VPNフラグのサポートが追加されました： connect-retry-max、dev-type、 keepalive、ping、ping-restart、pul、rcvbuf、 server-poll-timeout。 • 軽微なバグの修正と機能強化。	2021 年 9 月 28 日	サポートは終了しました。
1.0.1	• Ubuntu アプリケーションバーから終了するオプションが有効になりました。 • Open VPNフラグのサポートが追加されました: 非アクティブ、プルフィルター、ルート。 • 軽微なバグの修正と機能強化。	2021 年 8 月 4 日	サポートは終了しました。
1.0.0	初回リリース。	2021 年 6 月 11 日	サポートは終了しました。

OpenVPN クライアントを使用してクライアントVPNエンドポイントに接続する

一般的な Open クライアントアプリケーションを使用してVPN、クライアントVPNエンドポイントに接続できます。

> **Important**
>
> クライアントVPNエンドポイントが SAMLベースのフェデレーション認証 を使用するように設定されている場合、オープン VPNベースのVPNクライアントを使用してクライアントVPNエンドポイントに接続することはできません。

クライアントアプリケーション

- Windows クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する
- Android または iOS クライアントアプリケーションを使用してVPNクライアントVPNエンドポイントに接続する
- macOS クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する
- OpenVPN クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する

Windows クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する

このセクションでは、Windows ベースのVPNクライアントを使用してVPN接続を確立する方法について説明します。

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

トラブルシューティング情報については、Windows ベースのクライアントとのクライアントVPN接続のトラブルシューティングを参照してください。

> **Important**
>
> クライアントVPNエンドポイントが SAMLベースのフェデレーション認証 を使用するように設定されている場合、オープン VPNベースのVPNクライアントを使用してクライアントVPNエンドポイントに接続することはできません。

タスク

- Open で Windows Certificate System Store の証明書を使用するVPN
- Open を使用するVPN GUI
- OpenVPN Connect クライアントを使用する

Open で Windows Certificate System Store の証明書を使用するVPN

Windows Certificate System Store から証明書とプライベートキーを使用するように OpenVPN クライアントを設定できます。このオプションは、クライアントVPN接続の一部としてスマートカードを使用する場合に便利です。Open client cryptoapicert オプションの詳細については、VPN「Open ウェブサイト」の「Open VPNのリファレンスマニュアル」を参照してください。VPN

> **Note**
>
> 証明書はローカルコンピュータに保存する必要があります。

Open で cryptoapicert オプションを使用するにはVPN

1. クライアント証明書と秘密キーを含む .pfx ファイルを作成します。
2. .pfx ファイルをローカルコンピュータの個人証明書ストアにインポートします。詳細については、Microsoft ウェブサイトの「ハウツー: MMCスナップインで証明書を表示する」を参照してください。
3. アカウントにローカルコンピュータの証明書を読み取るためのアクセス権限があることを確認します。Microsoft マネジメントコンソールを使用して、アクセス権限を変更できます。詳細については、Microsoft Technet ウェブサイトの「Rights to see the local computer certificates store」をご参照ください。
4. Open VPN設定ファイルを更新し、証明書の件名または証明書のサムプリントを使用して証明書を指定します。

サブジェクトを使用して証明書を指定する例を次に示します。

```
cryptoapicert “SUBJ:Jane Doe”
```

サムプリントを使用して証明書を指定する例を次に示します。サムプリントは、Microsoft マネジメントコンソールを使用して検索できます。詳細については、Microsoft Technet ウェブサイトの「方法: 証明書のサムプリントを取得する」をご参照ください。

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

設定が完了したら、Open VPNを使用して接続を確立します。

Open を使用するVPN GUI

次の手順は、Windows コンピュータで Open VPNGUIクライアントアプリケーションを使用してVPN接続を確立する方法を示しています。

> **Note**
>
> Open クライアントアプリケーションの詳細については、VPN「Open ウェブサイト」の「コミュニティダウンロードVPN」を参照してください。

VPN 接続を確立するには

1. Open VPNクライアントアプリケーションを起動します。
2. Windows タスクバーで、アイコンの表示/非表示 を選択します。Open VPNGUIを右クリックし、ファイル のインポートを選択します。
3. Open ダイアログボックスで、クライアントVPN管理者から受け取った設定ファイルを選択し、Open を選択します。
4. Windows タスクバーで、アイコンの表示/非表示 を選択します。Open VPNGUIを右クリックし、Connect を選択します。

OpenVPN Connect クライアントを使用する

次の手順は、Windows コンピュータで OpenVPN Connect Client アプリケーションを使用してVPN接続を確立する方法を示しています。

> **Note**
>
> 詳細については、OpenVPN ウェブサイトの「Windows で Access Server に接続する」を参照してください。

VPN 接続を確立するには

1. OpenVPN Connect Client アプリケーションを起動します。
2. Windows タスクバーで、アイコンの表示/非表示 を選択します。Open VPNを右クリックし、プロファイルのインポート を選択します。
3. ファイルからインポートを選択し、クライアントVPN管理者から受け取った設定ファイルを選択します。
4. 接続を開始するには、接続プロファイルを選択します。

Android または iOS クライアントアプリケーションを使用してVPNクライアントVPNエンドポイントに接続する

> **Important**
>
> クライアントVPNエンドポイントが SAMLベースのフェデレーション認証 を使用するように設定されている場合、オープン VPNベースのVPNクライアントを使用してクライアントVPNエンドポイントに接続することはできません。

次の情報は、Android または iOS モバイルデバイスで Open VPNクライアントアプリケーションを使用してVPN接続を確立する方法を示しています。Android 用の手順と iOS 用の手順は同じです。

> **Note**
>
> iOS または Android 用の OpenVPN クライアントアプリケーションのダウンロードと使用の詳細については、「Open ウェブサイト」の「OpenVPN Connect ユーザーガイド」を参照してください。VPN

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

接続を確立するには、オープンVPNクライアントアプリケーションを起動し、クライアントVPN管理者から受け取ったファイルをインポートします。

macOS クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する

このセクションでは、macOS ベースのVPNクライアントを使用してVPN接続を確立する方法について説明します。

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

トラブルシューティング情報については、macOS クライアントとのクライアントVPN接続のトラブルシューティングを参照してください。

> **Important**
>
> クライアントVPNエンドポイントが SAMLベースのフェデレーション認証 を使用するように設定されている場合、オープン VPNベースのVPNクライアントを使用してクライアントVPNエンドポイントに接続することはできません。

トピック

- Tunnelblick を起動して接続を確立する AWS Client VPN
- OpenVPN Connect Client を使用して AWS Client VPN エンドポイントに接続する

Tunnelblick を起動して接続を確立する AWS Client VPN

次の手順は、macOS コンピュータで Tunnelblick クライアントアプリケーションを使用してVPN接続を確立する方法を示しています。

> **Note**
>
> macOS 用 Tunnelblick クライアントアプリケーションの詳細については、Tunnelblick ウェブサイトのTunnelblick マニュアルを参照してください。

VPN 接続を確立するには

1. Tunnelblick クライアントアプリケーションを起動し、[I have configuration files (設定ファイルを持っている)] を選択します。
2. 設定パネルでVPN管理者から受け取った設定ファイルをドラッグアンドドロップします。
3. [Configurations (設定)] パネルで設定ファイルを選択し、[Connect (接続)] を選択します。

OpenVPN Connect Client を使用して AWS Client VPN エンドポイントに接続する

次の手順は、macOS コンピュータで OpenVPN Connect Client アプリケーションを使用してVPN接続を確立する方法を示しています。

> **Note**
>
> 詳細については、OpenVPN ウェブサイトのmacOS を使用した Access Server への接続」を参照してください。

VPN 接続を確立するには

1. Open VPNアプリケーションを起動し、「インポート」、「ローカルファイルから」を選択します。
2. VPN 管理者から受け取った設定ファイルに移動し、 を開くを選択します。

OpenVPN クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続する

このセクションでは、Open VPNベースのVPNクライアントを使用してVPN接続を確立する方法について説明します。

開始する前に、クライアントVPN管理者がクライアントVPNエンドポイントを作成し、クライアントVPNエンドポイント設定ファイル を提供したことを確認してください。

トラブルシューティング情報については、Linux ベースのクライアントとのクライアントVPN接続のトラブルシューティングを参照してください。

> **Important**
>
> クライアントVPNエンドポイントが SAMLベースのフェデレーション認証 を使用するように設定されている場合、オープン VPNベースのVPNクライアントを使用してクライアントVPNエンドポイントに接続することはできません。

トピック

- OpenVPN - Network Manager AWS Client VPN を使用して への接続を作成する
- Open AWS Client VPN を使用して への接続を作成するVPN

OpenVPN - Network Manager AWS Client VPN を使用して への接続を作成する

次の手順は、GUIUbuntu コンピュータの Network Manager を介して Open VPNアプリケーションを使用してVPN接続を確立する方法を示しています。

VPN 接続を確立するには

1. 次のコマンドを使用して、ネットワークマネージャーモジュールをインストールします。

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

2. [Settings (設定)]、[Network (ネットワーク)] に移動します。

3. の横にあるプラス記号 (+) を選択しVPN、ファイルからインポート... を選択します。
4. VPN 管理者から受け取った設定ファイルに移動し、 を開くを選択します。
5. 「追加VPN」ウィンドウで「追加」を選択します。
6. 追加したVPNプロファイルの横にあるトグルを有効にして、接続を開始します。

Open AWS Client VPN を使用して への接続を作成するVPN

次の手順は、Ubuntu コンピュータで Open VPNアプリケーションを使用してVPN接続を確立する方法を示しています。

VPN 接続を確立するには

1. 次のコマンドを使用して OpenVPN をインストールします。

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

2. VPN 管理者から受け取った設定ファイルをロードして接続を開始します。

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

クライアントVPN接続のトラブルシューティング

次のトピックでは、クライアントアプリケーションを使用してクライアントVPNエンドポイントに接続するときに発生する可能性のある問題をトラブルシューティングします。

トピック

管理者向けのクライアントVPNエンドポイントのトラブルシューティング

このガイドのステップの一部は、ユーザーが実行することができます。その他のステップは、クライアントVPN管理者がクライアントVPNエンドポイント自体で実行する必要があります。次のセクションでは、管理者に問い合わせる必要がある場合について説明します。

クライアントVPNエンドポイントの問題のトラブルシューティングの詳細については、「 AWS Client VPN 管理者ガイド」の「 クライアントのトラブルシューティングVPN」を参照してください。

AWS 提供されたクライアントの AWS Support に診断ログを送信する

AWS 提供されたクライアントに問題がある場合、トラブルシューティングのために AWS Support に連絡する必要がある場合、 AWS 提供されたクライアントには診断ログを に送信するためのオプションがあります AWS Support。このオプションは、Windows、macOS、および Linux クライアントアプリケーションで使用できます。

ファイルを送信する前に、 が診断ログにアクセス AWS Support することを許可することに同意する必要があります。同意すると、ファイルにすぐにアクセス AWS Support できるように、 に付与できる参照番号が提供されます。

診断ログの送信

AWS 提供されたクライアントは、次のステップではAWS VPN クライアントとも呼ばれます。

AWS が提供する Windows 用クライアントを使用して診断ログを送信するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [Help] (ヘルプ)、[Send Diagnostic Logs] (診断ログの送信) を選択します。
3. [Send Diagnostic Logs] (診断ログの送信) ウィンドウで、[Yes] (はい) を選択します。
4. [Send Diagnostic Logs] (診断ログの送信) ウィンドウで、次のいずれかの操作を実行します。
   - 参照番号をクリップボードにコピーするには、[はい] を選択してから [OK] を選択します。
   - 参照番号を手動で追跡するには、[No] (いいえ) を選択します。

   に連絡するときは AWS Support、参照番号を提供する必要があります。

AWS 提供された macOS 用クライアントを使用して診断ログを送信するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [Help] (ヘルプ)、[Send Diagnostic Logs] (診断ログの送信) を選択します。
3. [Send Diagnostic Logs] (診断ログの送信) ウィンドウで、[Yes] (はい) を選択します。
4. 確認ウィンドウに表示される参照番号を書き留めて、[OK] を選択します。

   に連絡するときは AWS Support、参照番号を提供する必要があります。

Ubuntu 用に AWS 提供されたクライアントを使用して診断ログを送信するには

1. AWS VPN クライアントアプリケーションを開きます。
2. [Help] (ヘルプ)、[Send Diagnostic Logs] (診断ログの送信) を選択します。
3. [診断ログの送信] ウィンドウで、[送信] を選択します。
4. 確認ウィンドウに表示される参照番号を書き留めます。情報をクリップボードにコピーする選択ができます。

   に連絡するときは AWS Support、参照番号を提供する必要があります。

Windows ベースのクライアントとのクライアントVPN接続のトラブルシューティング

以下のセクションでは、Windows ベースのクライアントを使用してクライアントVPNエンドポイントに接続するときに発生する可能性のある問題について説明します。

トピック

- AWS が提供するクライアント
- オープンVPN GUI
- 接続VPNクライアントを開く

AWS が提供するクライアント

AWS が提供するクライアントは、イベントログを作成し、コンピュータ上の次の場所に保存します。

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

次のタイプのログを使用できます。

- アプリケーションログ: アプリケーションに関する情報が含まれます。これらのログには「aws_vpn_client_」が前に付けられます。
- オープンVPNログ： オープンVPNプロセスに関する情報が含まれます。これらのログには「ovpn_aws_vpn_client_」が前に付けられます。

AWS が提供するクライアントは、Windows サービスを使用してルートオペレーションを実行します。Windows サービスログは、コンピュータ上の次の場所に保存されます。

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

トピック

- クライアントが接続できない
- クライアントがTAP「Windows アダプターなし」というログメッセージで接続できない
- クライアントが再接続状態でスタックしている

- VPN 接続プロセスが予期せず終了する
- アプリケーションが起動しない
- クライアントがプロファイルを作成できない
- Windows 10 または 11 PCsを使用して Dell でクライアントクラッシュが発生する
- VPN ポップアップメッセージで切断する

クライアントが接続できない

問題

AWS 提供されたクライアントは、クライアントVPNエンドポイントに接続できません。

原因

この問題の原因として、次のいずれかが考えられます。

- 別の Open VPNプロセスが既にコンピュータで実行されているため、クライアントは接続できません。
- 設定 (.ovpn) ファイルが有効ではありません。

ソリューション

コンピュータで実行されている他の Open VPNアプリケーションがあるかどうかを確認します。存在する場合は、これらのプロセスを停止または終了し、クライアントVPNエンドポイントへの接続を再試行してください。オープンVPNログにエラーがないか確認し、クライアントVPN管理者に次の情報を確認するよう依頼します。

- 設定ファイルに、正しいクライアントキーと証明書が含まれている。詳細については、AWS Client VPN 管理者ガイドの「クライアント設定のエクスポート」を参照してください。
- がまだ有効CRLであること。詳細については、「 AWS Client VPN 管理者ガイド」の「クライアントがクライアントVPNエンドポイントに接続できない」を参照してください。

クライアントがTAP「Windows アダプターなし」というログメッセージで接続できない

問題

AWS 提供されたクライアントはクライアントVPNエンドポイントに接続できず、アプリケーションログに「このシステムには TAP-Windows アダプターがありません。Start TAP-> All Programs

-> -Windows -> Utilities TAP-> Add a new -Windows virtual ethernet Adapter" に移動して、TAP-Windows アダプターを作成できるはずです。

ソリューション

この問題は、次の 1 つまたは複数のアクションを実行することで解決できます。

- TAP-Windows アダプターを再起動します。
- TAP-Windows ドライバーを再インストールします。
- 新しい TAP-Windows アダプターを作成します。

クライアントが再接続状態でスタックしている

問題

AWS 提供されたクライアントはクライアントVPNエンドポイントに接続しようとしていますが、再接続状態でスタックしています。

原因

この問題の原因として、次のいずれかが考えられます。

- コンピュータがインターネットに接続されていません。
- DNS ホスト名は IP アドレスに解決されません。
- OpenVPN プロセスは、エンドポイントへの接続を無期限に試行しています。

ソリューション

コンピュータがインターネットに接続されていることを確認します。クライアントVPN管理者に依頼して、設定ファイル内の `remote` ディレクティブが有効な IP アドレスに解決されていることを確認します。クライアントウィンドウで切断を選択してVPNセッションを AWS VPN切断し、再度接続を試みることもできます。

VPN 接続プロセスが予期せず終了する

問題

クライアントVPNエンドポイントへの接続中に、クライアントは予期せず終了します。

原因

TAP- Windows がコンピュータにインストールされていません。このソフトウェアは、クライアントを実行するために必要です。

ソリューション

AWS 提供されたクライアントインストーラーを再実行して、必要な依存関係をすべてインストールします。

アプリケーションが起動しない

問題

Windows 7 では、 AWS 提供のクライアントは、開こうとすると起動しません。

原因

。NET Framework 4.7.2 以降はコンピュータにインストールされません。これは、クライアントを実行するために必要です。

ソリューション

AWS 提供されたクライアントインストーラーを再実行して、必要な依存関係をすべてインストールします。

クライアントがプロファイルを作成できない

問題

AWS が提供するクライアントを使用してプロファイルを作成しようとすると、次のエラーが表示されます。

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

原因

クライアントVPNエンドポイントが相互認証を使用する場合、設定 (.ovpn) ファイルにはクライアント証明書とキーが含まれません。

ソリューション

クライアントVPN管理者がクライアント証明書とキーを設定ファイルに追加していることを確認します。詳細については、AWS Client VPN 管理者ガイドの「クライアント設定のエクスポート」を参照してください。

Windows 10 または 11 PCsを使用して Dell でクライアントクラッシュが発生する

問題

Windows 10 または 11 を実行している特定の Dell PCs (デスクトップおよびラップトップ) では、ファイルシステムを参照してVPN設定ファイルをインポートするときにクラッシュが発生する可能性があります。この問題が発生すると、 AWS 提供されたクライアントのログに次のようなメッセージが表示されます。

```
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()
```

原因

Windows 10 および 11 の Dell Backup and Recovery システムは、 AWS 提供されたクライアント、特に次の 3 つの と競合する可能性がありますDLLs。

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

ソリューション

この問題を回避するには、まずクライアントが AWS 提供されているクライアントの最新バージョンで最新であることを確認します。AWS クライアントVPNのダウンロードに移動し、新しいバージョンが利用可能な場合は、最新バージョンにアップグレードします。

さらに、次のいずれかの操作を行います。

- Dell Backup and Recovery アプリケーションを使用している場合は、最新であることを確認してください。Dell のフォーラムの投稿によると、この問題は新しいバージョンのアプリケーションで解決されています。
- Dell Backup and Recovery アプリケーションを使用していない場合は、この問題が発生した場合でも、何らかのアクションを実行する必要があります。アプリケーションをアップグレードしない場合は、代わりにDLLファイルを削除または名前を変更できます。ただし、これにより、Dell Backup and Recovery アプリケーションが完全に機能しなくなります。

DLL ファイルの削除または名前の変更

1. Windows Explorer に移動し、Dell Backup and Recovery がインストールされている場所を参照します。通常、次の場所にインストールされますが、検索して見つける必要がある場合があります。

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

2. インストールディレクトリから次のDLLファイルを手動で削除するか、名前を変更します。どちらのアクションも、ロードされることを防ぎます。

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

   ファイルの名前を変更するには、ファイル名の末尾に「.bak」を追加します。例えば、DBROverlayIconBackuped.dll.bak です。

VPN ポップアップメッセージで切断する

問題

は、「デバイスが接続されているローカルネットワークのアドレス空間が変更されているため VPN、接続が終了しています。」というポップアップメッセージでVPN切断されます。新しいVPN接続を確立してください。」

原因

TAP- Windows アダプターに必要な説明が含まれていません。

ソリューション

Description 以下のフィールドが一致しない場合は、まず TAP-Windows アダプターを削除してから、 AWS 提供されたクライアントインストーラーを再実行して、必要な依存関係をすべてインストールします。

```
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
```

オープンVPN GUI

次のトラブルシューティング情報は、Windows 10 Home (64 ビット) および Windows Server 2016 (64 ビット) の OpenVPN GUIソフトウェアのバージョン 11.10.0.0 および 11.11.0.0 でテストされました。

設定ファイルは、コンピュータ上の次の場所に保存されます。

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

接続ログは、コンピュータ上の次の場所に保存されます。

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

接続VPNクライアントを開く

次のトラブルシューティング情報は、Windows 10 Home (64 ビット) および Windows Server 2016 (64 ビット) の OpenVPN Connect Client ソフトウェアのバージョン 2.6.0.100 および 2.7.1.101 でテストされました。

設定ファイルは、コンピュータ上の次の場所に保存されます。

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

接続ログは、コンピュータ上の次の場所に保存されます。

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

解決できません DNS

問題

接続が次のエラーで失敗します。

```
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.
```

原因

DNS 名前を解決できません。キャッシュを防ぐために、クライアントはDNS名前にランダムDNSな文字列を付加する必要があります。ただし、一部のクライアントはそうしません。

ソリューション

AWS Client VPN 管理者ガイドの「クライアントVPNエンドポイントDNS名を解決できない」の解決策を参照してください。

PKI エイリアスがありません

問題

相互認証を使用しないクライアントVPNエンドポイントへの接続は、次のエラーで失敗します。

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

原因

OpenVPN Connect Client ソフトウェアには、相互認証を使用して認証を試みるという既知の問題があります。設定ファイルにクライアントキーと証明書が含まれていない場合、認証は失敗します。

ソリューション

クライアントVPN設定ファイルにランダムなクライアントキーと証明書を指定し、新しい設定を OpenVPN Connect Client ソフトウェアにインポートします。または、Open VPNクライアント (v11.12.0.0) や Viscosity GUIクライアント (v.1.7.14) などの別のクライアントを使用します。

macOS クライアントとのクライアントVPN接続のトラブルシューティング

以下のセクションでは、macOS クライアントを使用する際のログと、発生する可能性のある問題について説明します。これらのクライアントの最新バージョンを実行していることを確認します。

トピック

AWS が提供するクライアント

AWS が提供するクライアントは、イベントログを作成し、コンピュータ上の次の場所に保存します。

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

次のタイプのログを使用できます。

- アプリケーションログ: アプリケーションに関する情報が含まれます。これらのログには「aws_vpn_client_」が前に付けられます。
- オープンVPNログ： オープンVPNプロセスに関する情報が含まれます。これらのログには「ovpn_aws_vpn_client_」が前に付けられます。

AWS 提供されたクライアントは、クライアントデーモンを使用してルートオペレーションを実行します。デーモンログは、コンピュータ上の次の場所に保存されます。

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

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

AWS 提供されたクライアントは、コンピュータ上の次の場所に設定ファイルを保存します。

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

トピック

クライアントが接続できない

問題

AWS 提供されたクライアントは、クライアントVPNエンドポイントに接続できません。

原因

この問題の原因として、次のいずれかが考えられます。

- 別の Open VPNプロセスが既にコンピュータで実行されているため、クライアントは接続できません。
- 設定 (.ovpn) ファイルが有効ではありません。

ソリューション

コンピュータで実行されている他の Open VPNアプリケーションがあるかどうかを確認します。存在する場合は、これらのプロセスを停止または終了し、クライアントVPNエンドポイントへの接続を再試行してください。オープンVPNログにエラーがないか確認し、クライアントVPN管理者に次の情報を確認するよう依頼します。

- 設定ファイルに、正しいクライアントキーと証明書が含まれている。詳細については、AWS Client VPN 管理者ガイドの「クライアント設定のエクスポート」を参照してください。
- がまだ有効CRLであること。詳細については、「 AWS Client VPN 管理者ガイド」の「クライアントがクライアントVPNエンドポイントに接続できない」を参照してください。

クライアントが再接続状態でスタックしている

問題

AWS 提供されたクライアントはクライアントVPNエンドポイントに接続しようとしていますが、再接続状態でスタックしています。

原因

この問題の原因として、次のいずれかが考えられます。

- コンピュータがインターネットに接続されていません。
- DNS ホスト名は IP アドレスに解決されません。
- OpenVPN プロセスは、エンドポイントへの接続を無期限に試行しています。

ソリューション

コンピュータがインターネットに接続されていることを確認します。クライアントVPN管理者に依頼して、設定ファイル内の `remote` ディレクティブが有効な IP アドレスに解決されていることを確認します。クライアントウィンドウで切断を選択してVPNセッションを AWS VPN切断し、再度接続を試みることもできます。

クライアントがプロファイルを作成できない

問題

AWS が提供するクライアントを使用してプロファイルを作成しようとすると、次のエラーが表示されます。

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

原因

クライアントVPNエンドポイントが相互認証を使用する場合、設定 (.ovpn) ファイルにはクライアント証明書とキーが含まれません。

ソリューション

クライアントVPN管理者がクライアント証明書とキーを設定ファイルに追加していることを確認します。詳細については、AWS Client VPN 管理者ガイドの「クライアント設定のエクスポート」を参照してください。

ヘルパーツールは必須ですエラー

問題

に接続しようとすると、次のエラーが表示されますVPN。

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

ソリューション

AWS re:Post に関する次の記事を参照してください。AWS VPN クライアント - ヘルパーツールは必須ですエラー

Tunnelblick

以下のトラブルシューティング情報は、macOS High Sierra 10.13.6 の Tunnelblick ソフトウェアのバージョン 3.7.8 (ビルド 5180) でテストされました。

プライベート設定の設定ファイルは、コンピュータ上の次の場所に保存されます。

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

共有設定の設定ファイルは、コンピュータ上の次の場所に保存されます。

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

接続ログは、コンピュータ上の次の場所に保存されます。

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

ログの詳細度を上げるには、Tunnelblick アプリケーションを開き、設定 を選択し、VPNログレベルの値を調整します。

暗号アルゴリズム 'AES-256-GCM' が見つかりません

問題

接続が失敗し、ログに次のエラーが返されます。

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

原因

アプリケーションは、暗号アルゴリズム AES-256- をサポートしていない OpenVPN バージョンを使用していますGCM。

ソリューション

以下を実行して、互換性のある Open VPNバージョンを選択します。

1. Tunnelblick アプリケーションを開きます。
2. [設定] を選択します。
3. オープンVPNバージョン で、2.4.6 を選択します。オープンSSLバージョンは v1.0.2q です。

接続が応答を停止し、リセットされます。

問題

接続が失敗し、ログに次のエラーが返されます。

```
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
```

原因

クライアント証明書が失効しました。認証を試みた後に接続が応答を停止し、最終的にサーバー側でリセットされます。

ソリューション

クライアントVPN管理者に新しい設定ファイルをリクエストします。

拡張キーの使用 (EKU)

問題

接続が失敗し、ログに次のエラーが返されます。

```
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,,,,,
```

原因

サーバー認証に成功しました。ただし、クライアント証明書でサーバー認証用に拡張キー使用法 (EKU) フィールドが有効になっているため、クライアント認証は失敗します。

ソリューション

正しいクライアント証明書とキーを使用していることを確認します。必要に応じて、クライアントVPN管理者に確認してください。このエラーは、クライアント証明書ではなくサーバー証明書を使用してクライアントVPNエンドポイントに接続する場合に発生する可能性があります。

証明書が失効している

問題

サーバー認証は成功しますが、クライアント認証は次のエラーで失敗します。

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

原因

クライアント証明書の有効期限が切れています。

ソリューション

クライアントVPN管理者に新しいクライアント証明書をリクエストします。

オープンVPN

次のトラブルシューティング情報は、macOS High Sierra 10.13.6 の OpenVPN Connect Client ソフトウェアのバージョン 2.7.1.100 でテストされました。

設定ファイルは、コンピュータ上の次の場所に保存されます。

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

接続ログは、コンピュータ上の次の場所に保存されます。

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

解決できない DNS

問題

接続が次のエラーで失敗します。

```
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
```

原因

OpenVPN Connect はクライアントVPNDNS名を解決できません。

ソリューション

AWS Client VPN 管理者ガイドの「クライアントVPNエンドポイントDNS名を解決できない」の解決策を参照してください。

Linux ベースのクライアントとのクライアントVPN接続のトラブルシューティング

次のセクションでは、ログに関する情報と、Linux ベースのクライアントを使用する際に発生する可能性のある問題について説明します。これらのクライアントの最新バージョンを実行していることを確認します。

トピック

- AWS が提供するクライアント
- OpenVPN (コマンドライン)
- Network Manager で VPNを開く (GUI)

AWS が提供するクライアント

AWS が提供するクライアントは、ログファイルと設定ファイルをシステム上の次の場所に保存します。

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

AWS が提供するクライアントデーモンプロセスは、ログファイルをシステム上の次の場所に保存します。

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

問題

VPN 接続が確立された後でも、クライアントVPNエンドポイントに設定されたネームサーバーではなく、デフォルトのシステムネームサーバーにDNSクエリが送られる場合があります。

原因

クライアントは、Linux システムで利用可能なサービスである systemd-resolved とやり取りします。これは、一元的なDNS管理として機能します。これは、クライアントVPNエンドポイントから

プッシュされるDNSサーバーを設定するために使用されます。この問題は、systemd-resolved がクライアントVPNエンドポイントによって提供されるDNSサーバーに最も高い優先度を設定していないために発生します。代わりに、ローカルシステムで設定されているサーバーの既存のリストにDNSサーバーを追加します。その結果、元のDNSサーバーが依然として最も優先度が高いため、DNSクエリの解決に使用される可能性があります。

ソリューション

1. Open VPNconfig ファイルの最初の行に次のディレクティブを追加して、すべてのDNSクエリがVPNトンネルに送信されていることを確認します。

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

2. systemd-resolved で提供されるスタブリゾルバーを使用する。これを行うには、システム上で次のコマンドを実行することによって、`/etc/resolv.conf` から `/run/systemd/resolve/stub-resolv.conf` へのシンボリックリンクを設定します。

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

3. （オプション) systemd-resolved でDNSクエリをプロキシせず、代わりにクエリを実際のDNSネームサーバーに直接送信する場合は、`/run/systemd/resolve/resolv.conf`代わりに にシンボリックリンク`/etc/resolv.conf`します。

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

   この手順は、DNS応答キャッシュ、インターフェイスごとの設定、DNSSec強制など、systemd-resolved DNS設定をバイパスするために実行できます。このオプションは、 に接続されているときにパブリックDNSレコードをプライベートレコードで上書きする必要がある場合に特に便利ですVPN。例えば、 のレコードVPCを持つプライベートリDNSゾルバーがプライベート IP に解決 www.example.com されている場合があります。このオプションを使用すると、パブリック IP に解決される www.example.com のパブリックレコードを上書きできます。

OpenVPN (コマンドライン)

問題

DNS 解決が機能していないため、接続が正しく機能しません。

原因

DNS サーバーがクライアントVPNエンドポイントで設定されていないか、クライアントソフトウェアによって受け入れられていません。

ソリューション

以下のステップを使用して、DNSサーバーが正しく設定され、動作していることを確認します。

1. ログにDNSサーバーエントリが存在することを確認します。次の例では、DNSサーバー 192.168.0.2 (クライアントVPNエンドポイントで設定) が最後の行で返されます。

   ```
   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
   ```

   DNS サーバーが指定されていない場合は、クライアントVPN管理者にクライアントVPNエンドポイントの変更を依頼し、クライアントVPNエンドポイントにDNSサーバー (VPCDNSサーバーなど) が指定されていることを確認します。詳細については、「 AWS Client VPN 管理者ガイド」の「クライアントVPNエンドポイント」を参照してください。
2. 次のコマンドを実行して、resolvconf パッケージがインストールされていることを確認します。

   ```
   sudo apt list resolvconf
   ```

   出力は、以下を返します。

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

   インストールされていない場合は、次のコマンドを使用してインストールします。

   ```
   sudo apt install resolvconf
   ```
3. テキストエディタでクライアントVPN設定ファイル (.ovpn ファイル) を開き、次の行を追加します。

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

```
down /etc/openvpn/update-resolv-conf
```

ログをチェックして、resolvconf スクリプトが呼び出されたことを確認します。ログには、次のような行が含まれている必要があります。

```
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
```

Network Manager で VPNを開く (GUI)

問題

Network Manager OpenVPN クライアントを使用する場合、接続は次のエラーで失敗します。

```
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
```

原因

remote-random-hostname フラグは受け入れられず、クライアントは network-manager-gnome パッケージを使用して接続できません。

ソリューション

AWS Client VPN 管理者ガイドの「クライアントVPNエンドポイントDNS名を解決できない」の解決策を参照してください。

クライアントの一般的なVPN問題のトラブルシューティング

以下は、クライアントを使用してクライアントVPNエンドポイントに接続するときに発生する可能性がある一般的な問題です。

TLS キーネゴシエーションに失敗しました

問題

TLS ネゴシエーションは、次のエラーで失敗します。

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

原因

この問題の原因として、次のいずれかが考えられます。

- ファイアウォールルールが UDPまたは TCPトラフィックをブロックしています。
- 設定 (.ovpn) ファイルで間違ったクライアントキーと証明書を使用しています。
- クライアント証明書失効リスト (CRL) の有効期限が切れています。

ソリューション

コンピュータのファイアウォールルールが、ポート 443 または 1194 のインバウンドTCP、アウトバウンド、またはUDPトラフィックをブロックしているかどうかを確認します。クライアントVPN管理者に依頼して、次の情報を確認します。

- クライアントVPNエンドポイントのファイアウォールルールが、ポート 443 TCPまたは 1194 のまたは UDPトラフィックをブロックしないこと。
- 設定ファイルに、正しいクライアントキーと証明書が含まれている。詳細については、AWS Client VPN 管理者ガイドの「クライアント設定のエクスポート」を参照してください。
- がまだ有効CRLであること。詳細については、「 AWS Client VPN 管理者ガイド」の「クライアントがクライアントVPNエンドポイントに接続できない」を参照してください。

ドキュメント履歴

次の表は、 AWS クライアントVPNユーザーガイドの更新を示しています。

変更	説明	日付
AWS が提供する Ubuntu 向けクライアント (3.15.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 8 月 12 日
AWS が提供する Windows 向けクライアント (3.14.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 8 月 12 日
AWS が提供する macOS 用クライアント (3.12.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 8 月 12 日
AWS が提供する Ubuntu 向けクライアント (3.14.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 7 月 29 日
AWS が提供する Windows 向けクライアント (3.13.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 7 月 29 日
AWS が提供する macOS 向けクライアント (3.11.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 7 月 29 日
AWS が提供する Windows 向けクライアント (3.12.1) をリリース	詳細については、リリースノートを参照してください。	2024 年 7 月 18 日
AWS が提供する Ubuntu 向けクライアント (3.13.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 5 月 21 日

AWS が提供する Windows 向けクライアント (3.12.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 5 月 21 日
AWS が提供する macOS 向けクライアント (3.10.0) をリリース	詳細については、リリースノートを参照してください。	2024 年 5 月 21 日
AWS が提供する macOS 向けクライアント (3.9.2) をリリース	詳細については、リリースノートを参照してください。	2024 年 4 月 11 日
AWS が提供する Ubuntu 向けクライアント (3.12.2) をリリース	詳細については、リリースノートを参照してください。	2024 年 4 月 11 日
AWS が提供する Windows 用クライアント (3.11.2) をリリース	詳細については、リリースノートを参照してください。	2024 年 4 月 11 日
AWS が提供する macOS 用クライアント (3.9.1) をリリース	詳細については、リリースノートを参照してください。	2024 年 2 月 16 日
AWS が提供する Ubuntu 向けクライアント (3.12.1) をリリース	詳細については、リリースノートを参照してください。	2024 年 2 月 16 日
AWS が提供する Windows 用クライアント (3.11.1) をリリース	詳細については、リリースノートを参照してください。	2024 年 2 月 16 日
AWS が提供する Ubuntu 向けクライアント (3.12.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 12 月 19 日
AWS が提供する macOS 向けクライアント (3.9.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 12 月 6 日

AWS が提供する Windows 向けクライアント (3.11.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 12 月 6 日
AWS が提供する Ubuntu 向けクライアント (3.11.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 12 月 6 日
AWS が提供する Ubuntu 向けクライアント (3.10.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 12 月 6 日
AWS が提供する Ubuntu 向けクライアント (3.9.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 24 日
AWS が提供する macOS 向けクライアント (3.8.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 24 日
AWS が提供する Windows 用クライアント (3.10.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 24 日
AWS が提供する Windows 向けクライアント (3.9.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 3 日
AWS が提供する Ubuntu 向けクライアント (3.8.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 3 日
AWS が提供する macOS 向けクライアント (3.7.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 8 月 3 日
AWS が提供する Windows 用クライアント (3.8.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日

AWS が提供する Windows 向けクライアント (3.7.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日
AWS が提供する Ubuntu 向けクライアント (3.7.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日
AWS が提供する macOS 用クライアント (3.6.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日
AWS が提供する Ubuntu 向けクライアント (3.6.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日
AWS が提供する macOS 用クライアント (3.5.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 15 日
AWS が提供する Windows 向けクライアント (3.6.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 14 日
AWS が提供する Ubuntu 向けクライアント (3.5.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 14 日
AWS が提供する macOS 向けクライアント (3.4.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 7 月 14 日
AWS が提供する macOS 用クライアント (3.3.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 4 月 27 日
AWS が提供する Windows 向けクライアント (3.5.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 4 月 3 日

AWS が提供する Windows 用クライアント (3.4.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 3 月 28 日
AWS が提供する Windows 用クライアント (3.3.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 3 月 17 日
AWS が提供する Ubuntu 向けクライアント (3.4.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 2 月 14 日
AWS が提供する macOS 向けクライアント (3.2.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 1 月 23 日
AWS が提供する Windows 向けクライアント (3.2.0) をリリース	詳細については、リリースノートを参照してください。	2023 年 1 月 23 日
AWS が提供する macOS 向けクライアント (3.1.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 5 月 23 日
AWS が提供する Windows 向けクライアント (3.1.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 5 月 23 日
AWS が提供する Ubuntu 向けクライアント (3.1.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 5 月 23 日
AWS が提供する macOS 用クライアント (3.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 3 月 3 日
AWS が提供する Windows 向けクライアント (3.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 3 月 3 日

AWS が提供する Ubuntu 向けクライアント (3.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 3 月 3 日
AWS が提供する macOS 向けクライアント (2.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 1 月 20 日
AWS が提供する Windows 向けクライアント (2.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 1 月 20 日
AWS が提供する Ubuntu 向けクライアント (2.0.0) をリリース	詳細については、リリースノートを参照してください。	2022 年 1 月 20 日
AWS が提供する macOS 向けクライアント (1.4.0) をリリース	詳細については、リリースノートを参照してください。	2021 年 11 月 9 日
AWS が提供する Windows 用クライアント (1.3.7) がリリースされました	詳細については、リリースノートを参照してください。	2021 年 11 月 8 日
AWS が提供する Ubuntu 向けクライアント (1.0.3) をリリース	詳細については、リリースノートを参照してください。	2021 年 11 月 8 日
AWS が提供する Ubuntu 向けクライアント (1.0.2) をリリース	詳細については、リリースノートを参照してください。	2021 年 9 月 28 日
AWS が提供する Windows (1.3.6) および macOS (1.3.5) 用のクライアントをリリース	詳細については、リリースノートを参照してください。	2021 年 9 月 20 日

AWS が提供する Ubuntu 18.04 LTSおよび Ubuntu 20.04 用のクライアントがLTSリリースされました	AWSが提供するクライアントは、Ubuntu 18.04 LTSおよびUbuntu 20.04 で使用できます。 LTS	2021 年 6 月 11 日
Windows Certificate System Store の証明書を使用した OpenVPN のサポート	Windows Certificate System Store の証明書で OpenVPN を使用できます。	2021 年 2 月 25 日
セルフサービスポータル	セルフサービスポータルにアクセスして、 AWS 提供された最新のクライアントと設定ファイルを取得できます。	2020 年 10 月 29 日
AWS が提供するクライアント	AWS が提供するクライアントを使用して、クライアントVPNエンドポイントに接続できます。	2020 年 2 月 4 日
初回リリース	このリリースでは、 AWS クライアント が導入されていますVPN。	2018 年 12 月 18 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。