AWS クライアント VPN

ユーザーガイド

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 VPN とは

AWS クライアント VPN は、AWS リソースやオンプレミスネットワーク内のリソースに安全にアクセスできるようにする、クライアントベースのマネージド 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 エンドポイントへの VPN 接続を確立する手順について説明します。

コンポーネント

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

- クライアント VPN エンドポイント — クライアント VPN 管理者が AWS でクライアント VPN エンドポイントを作成および設定します。管理者は VPN 接続を確立するときに、どのネットワークやリソースへのアクセスを可能とするかを管理します。
- 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、セキュアな 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。このファイルには、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。選択した VPN クライアントアプリケーションに、このファイルをロードします。

その他のリソース

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および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。

クライアント VPN の開始方法

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 セッションを確立するときに、どのネットワークやリソースへのアクセスを可能とするかを管理します。その後、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。

Client VPN エンドポイントの作成が必要な管理者の場合は、AWS Client VPN 管理者ガイドを参照して下さい。

トピック

Prerequisites

VPN 接続を確立するには、以下のものが必要です。

- 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は、以下のいずれかのブラウザを使用します。
  - 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 が提供するクライアントまたは別の OpenVPN ベースのクライアントアプリケーションを使用して VPN 接続を確立することができます。

AWS が提供するクライアントは、Windows、macOS、Ubuntu 18.04 LTS、および Ubuntu 20.04 LTS でサポートされています。AWS クライアント VPN のダウンロードでクライアントをダウンロードできます。

または、VPN 接続を確立するデバイス上に、OpenVPN 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

クライアント VPN エンドポイント設定ファイルを管理者から取得する必要があります。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 エンドポイント用のセルフサービスポータルを構成している場合は、AWS が提供す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、「」を参照してくださいセルフサービスポータルの使用 (p. 3)

ステップ 3: VPN に接続する

クライアント VPN エンドポイント設定ファイルを AWS 提供のクライアントまたは OpenVPN クライアントアプリケーションにインポートして VPN に接続します。VPN に接続するステップについては、次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接続する (p. 5)
- OpenVPN クライアントを使用して接続する (p. 18)

Active Directory 認証を使用するクライアント VPN エンドポイントでは、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、AWS が提供するクライアントは、お使いの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、企業の認証情報の入力を求められます。

セルフサービスポータルの使用

クライアント VPN エンドポイント管理者は、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できます。セルフサービスポータルは、AWS 提供の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。セルフサービスポータルの設定の詳細については、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。

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。ID は、クライアント VPN エンドポイント管理者から提供してもらうことができます。ID を含むセルフサービスポータル URL が提供されることもあります。

セルフサービスポータルにアクセスするには

1. セルフサービスポータル (https://self-service.clientvpn.amazonaws.com/) にアクセスするか、管理者から提供された URL を使用します。
2. 必要に応じて、クライアント VPN エンドポイントの ID (たとえば、`cvpn-endpoint-0123456abcd123456`) を入力します。[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 エンドポイントに接続するため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 エンドポイント用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の AWS 提供の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接続する

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

クライアント

- AWS Client VPN for Windows (p. 6)
- AWS Client VPN for macOS (p. 8)
- Linux の AWS Client VPN (p. 9)
- AWS が提供するクライアントのリリースノート (p. 13)

OpenVPN 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-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- cryptoapicert (Windows のみ)
- dev
- key
- nobind
- persist-key
- persist-tun
- proto
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb

AWS Client VPN for Windows

次の手順は、AWS が提供する Windows 用クライアントを使用して VPN 接続を確立する方法を示しています。AWS クライアント VPN のダウンロードで、クライアントを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。

目次

Requirements

AWS 提供の Windows 用クライアントを使用するには、次のものが必要です。

- Windows 10 64 ビットオペレーティングシステム、x64 プロセッサ
- .NET Framework 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、クライアントでは TCP ポート 35001 を予約します。

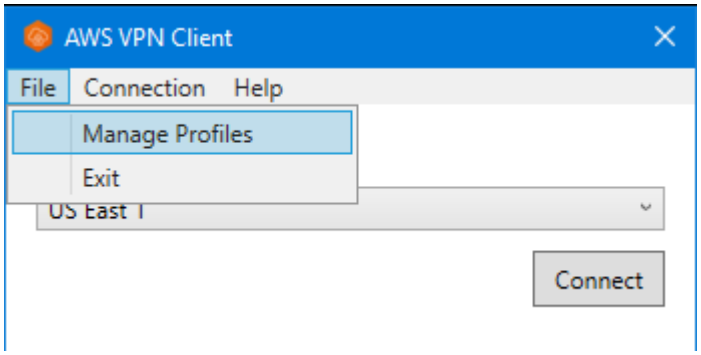
開始する前に、クライアント VPN 管理者がクライアント VPN エンドポイントを作成し、クライアント VPN エンドポイント設定ファイルを提供済みであることを確認します。

Connecting

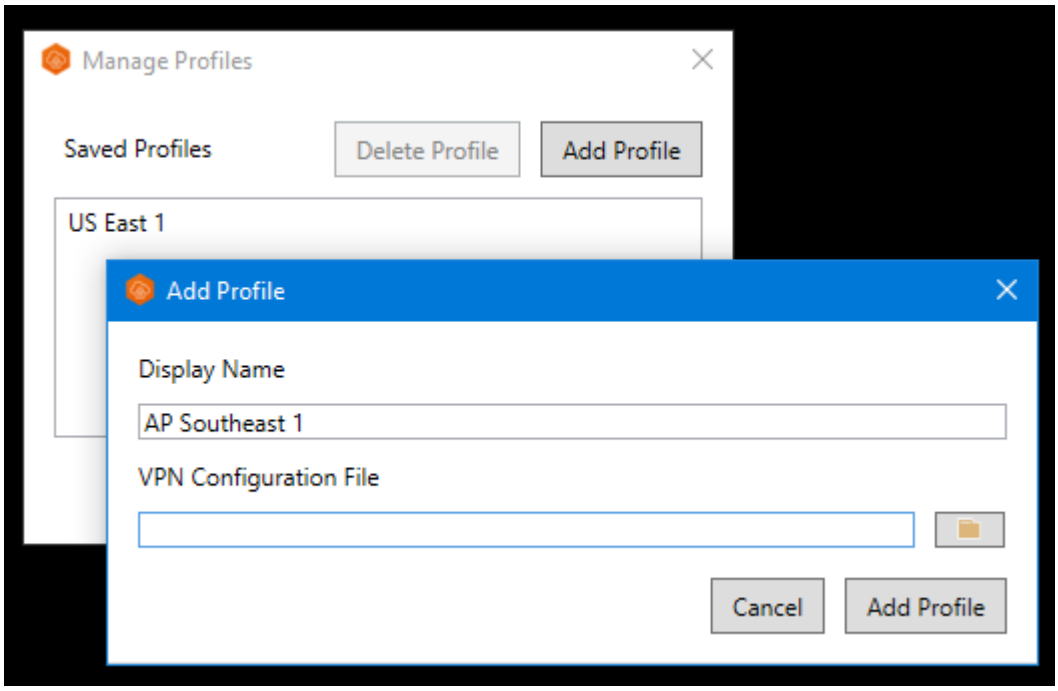
開始する前に、必ず「要件 (p. 6)」を参照してください。以下のステップでは、AWS 提供のクライアントは AWS VPN クライアントとも呼ばれます。

AWS 提供の Windows 用クライアントを使用して接続するには

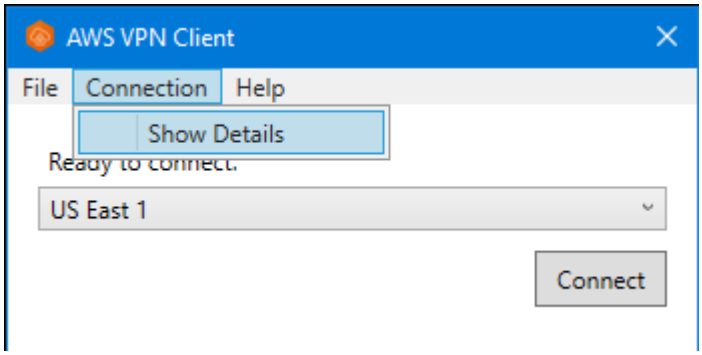
1. AWS VPN クライアントアプリケーションを開きます。
2. [File (ファイル)]、[Manage Profiles (プロファイルの管理)] の順に選択します。



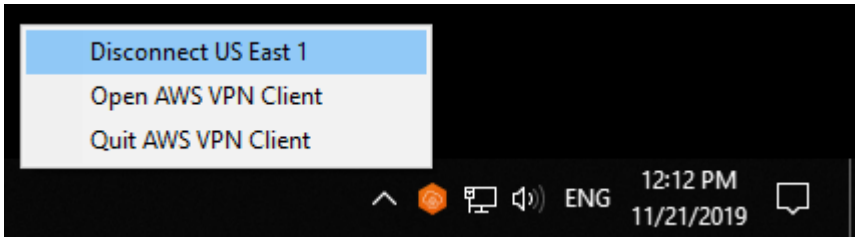
3. [Add Profile (プロファイルの追加)] を選択します。



4. [Display Name (表示名)] に、プロファイルの名前を入力します。
5. [VPN Configuration File (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、[Add Profile (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を入力するように求められます。
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。



リリースノート

Windows 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およびダウンロードリンクについては、Windows のリリースノート (p. 13) を参照してください。

AWS Client VPN for macOS

次の手順は、AWS が提供する macOS 用クライアントを使用して VPN 接続を確立する方法を示しています。AWS クライアント VPN のダウンロードで、クライアントを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。

目次

Requirements

AWS 提供の macOS 用クライアントを使用するには、次のものが必要です。

- 64 ビットの macOS Mojave (10.14)、Catalina (10.15)、Big Sur (11.0)

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、クライアントでは TCP ポート 35001 を予約します。

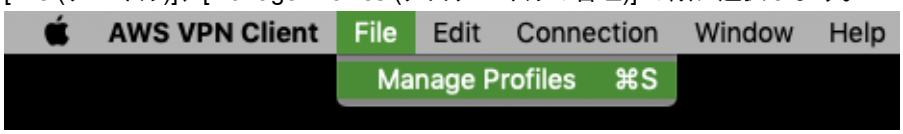
開始する前に、クライアント VPN 管理者がクライアント VPN エンドポイントを作成し、クライアント VPN エンドポイント設定ファイルを提供済みであることを確認します。

Connecting

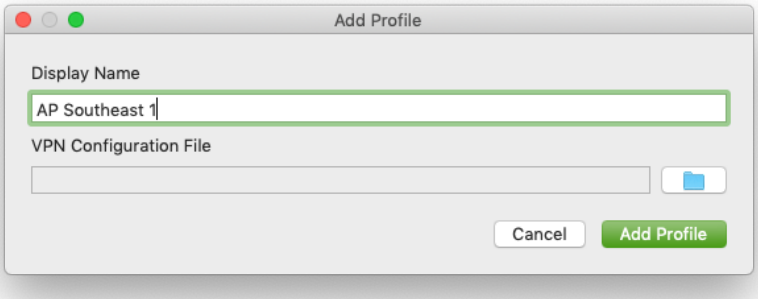
開始する前に、必ず「要件 (p. 8)」を参照してください。以下のステップでは、AWS 提供のクライアントは AWS VPN クライアントとも呼ばれます。

AWS 提供の 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。

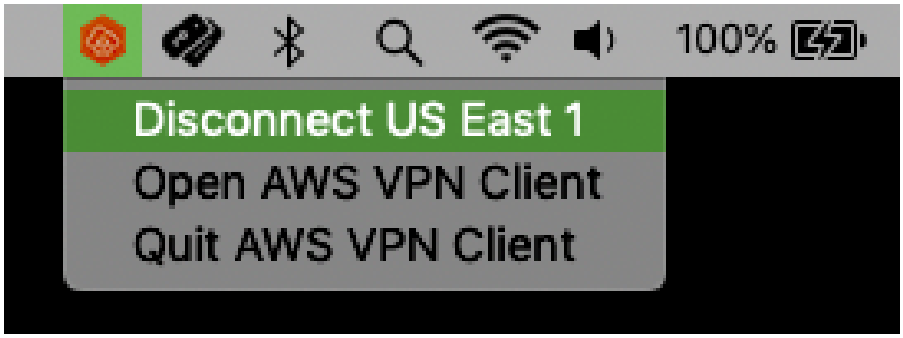


3. [Add Profile (プロファイルの追加)] を選択します。
4. [Display Name (表示名)] に、プロファイルの名前を入力します。



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を入力するように求められます。
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、メニューバーでクライアントアイコンを選択し、[<プロファイル名> の切断] を選択します。



リリースノート

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およびダウンロードリンクについては、macOS のリリースノート (p. 15) を参照してください。

Linux の AWS Client VPN

次の手順は、AWS 提供の Linux 用クライアントをインストールし、AWS 提供のクライアントを使用して VPN 接続を確立する方法を示しています。AWS 提供の Linux 用クライアントは、自動更新をサポートしていません。

目次

Requirements

AWS 提供の Linux 用クライアントを使用するには、次のものが必要です。

- 64 bit Ubuntu 18.04 LTS または 64 bit Ubuntu 20.04 LTS

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、クライアントでは 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済みであることを確認します。

Installation

AWS 提供の Linux 用クライアントをインストールするには、複数の方法があります。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 (p. 10)」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インストールする

1. Ubuntu OS に AWS VPN クライアントのパブリックキーを追加します。

```
wget -q -O - https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo/
awsvpnclient_public_key.asc | sudo apt-key add -
```

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、AWS 提供の Linux 用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インストールする

1. .deb ファイルを AWS Client VPN のダウンロード から、または次のコマンドを使用して、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、AWS 提供の Linux 用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

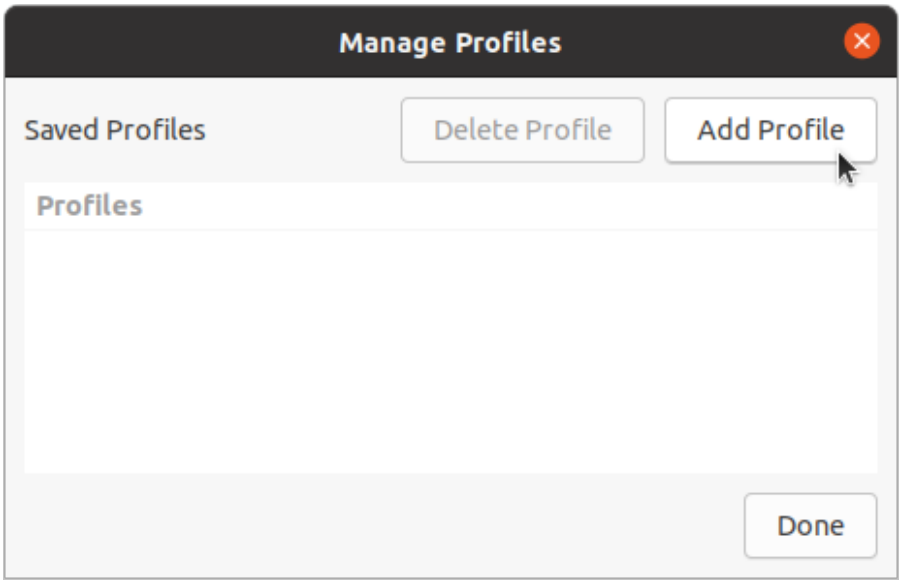
1. .deb パッケージファイルを AWS Client VPN のダウンロード からダウンロードします。
2. .deb パッケージファイルをダウンロードしたら、Ubuntu ソフトウェアセンターを使用してパッケージをインストールします。Ubuntu ソフトウェアセンターを使用してスタンドアロンの .deb パッケージからインストールする手順に従います。詳細については、Ubuntu Wiki を参照してください。

Connecting

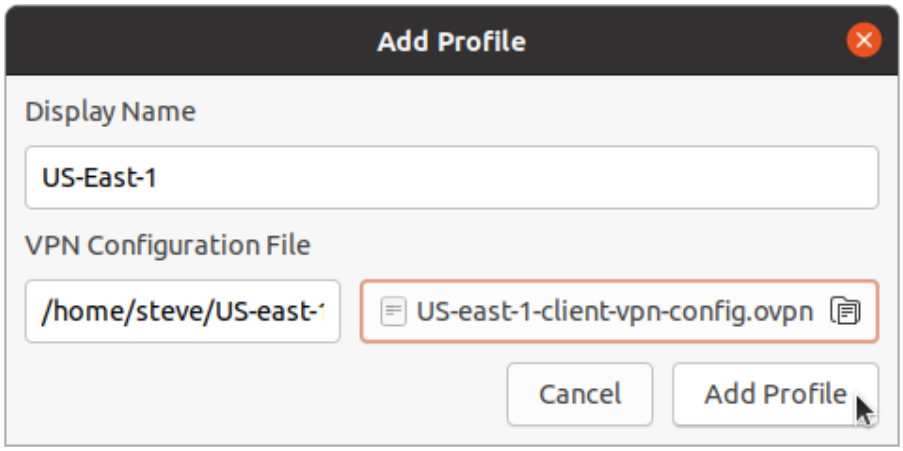
以下のステップでは、AWS 提供のクライアントは AWS VPN クライアントとも呼ばれます。

AWS 提供の Linux 用クライアントを使用して接続するには

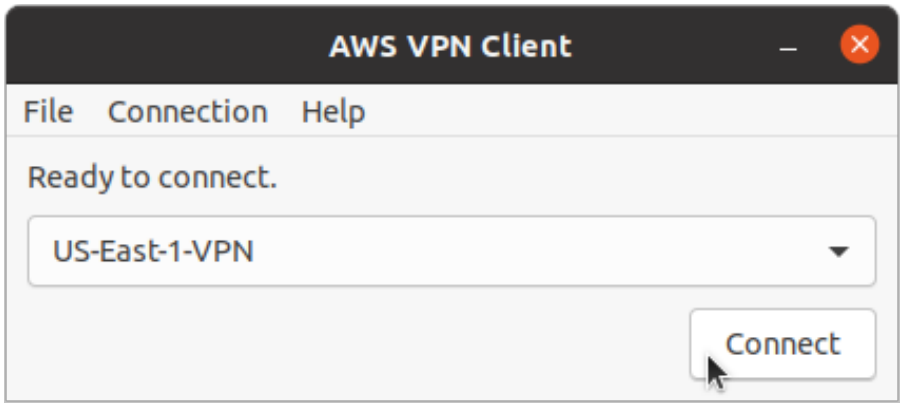
1. AWS VPN クライアントアプリケーションを開きます。
2. [File (ファイル)]、[Manage Profiles (プロファイルの管理)] の順に選択します。
3. [Add Profile (プロファイルの追加)] を選択します。



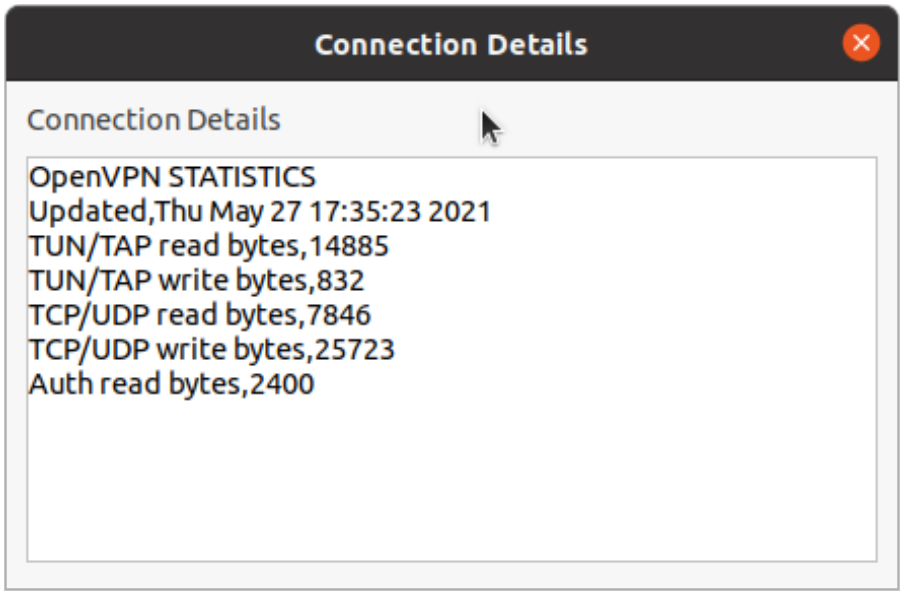
4. [Display Name (表示名)] に、プロファイルの名前を入力します。
5. [VPN 設定ファイル] で、クライアント VPN 管理者から受け取った設定ファイルを参照します。[Open (開く)] を選択します。
6. [Add Profile (プロファイルの追加)] を選択します。



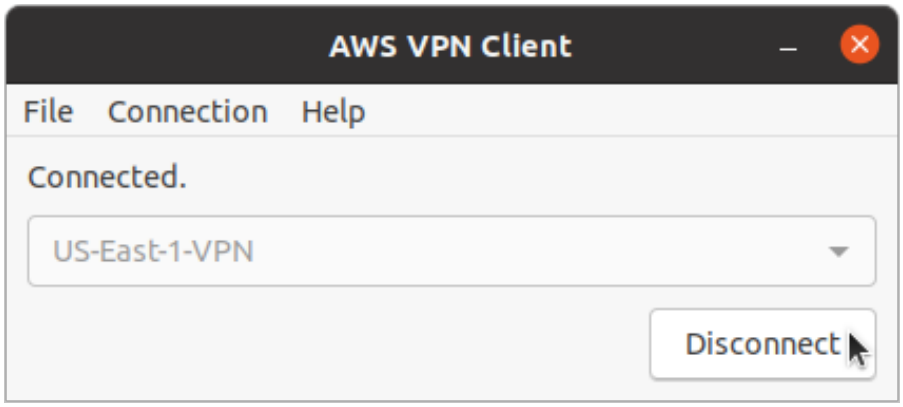
7. [AWS VPN クライアント] ウィンドウで、プロファイルが選択されていることを確認し、[接続] を選択します。クライアント VPN エンドポイントが認証情報ベースの認証を使用するように設定されている場合は、ユーザー名とパスワードを入力するように求められます。



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。



リリースノート

Linux 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およびダウンロードリンクについては、Linux のリリースノート (p. 17) を参照してください。

AWS が提供するクライアントのリリースノート

以下のセクションには、AWS が提供するクライアント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が示されています。

目次

Windows のリリースノート

次の表には、Windows 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が示されています。

バージョン	変更	日付	ダウンロードリンク
1.3.6	• OpenVPN フラグのサポートが追加されました。接続再試行最大、開発タイプ、キープアライブ、ping、ping、再起動、プル、rcvbuf、サーバーポーリングタイムアウト。 • 軽微なバグの修正と機能強化。	2021 年 9 月 20 日	バージョン 1.3.6 をダウンロード
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	バージョン 1.3.5 をダウンロード
1.3.4	• OpenVPN フラグ: dhcp-option 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 8 月 4 日	ダウンロードバージョン 1.3.4

バージョン	変更	日付	ダウンロードリンク
1.3.3	• 次の OpenVPN フラグのサポートが追加されました: inactive、pull-filter、route。 • 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	バージョン 1.3.3 をダウンロード
1.3.2	• IPv6 リーク防止が設定されている場合は、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	ダウンロードバージョン 1.3.2
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」OpenVPN 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	ダウンロードバージョン 1.3.1
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	バージョン 1.3.0 をダウンロード
1.2.7	• cryptoapicert OpenVPN ディレクティブのサポートを追加しました。 • 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	ダウンロードバージョン 1.2.7
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	• OpenVPN 設定のコメントのサポートを追加。 • TLS ハンドシェイクエラーのエラーメッセージを追加。	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。

バージョン	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を追加。 • 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の表示/非表示を切り替える、OpenVPN 静的チャレンジエコー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。

macOS のリリースノート

次の表には、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が示されています。

バージョン	変更	日付	ダウンロードリンク
1.3.5	• OpenVPN フラグのサポートが追加されました。接続再試行最大、開発タイプ、キープアライブ、ping、ping、再起動、プル、rcvbuf、サーバーポーリングタイムアウト。 • 軽微なバグの修正と機能強化。	2021 年 9 月 20 日	バージョン 1.3.5 をダウンロード
1.3.4	• OpenVPN フラグ: dhcp-option 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 8 月 4 日	ダウンロードバージョン 1.3.4
1.3.3	• 次の OpenVPN フラグのサポートが追加されました: inactive、pull-filter、route。 • 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	バージョン 1.3.3 をダウンロード

バージョン	変更	日付	ダウンロードリンク
1.3.2	• IPv6 リーク防止が設定されている場合は、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	ダウンロードバージョン 1.3.2
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で設定された DNS 設定が削除された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」OpenVPN 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	ダウンロードバージョン 1.3.1
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	バージョン 1.3.0 をダウンロード
1.2.5	軽微なバグの修正と機能強化。	2021 年 2 月 25 日	ダウンロードバージョン 1.2.5
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	• OpenVPN 設定のコメントのサポートを追加。 • TLS ハンドシェイクエラーのエラーメッセージを追加。 • 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。
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を追加。 • 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	• DNS が解決されなかった問題を修正。 • 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 の問題を修正。	2020 年 4 月 2 日	サポートは終了しました。

バージョン	変更	日付	ダウンロードリンク
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の表示/非表示を切り替える、OpenVPN 静的チャレンジエコー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。

Linux のリリースノート

次の表には、Linux 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が示されています。

バージョン	変更	日付	ダウンロードリンク
1.0.2	• OpenVPN フラグのサポートが追加されました。接続再試行最大、開発タイプ、キープアライブ、ping、ping、再起動、プル、rcvbuf、サーバーポーリングタイムアウト。 • 軽微なバグの修正と機能強化。	2021 年 9 月 28 日	バージョン 1.0.2 をダウンロード
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。 • 次の OpenVPN フラグのサポートが追加されました: inactive、pull-filter、route。 • 軽微なバグの修正と機能強化。	2021 年 8 月 4 日	ダウンロードバージョン 1.0.1
1.0.0	初回リリース。	2021 年 6 月 11 日	ダウンロードバージョン 1.0.0

OpenVPN クライアントを使用して接続する

共通の Open 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できます。

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接続する (p. 18)
- Android または iOS VPN クライアントアプリケーションを使用して接続する (p. 20)
- macOS クライアントアプリケーションを使用して接続する (p. 21)
- OpenVPN クライアントアプリケーションを使用して接続する (p. 23)

Windows クライアントアプリケーションを使用して接続する

次の手順は、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を示しています。

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済みであることを確認します。

トラブルシューティング情報については、「Windows のトラブルシューティング (p. 25)」を参照してください。

Windows 証明書システムストアの証明書を使用する OpenVPN

Windows 証明書システムストアの証明書と秘密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。OpenVPN クライアント cryptoapicert オプションの詳細については、OpenVPN のウェブサイトの「Reference Manual for OpenVPN」をご参照ください。

> 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。

OpenVPN で cryptoapicert オプションを使用するには

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 のウェブサイトの「方法: MMC スナップインを使用して証明書を表示する」をご参照ください。
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. OpenVPN 設定ファイルを更新し、証明書のサブジェクト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、OpenVPN を使用して接続を確立します。

OpenVPN GUI

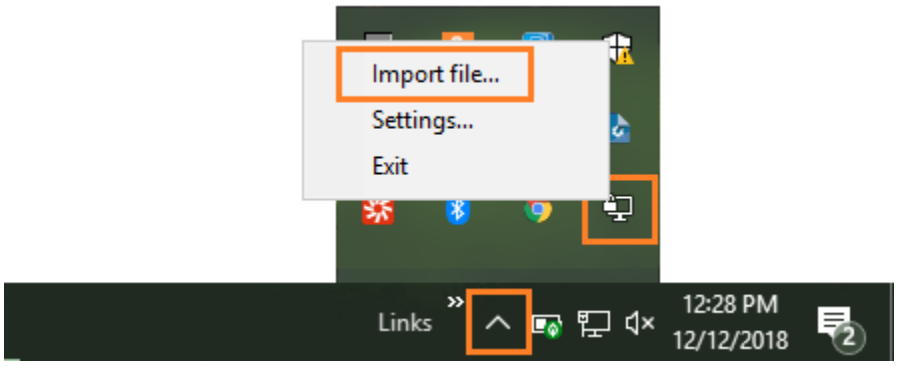
次の手順は、Windows コンピュータで OpenVPN GUI クライアントアプリケーションを使用し、VPN 接続を確立する方法を示します。

Note

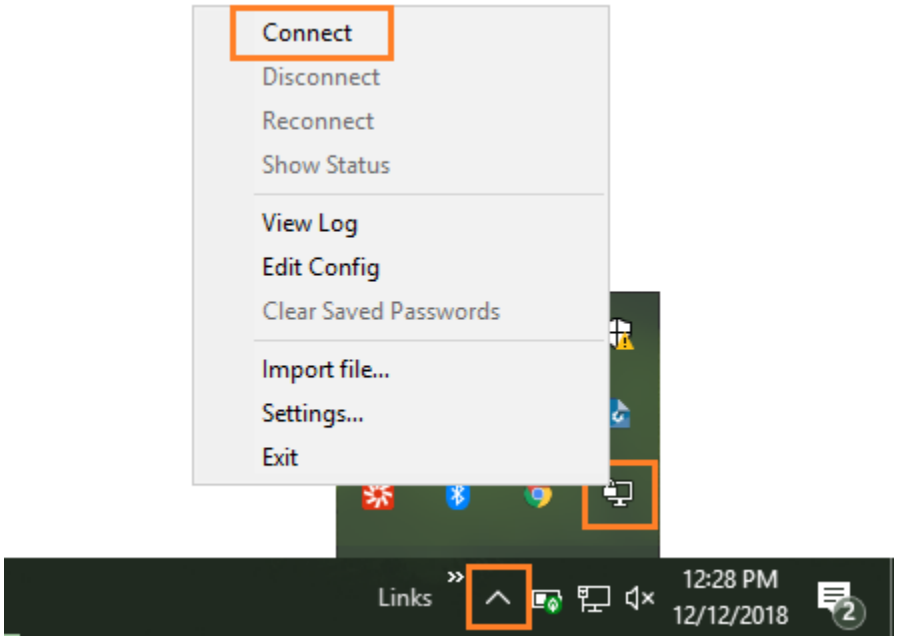
OpenVPN クライアントアプリケーションの詳細については、OpenVPN ウェブサイトの「コミュニティダウンロード」を参照してください。

VPN 接続を確立するには

1. OpenVPN クライアントアプリケーションを起動します。
2. Windows のタスクバーで、[表示/非表示アイコン] を選択して [OpenVPN GUI] を右クリックし、[Import file (ファイルのインポート)] を選択します。



3. [Open (開く)] 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 (開く)] を選択します。
4. Windows のタスクバーで、[表示/非表示アイコン] を選択して [OpenVPN GUI] を右クリックし、[Connect (接続)] を選択します。



OpenVPN 接続クライアント

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

> Note
>
> 詳細については、OpenVPN ウェブサイトの「Windows でアクセスサーバーに接続する」を参照してください。

VPN 接続を確立するには

1. OpenVPN 接続クライアントアプリケーションを起動します。
2. Windows のタスクバーで、[表示/非表示アイコン] を選択して [OpenVPN] を右クリックし、[Import profile (プロファイルのインポート)] を選択します。
3. [Import from File (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 VPN クライアントアプリケーションを使用して接続する

Android または iOS モバイルデバイスで OpenVPN クライアントアプリケーションを使用し、 VPN 接続を確立する方法を次に示します。Android 用の手順と iOS 用の手順は同じです。

> Note
>
> Android 用 OpenVPN クライアントアプリケーションの詳細については、OpenVPN ウェブサイトの「FAQ regarding OpenVPN Connect Android」を参照してください。

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済みであることを確認します。

接続を確立するには、OpenVPN クライアントアプリケーションを起動した後、クライアント VPN 管理者から受信し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接続する

次の手順は、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を示しています。

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済みであることを確認します。

トラブルシューティング情報については、「macOS のトラブルシューティング (p. 29)」を参照してください。

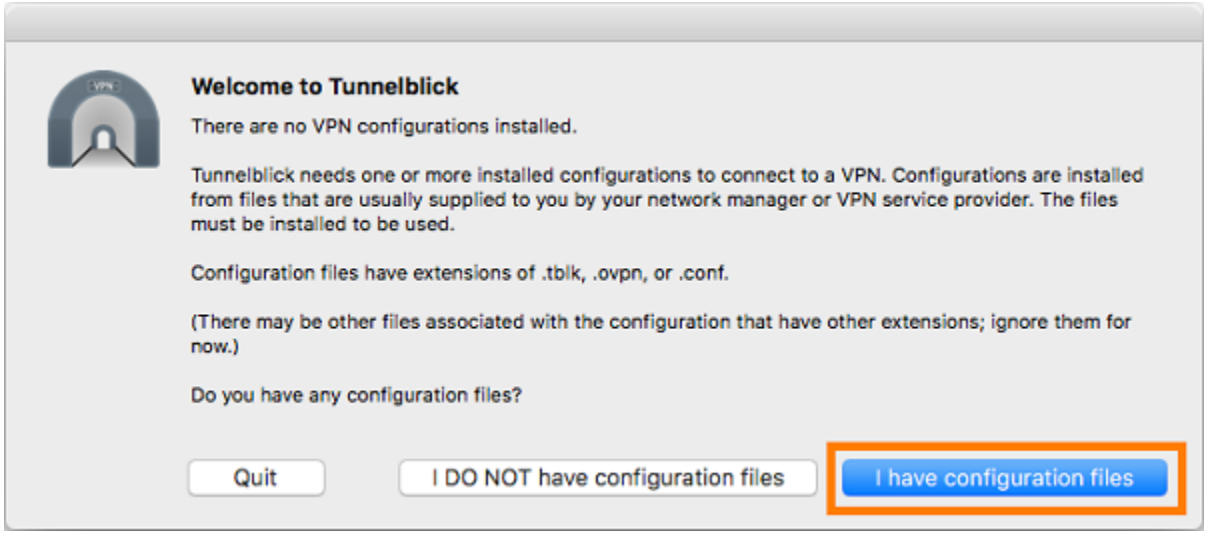
Tunnelblick

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、 VPN 接続を確立する方法を示します。

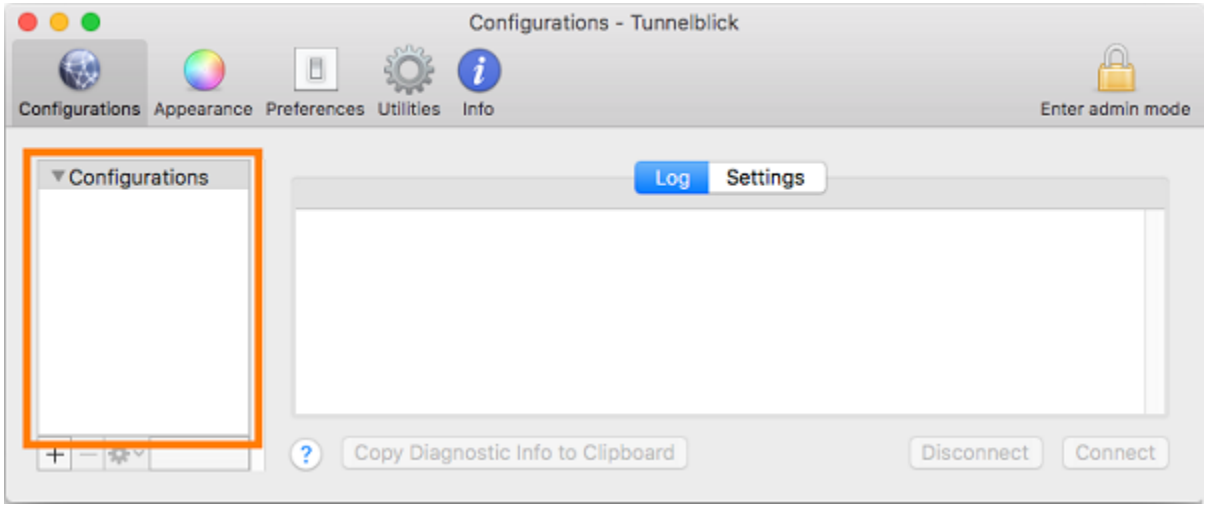
> Note
>
> macOS 用 Tunnelblick クライアントアプリケーションの詳細については、Tunnelblick ウェブサイトのTunnelblick マニュアルを参照してください。

VPN 接続を確立するには

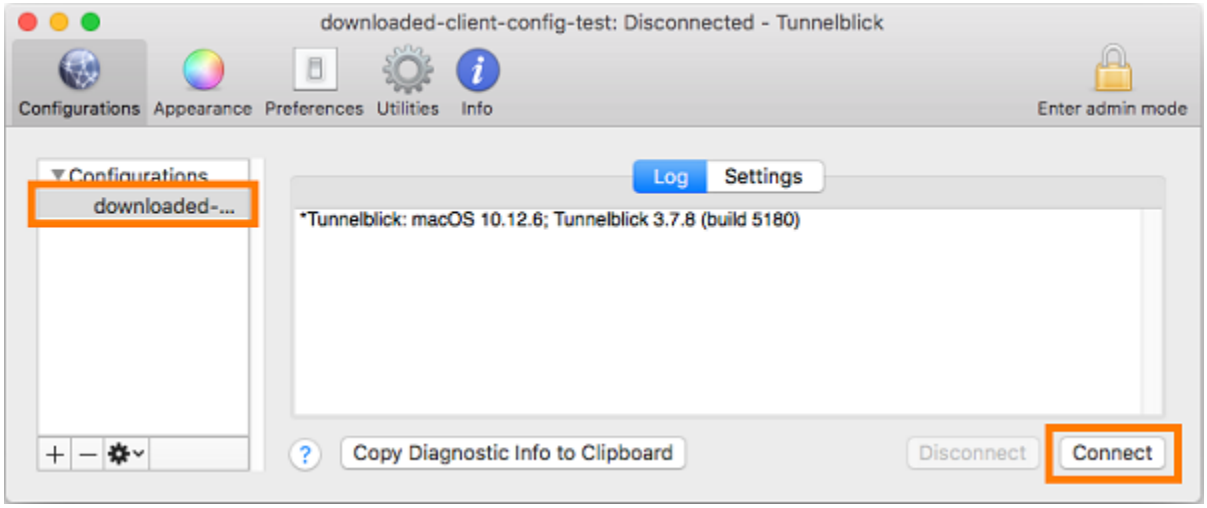
1. Tunnelblick クライアントアプリケーションを起動し、[I have configuration files (設定ファイルを持っている)] を選択します。



2. VPN 管理者から受け取った設定ファイルをドラッグし、[Configurations (設定)] パネルにドロップします。



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 接続クライアント

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

Note

詳細については、OpenVPN ウェブサイトの「macOS でアクセスサーバーに接続する」を参照してください。

VPN 接続を確立するには

1. OpenVPN 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...] の順に選択します。
2. VPN 管理者から受信した設定ファイルに移動し、[開く] をクリックします。

OpenVPN クライアントアプリケーションを使用して接続する

次の手順は、OpenVPN 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を示しています。

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済みであることを確認します。

トラブルシューティング情報については、「Linux のトラブルシューティング (p. 33)」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、OpenVPN 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。

OpenVPN - ネットワークマネージャー

次の手順は、Ubuntu コンピュータでネットワークマネージャー GUI で、OpenVPN 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. [VPN] の横のプラス記号 (+) を選択し、[Import from file... (ファイルからインポート...)] を選択します。
4. VPN 管理者から受信した設定ファイルに移動し、[Open (開く)] を選択します。
5. [VPN の追加] 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。

OpenVPN

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

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

次のトピックを使用して、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がある問題のトラブルシューティングを行います。

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 エンドポイントでクライアント VPN 管理者が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 VPN のトラブルシューティング」を参照してください。

AWS が提供するクライアントで AWS Support に診断ログを送信する

AWS が提供するクライアントに問題があり、AWS Support に連絡してトラブルシューティングを行う必要がある場合に備えて、クライアントから AWS Support に診断ログを送信するオプションが用意されています。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、AWS Support が診断ログにアクセスすることを許可することに同意する必要があります。お客様が同意すると、参照番号が用意されます。これを提供することによって、AWS Support が直ちにファイルにアクセスできるようなります。

診断ログの送信

以下のステップでは、AWS 提供のクライアントは AWS VPN クライアントとも呼ばれます。

Windows 用に AWS が提供する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。

   AWS Support に連絡する際には、参照番号をお知らせください。

macOS 用に AWS が提供する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。

   AWS Support に連絡する際には、参照番号をお知らせください。

Ubuntu 用に AWS が提供する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。必要に応じて、情報をクリップボードにコピーすることもできます。

   AWS Support に連絡する際には、参照番号をお知らせください。

Windows のトラブルシューティング

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の情報を以下に示します。

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

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。

- OpenVPN ログ: OpenVPN 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

Problem

AWS が提供するクライアントは、クライアント VPN エンドポイントに接続できません。

Cause

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 OpenVPN プロセスがコンピュータ上で既に実行されているため、クライアントが接続できません。
- 設定 (.ovpn) ファイルが有効ではありません。

Solution

コンピュータ上で他の OpenVPN アプリケーションが実行されているかどうか確認します。実行されている場合は、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ます。OpenVPN 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。
- CRL がまだ有効である。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

Problem

AWS が提供するクライアントは、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。

Cause

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 ホスト名が IP アドレスに解決されていません。
- OpenVPN プロセスがエンドポイントに無期限に接続しようとしています。

Solution

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、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するよう依頼します。また、AWS VPN Client ウィンドウで [切断] を選択して、VPN セッションを切断し、もう一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に終了する

Problem

クライアント VPN エンドポイントへの接続中に、クライアントが予期せずに終了します。

Cause

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。

Solution

AWS が提供するクライアントインストーラを再実行して、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

Problem

Windows 7 で、AWS が提供するクライアントを開こうとしても起動しません。

Cause

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

Solution

AWS が提供するクライアントインストーラを再実行して、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

Problem

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.
```

Cause

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) ファイルにクライアント証明書とキーは含まれていません。

Solution

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。

OpenVPN 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
```

OpenVPN 接続クライアント

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 接続クライアント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
```

DNS を解決できない

Problem

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.
```

Cause

DNS 名を解決できません。クライアントは、DNS キャッシュを防止するために、DNS 名の前にランダム文字列を付ける必要がありますが、一部のクライアントはこれを行っていません。

Solution

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 エイリアスがない

Problem

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
```

Cause

OpenVPN 接続クライアントソフトウェアには、相互認証を使用して認証を試みる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。

Solution

クライアント VPN 設定ファイルで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 接続クライアントソフトウェアにインポートします。または、OpenVPN GUI クライアント (v11.12.0.0) や Viscosity 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 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。
- OpenVPN ログ: OpenVPN 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、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
```

設定ファイルは、AWS が提供するクライアントによってコンピュータ上の以下の場所に保存されます。

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

トピック

クライアントが接続できない

Problem

AWS が提供するクライアントは、クライアント VPN エンドポイントに接続できません。

Cause

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 OpenVPN プロセスがコンピュータ上で既に実行されているため、クライアントが接続できません。
- 設定 (.ovpn) ファイルが有効ではありません。

Solution

コンピュータ上で他の OpenVPN アプリケーションが実行されているかどうか確認します。実行されている場合は、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ます。OpenVPN 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。
- CRL がまだ有効である。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

Problem

AWS が提供するクライアントは、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。

Cause

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 ホスト名が IP アドレスに解決されていません。
- OpenVPN プロセスがエンドポイントに無期限に接続しようとしています。

Solution

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、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するよう依頼します。また、AWS VPN Client ウィンドウで [切断] を選択して、VPN セッションを切断し、もう一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

Problem

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.
```

Cause

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) ファイルにクライアント証明書とキーは含まれていません。

Solution

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。

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
```

ログの冗長性を高めるには、Tunnelblick アプリケーションを開き、[Settings] を選択し、[VPN log level] の値を調整します。

暗号アルゴリズム「AES-256-GCM」が見つからない

Problem

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
```

Cause

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

Solution

次の手順を実行して、互換性のある OpenVPN 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. [OpenVPN version] の場合は、[2.4.6 - OpenSSL version is v1.0.2q] を選択します。

接続が応答を停止し、リセットされます。

Problem

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
```

Cause

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。

Solution

クライアント VPN 管理者に新しい設定ファイルを要求します。

拡張キー使用法 (EKU)

Problem

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,,,,,
```

Cause

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に、サーバー認証に対して有効になっている拡張キー使用法 (EKU) フィールドがあるため、クライアント認証は失敗します。

Solution

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。必要な場合は、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

Problem

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”
```

Cause

クライアント証明書の有効期限が切れています。

Solution

クライアント VPN 管理者に新しいクライアント証明書を要求します。

OpenVPN

以下のトラブルシューティング情報は、macOS High Sierra 10.13.6 上の OpenVPN 接続クライアント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
```

DNS を解決できない

Problem

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
```

Cause

OpenVPN 接続はクライアント VPN DNS 名を解決できません。

Solution

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 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

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の以下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の以下の場所に保存します。

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

Problem

VPN 接続が確立された後のある種の状況下では、DNS クエリは、ClientVPN エンドポイント用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送信されます。

Cause

AWS VPN クライアントは systemd-resolved と連携します。これは、Linux システムで利用可能なサービスであり、DNS 管理の中心的な部分として機能します。これは、ClientVPN 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、ClientVPN エンドポイントによって提供される DNS サーバーに最高の優先順位を設定しないことによって発生します。そうではなく、ローカルシステム上に構成されている DNS サーバーの既存のリストに、サーバーを追加します。その結果、元の DNS サーバーの優先順位が最高になったままであるため、DNS クエリの解決に使用される可能性があります。

Solution

1. OpenVPN 設定に次の指令を追加して、すべての DNS クエリが VPN トンネルに送信されるようにします。

   ```
   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 が DNS クエリに対してプロキシとなるのではなく、クエリを実際の DNS ネームサーバーに直接送信したい場合は、`/etc/resolv.conf` から `/run/systemd/resolve/resolv.conf` へのシンボリックリンクとします。。

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

   DNS 応答キャッシング、インターフェイスごとの DNS 設定、DNSSec の強制適用など、systemd-resolved の設定をバイパスするためにこの手順を適用することができます。このオプションは、VPN に接続し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。たとえば、プライベート VPC 内にプライベート DNS リゾルバーがあり、プライ

ベート IP に解決される www.example.com のレコードがあるとします。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)

Problem

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。

Cause

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。

Solution

DNS サーバーが設定され、正しく機能していることを確認するには、次のステップを実行します。

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、最後の行に 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 エンドポイントを変更するよう依頼し、クライアント VPN エンドポイントに DNS サーバー (VPC DNS 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 (GUI) を介した OpenVPN

Problem

Network Manager OpenVPN クライアントを使用すると、次のエラーで接続が失敗します。

```
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
```

Cause

`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。

Solution

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。

よくある問題

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一般的な問題を次に示します。

TLS キーネゴシエーションが失敗した

Problem

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
```

Cause

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。

Solution

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 のインバウンドまたはアウトバウンドの TCP または UDP トラフィックをブロックしているかどうか確認します。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。

- 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 または 1194 の TCP または UDP トラフィックをブロックしていない。
- 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。
- CRL がまだ有効である。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 Client VPN ユーザーガイドの更新について説明しています。

更新履歴の変更	更新 - 履歴 - 記述	更新 - 履歴 - 日付
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) 向け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 LTS 向けクライアントをリリース	AWS が提供するクライアントを Ubuntu 18.04 LTS や Ubuntu 20.04 LTS で使用できます。	2021 年 6 月 11 日
Windows 証明書システムストアの証明書を使用する OpenVPN をサポート	Windows 証明書システムストアの証明書で 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 が提供する最新のクライアントおよび設定ファイルを入手できます。	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 (p. 38)	このリリースでは、AWS クライアント VPN が導入されています。	2018 年 12 月 18 日