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 Client VPN とは

AWS Client 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。

クライアント VPN コンポーネント

AWS Client 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。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。AWS が提供するクライアントでは、5 つの同時セッションに接続できます。各セッションには、クライアント VPN 管理者が提供する独自の設定ファイルがあります。同時セッションの詳細については、「同時接続のサポート」を参照してください。

クライアント VPN を設定するための追加リソース

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。

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

クライアント VPN を使用するための前提条件

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
- サポートされているバージョンの Windows、macOS、または Linux。
- 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。

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を使用して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、「AWS クライアント VPN ダウンロード」からクライアント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” を実施し、管理者からエンドポイント設定ファイルを取得します。複数のプロファイルに接続する場合は、プロファイルごとに設定ファイルが必要です。
- 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、「the section called “クライアント VPN をダウンロード”」を参照してください。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、the section called “ステップ 3: VPN に接続する” に進みます。

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 提供された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から AWS Client VPN をダウンロードする」を参照してください。

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 指定された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、VPN に接続します。 AWS 提供されたクライアントの 1 つ以上の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 提供されたクライアントを使用して AWS Client 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 AWS Client 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 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、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から AWS Client VPN をダウンロードする

セルフサービスポータルは、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 VPN クライアントの設定ファイルを 1 つ以上事前に設定している場合は、このポータルからそのクライアント VPN アプリケーションと設定ファイルを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、「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、ダウンロードする各クライアント 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 か、または ID を含むセルフサービスポータル URL を提供できます。複数のエンドポイント接続の場合、接続する各プロファイルのエンドポイント ID が必要です。

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。複数のエンドポイントに接続する場合は、各エンドポイントの設定ファイルをダウンロードする必要があります。
   - 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。
5. 接続プロファイルを作成するエンドポイント設定ファイルごとに、これらのステップを繰り返します。

AWS 提供されたクライアントを使用して AWS Client VPN エンドポイントに接続する

Windows、macOS、および Ubuntu でサポートされている 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、最大 5 つの同時接続と OpenVPN ディレクティブもサポートします。

トピック

セキュリティ

AWS 提供されたクライアントでは、セキュリティが最優先事項です。アプリケーションのセキュリティ体制を改善するために、定期的にパッチをリリースしています。AWS が提供するクライアントには、SAML 認証、クライアントルート強制、デバイス設定のモニタリングなど、他の OpenVPN クライアントにはない、いくつかの独自のセキュリティ機能が含まれています。

AWS 提供されたクライアントは、設定ミスや侵害されたネットワーク環境に起因する脅威を軽減するように設計されていますが、環境を変更したり、ソースにある外部脅威を排除したりする責任はありません。 AWS 提供されたクライアントは、安全で適切に設定された環境を維持するために、お客様に依存しています。これには、以下が含まれます。

- ローカルユーザーによる不正な変更や不正使用を防止すること
- 管理者権限を付与する対象を信頼されたユーザーに限定すること
- 最新のセキュリティパッチが適用された状態を維持すること

AWS が提供するクライアントを使用した同時接続のサポート

AWS 提供されたクライアントにより、 は複数の同時セッションに接続できます。これは、複数の AWS 環境のリソースにアクセスする必要があり、それらのリソースのエンドポイントが異なる場合に役立ちます。たとえば、現在接続しているエンドポイントとは異なるエンドポイントの環境にあるデータベースにアクセスする必要があるものの、現在の接続を切断したくない場合がこれに該当します。 AWS 提供されたクライアントが現在のセッションに接続できるようにするには、管理者が各工

ンドポイント用に作成した設定ファイルをダウンロードし、ファイルごとに接続プロファイルを作成します。 AWS 提供されたクライアントを使用して、現在開いているセッションから切断することなく、複数のセッションに接続できます。これは、 AWS 提供されたクライアントでのみサポートされます。同時セッションへの接続の手順については、以下を参照してください。

- AWS 提供された Windows 用クライアントを使用して接続する
- AWS 提供された macOS 用クライアントを使用して接続する
- Linux 用の AWS が提供するクライアントを使用して接続する

複数のエンドポイントに接続する場合、クライアント VPN はチェックを実装して、他のオープンエンドポイント接続と競合していないことを確認します。例えば、2 つのセッションに競合する CIDR ブロックまたはルーティングポリシーがある場合、または既に完全なトンネル接続に接続されている場合などがこれに該当します。チェックで競合が検出された場合、オープン接続と競合しない別の接続を選択するか、競合の原因となっているオープンセッションから切断されるまで、接続は確立されません。

同時 DNS 接続が許可されます。いずれかの DNS 対応接続の DNS サーバーが適用されます。DNS サーバーによっては、その再接続中に認証を求められる場合があります。

> **Note**
>
> 同時セッションの最大数は 5 件です。

OpenVPN ディレクティブ

AWS 提供されたクライアントは、次の OpenVPN ディレクティブをサポートしています。これらのディレクティブの詳細については、OpenVPN ウェブサイトのドキュメントを参照してください。

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- block-outside-dns
- ca

- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive
- key
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- ping-exit
- 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
- tap-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN for Windows

このセクションでは、Windows x64 および Windows Arm64 システム用に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。[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提供された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提供されているクライアントは、Windows x64 システムと Arm64 システムの両方をサポートしています。各オペレーティングシステムには以下が必要です。

Windows Arm64 オペレーティングシステム

- Windows 11 (64 ビットオペレーティングシステム、Arm64 プロセッサ)
- .NET Framework 4.8.1 以降

> **Note**
>
> このアプリケーションには、Arm64 エミュレーションを利用するバックグラウンドプロセスが含まれています。これは Windows 11 Arm64 デバイスで完全にサポートされ、デフォルト

で有効になっているため、追加のセットアップを必要とせずにシームレスに操作できます。詳細については、「Arm でのエミュレーションの仕組み」を参照してください。

Windows x64 オペレーティングシステム

- 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 Framework 4.7.2 以降

> **Note**
>
> Windows x64 オペレーティングシステムと Arm64 オペレーティングシステムのどちらにおいても、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、クライアントはコンピュータの TCP ポート 8096-8115 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。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

トピック

- Windows 用の AWS 提供のクライアント AWS Client VPN を使用して 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 AWS Client VPN を使用して 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Site-to-Site VPN クライアントとも呼ばれます。

Windows x64 ベースまたは Windows Arm64-basedシステム用に AWS 提供されたクライアントを使用して接続するには:

1. Site-to-Site 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. 複数の接続を作成する場合は、追加する設定ファイルごとに [プロファイルの追加] のステップを繰り返します。プロファイルはいくつでも追加できますが、オープン接続の上限は 5 つです。
7. [Site-to-Site VPN クライアント] ウィンドウで、接続するプロファイルを選択し、[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。開始するプロファイル接続ごとにこのステップを繰り返し、最大 5 つの同時エンドポイントを接続します。

   > **Note**
   >
   > 接続するプロファイルが現在開いているセッションと競合する場合、接続を行うことはできません。新しい接続を選択するか、競合の原因となるセッションから切断します。

8. 接続の統計を表示するには、[AWS VPN クライアント] ウィンドウで [接続] を選択し、[詳細を表示] を選択して、詳細を表示する接続を選択します。
9. 接続を切断するには、[AWS VPN クライアント] ウィンドウで接続を選択し、[切断] を選択します。複数のオープン接続がある場合は、各接続を個別に閉じる必要があります。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、Windows x64 ベースおよび AWS Client VPN Windows Arm64-basedシステム用の 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**
>
> すべてのリリースで、引き続きユーザビリティとセキュリティの修正を提供します。常に最新のプラットフォームバージョンを使用することをお勧めします。古いバージョンは、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。

バージョン	変更	日付	ダウンロードリンクと SHA256
5.3.4 (x64 および Arm64)	• 軽微なバグの修正と機能強化 • セキュリティ態勢の強化	2026 年 3 月 27 日	• Windows x64 バージョン 5.3.4 をダウンロードする sha256: 81a5c5101 624c5f74d e8afdcb81 6f03ea8ff 9e8c6a5ea a8890a957 79a94dbe41 • Windows Arm64 バージョン 5.3.4 をダウンロードする sha256: 3410282eb b024e6481 2a63668b3 0117657d4 70ed4c51f 05e96fc81 2b8871587d
5.3.3 (x64 および Arm64)	• バージョン 5.3.2 の接続エラーを修正しました	2026 年 2 月 28 日	• Windows x64 バージョン 5.3.3 をダウンロードする

バージョン	変更	日付	ダウンロードリンクと SHA256
			sha256: bbaebb977 b270add64 97c941505 fed5913b5 8056e980e 372170733 7dc051ac86 • Windows Arm64 バージョン 5.3.3 をダウンロードする sha256: c30b6d012 1a5070643 fdbebc27e 7f9569d57 4a5698631 480becb5c b96cac9fde

バージョン	変更	日付	ダウンロードリンクと SHA256
5.3.2 (x64 および Arm64)	• 軽微なバグの修正と機能強化。 • セキュリティ体制を強化しました。	2026 年 2 月 17 日	• Windows x64 バージョン 5.3.2 をダウンロードする sha256: dd1e4fb67 18dddbf13 a5aee5421 75761bf8e d854290c5 76a488b98 173a0ccf92 • Windows Arm64 バージョン 5.3.2 をダウンロードする sha256: d2d18d91c a9ef53cc5 57434db18 ef5d0002e 7825a998f 2d739eac4 43b034af00

バージョン	変更	日付	ダウンロードリンクと SHA256
5.3.1 (x64 および Arm64)	軽微なバグの修正と機能強化。	2025 年 9 月 30 日	• Windows x64 バージョン 5.3.1 をダウンロードする sha256: b71ddbc78230630963acf3ebba7afeb6e52599843091ff589aed6afce4c9eb06 • Windows Arm64 バージョン 5.3.1 をダウンロードする sha256: e691bdb0bdcb55b3da36f4fb2e5198f20f1878dc22a00bf55bc660999698500b

バージョン	変更	日付	ダウンロードリンクと SHA256
5.3.0 (Arm64)	Windows Arm64-basedオペレーティングシステムの新しい AWS Client VPN サポート。 このリリースには、Windows (x64) 5.3.0 リリースのすべての更新が含まれています。	2025 年 8 月 26 日	Windows Arm64 バージョン 5.3.0 をダウンロードする sha256: 3f1be6b487af8307dafbb0f7737cd597cf71dc64dcd31775aeeebf91d04b8dce
5.3.0	• 軽微な機能強化。 • IPv6 接続のサポートを追加	2025 年 8 月 14 日	Windows x64 バージョン 5.3.0 をダウンロードする sha256: e3cf1aff6e14d79aa44378229a3a0602a9e9c2a0c6d0d055df901440b6d1454a
5.2.2	セキュリティ体制を強化しました。	2025 年 6 月 2 日	ダウンロードバージョン 5.2.2 sha256: f27cb0eed7c9c5354caa5d7e37595eefbb048d7481bf698b2e5fb653b667c190

バージョン	変更	日付	ダウンロードリンクと SHA256
5.2.1	• `ping-exit` OpenVPN フラグのサポートを追加しました。 • OpenSSL ライブラリを更新しました。 • 軽微なバグの修正と機能強化。	2025 年 4 月 21 日	サポートは終了しました。
5.2.0	• 軽微な機能強化。 • クライアントルート強制のサポートを追加しました。	2025 年 4 月 8 日	サポートは終了しました。
5.1.0	• 非アクティブタイムアウト切断後に AWS Client VPN バージョン 5.0.x が VPN に自動的に再接続する問題を修正しました。 • 軽微なバグの修正と機能強化。	2025 年 3 月 17 日	サポートは終了しました。
5.0.2	• 同時接続の DNS の問題を修正しました。 • 新しい TAP アダプターをインストールする際の散発的な問題を修正しました。	2025 年 2 月 24 日	サポートは終了しました。
5.0.1	Windows クライアントバージョン 5.0.0 で散発的な VPN 接続エラーが発生する問題を修正しました。	2025 年 1 月 30 日	サポートは終了しました。
5.0.0	• 同時接続のサポートが追加されました。 • TAP ドライバーのバージョンを更新しました。 • グラフィカルユーザーインターフェイスを更新しました。 • 軽微なバグの修正と機能強化	2025 年 1 月 21 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と SHA256
4.1.0	軽微なバグの修正と機能強化。	2024 年 11 月 12 日	サポートは終了しました。
4.0.0	軽微な機能強化。	2024 年 9 月 25 日	ダウンロードバージョン 4.0.0 sha256: 6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc
3.14.2	`mssfix` OpenVPN フラグのサポートを追加しました。	2024 年 9 月 4 日	ダウンロードバージョン 3.14.2 sha256: c171639d7e07e5fd48998cf76f74e6e49e5cbe3356c6264a67b4a9bf473b5f5d

バージョン	変更	日付	ダウンロードリンクと SHA256
3.14.1	軽微なバグの修正と機能強化。	2024 年 8 月 22 日	ダウンロードバージョン 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	• `tap-sleep` OpenVPN フラグのサポートを追加しました。 • OpenVPN ライブラリと OpenSSL 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: 812fb2f6d 263288c66 4d598f6bd 70e3f601d 11dcb89e6 3b281b0a9 6b96354516
3.13.0	OpenVPN ライブラリと OpenSSL 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 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b

バージョン	変更	日付	ダウンロードリンクと SHA256
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 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: 5ed34aee6c03aa281e625acdbed272896c67046364a9e5846ca697e05dbfec08
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、自動的に再接続されます。 • SAML エンドポイントに接続している場合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
3.11.2	バージョン 123 以降、Chromium ベースのブラウザで SAML 認証の問題が解決されました。	2024 年 4 月 11 日	ダウンロードバージョン 3.11.2 sha256: 8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc

バージョン	変更	日付	ダウンロードリンクと SHA256
3.11.1	• バッファオーバーフローアクションを修正しました。これにより、ローカルアクターがより強い権限を持つ任意のコマンドを実行できるようになっていたためです。 • 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: fb67b60aa837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Windows 仮想マシンが原因で発生した接続の問題を修正しました。 • 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
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に関する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

バージョン	変更	日付	ダウンロードリンクと SHA256
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
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

バージョン	変更	日付	ダウンロードリンクと SHA256
3.2.0	• 「verify-x509-name」OpenVPN 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。 • TAP Windows ドライバの命名により、他のドライバ名が影響を受ける問題を修正しました。 • 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
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

バージョン	変更	日付	ダウンロードリンクと SHA256
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	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	• 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	サポートは終了しました
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	サポートは終了しました
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	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と SHA256
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	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
1.2.7	• 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	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	• 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と SHA256
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

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。[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提供された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提供されたクライアントを macOS で使用するには、以下が必要です。

- macOS Sonoma (14.0)、Sequoia (15.0)、または Tahoe (26.0)
- x86_64 または ARM64 プロセッサ互換。
- 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、クライアントではコンピュータの TCP ポート 8096-8115 を予約します。

トピック

- macOS 用の AWS が提供するクライアント AWS Client VPN を使用して 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 AWS Client VPN を使用して 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済みであることを確認します。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

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Site-to-Site 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. Site-to-Site 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. 複数の接続を作成する場合は、追加する設定ファイルごとに [プロファイルの追加] のステップを繰り返します。プロファイルはいくつでも追加できますが、オープン接続の上限は 5 つです。
7. [Site-to-Site VPN クライアント] ウィンドウで、接続するプロファイルを選択し、[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。開始するプロファイル接続ごとにこのステップを繰り返し、最大 5 つの同時エンドポイントを接続します。

   > **Note**
   >
   > 接続するプロファイルが現在開いているセッションと競合する場合、接続を行うことはできません。新しい接続を選択するか、競合の原因となるセッションから切断します。

8. 接続の統計を表示するには、[AWS VPN クライアント] ウィンドウで [接続] を選択し、[詳細を表示] を選択して、詳細を表示する接続を選択します。

9. 接続を切断するには、[AWS VPN クライアント] ウィンドウで接続を選択し、[切断] を選択します。複数のオープン接続がある場合は、各接続を個別に閉じる必要があります。

AWS Client VPN for macOS リリースノート

次の表に、 AWS Client VPN macOS 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**
>
> すべてのリリースで、引き続きユーザビリティとセキュリティの修正を提供します。常に最新のプラットフォームバージョンを使用することをお勧めします。古いバージョンは、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。

バージョン	変更	日付	ダウンロードリンク
5.3.4	• ARM マシンの Intel 互換レイヤー (Rosetta) 要件を削除 • 軽微なバグの修正と機能強化	2026 年 2 月 17 日	• macOS ARM64 バージョン 5.3.4 をダウンロードする sha256: b6b019d3f037c8ea8f94db1fc043654667c2bae6f23ea1cc1e8754576cae170a • macOS x64 バージョン 5.3.4 をダウンロードする sha256: df93932dcbb1d8a23b0f9a6fc4df98a5d8d265a603db6f4b4c70bbc3c44d6583

バージョン	変更	日付	ダウンロードリンク
5.3.3	• 軽微なバグの修正と機能強化。 • セキュリティ体制を強化しました。	2025 年 12 月 26 日	• macOS ARM64 バージョン 5.3.3 をダウンロードする sha256: 97c4b869e a5a544a4a4fe661580 ec21f412b141bb2187 fd32fcd97e75581b018 • macOS x64 バージョン 5.3.3 をダウンロードする sha256: cf8d16ec3 5b330969510a6cfc82 8db1157088ad7bb77e 0344b87bd7a59921c1f

バージョン	変更	日付	ダウンロードリンク
5.3.2	• Apple Silicon アーキテクチャのネイティブサポートと新しい macOS ARM64 インストーラが追加されました。 • 軽微なバグの修正と機能強化。	2025 年 10 月 27 日	• macOS ARM64 バージョン 5.3.2 をダウンロードする sha256: ef0e323f7c262263018ae303d1cfd0333c976963a5e1055706b988d7463e1dd2 • macOS x64 バージョン 5.3.2 をダウンロードする sha256: 29c0fc329b7ac457bbbb3ee71004bf4f7ef76a928b08c8c589a04f65804f8986
5.3.1	• 軽微なバグの修正と機能強化。	2025 年 9 月 9 日	ダウンロードバージョン 5.3.1 sha256: e71c70072c338bd41f3925a541f5d7a73d9e063a00786a603ea9043ced1baa16
5.3.0	• 軽微な機能強化。 • IPv6 接続のサポートが追加されました。	2025 年 8 月 14 日	ダウンロードバージョン 5.3.0 sha256: ec5b7c562b1e91d902168f32c426c0a074ee0fdbfc061ef862165d6a42d2cf79

バージョン	変更	日付	ダウンロードリンク
5.2.1	• ping-exit OpenVPN フラグのサポートを追加しました。 • OpenSSL ライブラリを更新しました。 • セキュリティ体制を強化しました。 • 軽微なバグの修正と機能強化。	2025 年 6 月 18 日	ダウンロードバージョン 5.2.1 sha256: 906f77fbca3334fbdcd1145dd6f2725beab82a30b9b51eafd1a25c3fe7d669eb
5.2.0	• 軽微な機能強化。 • クライアントルート強制のサポートを追加しました。	2025 年 4 月 8 日	サポートは終了しました。
5.1.0	• 非アクティブタイムアウト切断後に AWS Client VPN バージョン 5.0.x が VPN に自動的に再接続する問題を修正しました。 • Windows 形式の行末の設定ファイルに対して が VPN 接続を確立 AWS Client VPN できない問題を修正しました。 • 軽微なバグの修正と機能強化。	2025 年 3 月 17 日	サポートは終了しました。
5.0.3	軽微なバグの修正と機能強化。	2025 年 3 月 6 日	サポートは終了しました。
5.0.2	[接続] を選択したときに散発的なエラーが発生する問題を修正しました。	2025 年 2 月 17 日	サポートは終了しました。
5.0.1	クライアントバージョン 5.0.0 がスペースを含むプロファイル名の VPN 接続を確立できない問題を修正しました。	2025 年 1 月 22 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
5.0.0	• 同時接続のサポートが追加されました。 • グラフィカルユーザーインターフェイスを更新しました。 • 軽微なバグの修正と機能強化。	2025 年 1 月 21 日	サポートは終了しました。
4.1.0	軽微なバグの修正と機能強化。	2024 年 11 月 12 日	サポートは終了しました。
4.0.0	軽微な機能強化。	2024 年 9 月 25 日	サポートは終了しました。
3.12.1	`mssfix` OpenVPN フラグのサポートを追加しました。	2024 年 9 月 4 日	サポートは終了しました。
3.12.0	• `tap-sleep` OpenVPN フラグのサポートを追加しました。 • OpenVPN ライブラリと OpenSSL ライブラリを更新しました。	2024 年 8 月 12 日	サポートは終了しました。
3.11.0	• OpenVPN ライブラリと OpenSSL ライブラリを更新しました。	2024 年 7 月 29 日	サポートは終了しました。
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、自動的に再接続されます。 • 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。 • SAML エンドポイントに接続している場合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。

バージョン	変更	日付	ダウンロードリンク
3.9.2	• バージョン 123 以降、Chromium ベースのブラウザで SAML 認証の問題が解決されました。 • 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	サポートは終了しました。
3.9.1	• バッファオーバーフローアクションを修正しました。これにより、ローカルアクターがより強い権限を持つ任意のコマンドを実行できるようになっていたためです。 • 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	サポートは終了しました。
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	サポートは終了しました。
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	サポートは終了しました。
3.7.0	• セキュリティ体制を強化しました。	2023 年 8 月 3 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 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。

バージョン	変更	日付	ダウンロードリンク
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」OpenVPN 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	• 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。

バージョン	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	• 接続中に DNS サーバーモニタリングを追加しました。VPN 設定と一致しない場合、設定は再構成されます。 • 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	• 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	サポートは終了しました。
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	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
1.3.3	• 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	サポートは終了しました。
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	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
1.3.1	• 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	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	• 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。

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。 • 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。
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。

AWS Client VPN Linux 用

このセクションでは、Linux 用に AWS 提供されたクライアントをインストールし、 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。Linux 用に AWS 提供されているクライアントは、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、「the section called “リリースノート”」を参照してください。

Linux 用の AWS 提供のクライアントを使用してクライアント VPN に接続するための要件

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

- Ubuntu 22.04 LTS (AMD64) または Ubuntu 24.04 LTS (AMD64 のみ)

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、クライアントではコンピュータの TCP ポート 8096-8115 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。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

トピック

- Linux AWS Client VPN 用に提供されている をインストールする
- Linux AWS Client VPN 用に提供されている に接続する
- AWS Client VPN for Linux リリースノート

Linux AWS Client VPN 用に提供されている をインストールする

Linux 用に AWS 提供された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インストールする

1. AWS VPN クライアントのパブリックキーを 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. 次のコマンドを使用して、リポジトリを Ubuntu OS (バージョン 22.04 以降) に追加します。

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

3. 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 提供された 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、Linux 用の AWS 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。

Linux AWS Client VPN 用に提供されている に接続する

以下のステップでは、 AWS 提供されたクライアントはSite-to-Site 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. Site-to-Site 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. 複数の接続を作成する場合は、追加する設定ファイルごとに [プロファイルの追加] のステップを繰り返します。プロファイルはいくつでも追加できますが、オープン接続の上限は 5 つです。
8. [Site-to-Site VPN クライアント] ウィンドウで、接続するプロファイルを選択し、[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。開始するプロファイル接続ごとにこのステップを繰り返し、最大 5 つの同時エンドポイントを接続します。

   > **Note**
   >
   > 接続するプロファイルが現在開いているセッションと競合する場合、接続を行うことはできません。新しい接続を選択するか、競合の原因となるセッションから切断します。

9. 接続の統計を表示するには、[AWS VPN クライアント] ウィンドウで [接続] を選択し、[詳細を表示] を選択して、詳細を表示する接続を選択します。
10. 接続を切断するには、[AWS VPN クライアント] ウィンドウで接続を選択し、[切断] を選択します。複数のオープン接続がある場合は、各接続を個別に閉じる必要があります。

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**
>
> すべてのリリースで、引き続きユーザビリティとセキュリティの修正を提供します。常に最新のプラットフォームバージョンを使用することをお勧めします。古いバージョンは、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。

バージョン	変更	日付	ダウンロードリンク
5.3.2	• 軽微なバグの修正と機能強化。 • セキュリティ体制を強化しました。	2025 年 12 月 17 日	ダウンロードバージョン 5.3.2 sha256: 89e4b9f2c9f7def37167f5f137f4ff9c6c5246fd6e0a7244b70c196a17683569
5.3.1	• 軽微な機能強化。	2025 年 9 月 25 日	ダウンロードバージョン 5.3.1 sha256: 4a426cc226382748d683a4946340447dab87ec42583977d9488ee45d11cdcec0
5.3.0	• 軽微な機能強化。 • IPv6 接続のサポートが追加されました。	2025 年 8 月 14 日	ダウンロードバージョン 5.3.0 sha256: 31edb55f12dcd68a7a4ca9b6233ddbeebcd37e01f87655a520cc7e7542bbfcb4
5.2.0	• 軽微な機能強化。	2025 年 4 月 8 日	ダウンロードバージョン 5.2.0

バージョン	変更	日付	ダウンロードリンク
	• クライアントルート強制のサポートを追加しました。		sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• 非アクティブタイムアウト切断後に AWS Client VPN バージョン 5.0.x が VPN に自動的に再接続する問題を修正しました。 • 軽微なバグの修正と機能強化。	2025 年 3 月 17 日	ダウンロードバージョン 5.1.0 sha256: 14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba
5.0.0	• 複数の同時接続のサポートが追加されました。 • グラフィカルユーザーインターフェイスを更新しました。 • 軽微なバグの修正と機能強化。	2025 年 1 月 21 日	ダウンロードバージョン 5.0.0 sha256: 645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c

バージョン	変更	日付	ダウンロードリンク
4.1.0	• Ubuntu 22.04 および 24.04 のサポートが追加されました。 • バグが修正されました。	2024 年 11 月 12 日	ダウンロードバージョン 4.1.0 sha256: 334d00222 458fbfe9d ade16c99f e97e9ebcb d51fff017 d0d6b1d1b 764e7af472
4.0.0	軽微な機能強化。	2024 年 9 月 25 日	ダウンロードバージョン 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	`mssfix` OpenVPN フラグのサポートを追加しました。	2024 年 9 月 4 日	ダウンロードバージョン 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2

バージョン	変更	日付	ダウンロードリンク
3.15.0	• `tap-sleep` OpenVPN フラグのサポートを追加しました。 • OpenVPN ライブラリと OpenSSL 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	• OpenVPN ライブラリと OpenSSL 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、自動的に再接続されます。	2024 年 5 月 21 日	ダウンロードバージョン 3.13.0 sha256: e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1

バージョン	変更	日付	ダウンロードリンク
3.12.2	• バージョン 123 以降、Chromium ベースのブラウザで SAML 認証の問題が解決されました。	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	• バッファオーバーフローアクションを修正しました。これにより、ローカルアクターがより強い権限を持つ任意のコマンドを実行できるようになっていたためです。 • 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

バージョン	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: 86c0fa1bf1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
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: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
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 3.9.0 sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454

バージョン	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」OpenVPN 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。

バージョン	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	• 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	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。 • 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	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 AWS Client VPN エンドポイントに接続する

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 VPN は、以下のオペレーティングシステムでサポートされています。

- Windows

  Windows 証明書ストアの証明書とプライベートキーを使用します。証明書とキーを生成したら、OpenVPN GUI AWS クライアントアプリケーションまたは OpenVPN GUI Connect OpenVPN クライアントを使用してクライアント接続を確立できます。証明書とキーを作成する手順については、「Windows の証明書を使用して VPN 接続を確立する」を参照してください。

- macOS

  macOS ベースの Tunnelblick または AWS クライアント VPN の設定ファイルを使用して VPN 接続を確立します。詳細については、「macOS で VPN 接続を確立する」を参照してください。

- Linux

  OpenVPN - Network Manager インターフェイスまたは OpenVPN アプリケーションを使用して、Linux で VPN 接続を確立します。OpenVPN - Network Manager インターフェイスを使用するには、ネットワークマネージャーモジュールをまずインストールする必要があります (まだインストールされていない場合)。詳細については、「Linux で VPN 接続を確立する」を参照してください。

- Android および iOS

  次の手順は、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示します。詳細については、「Android および iOS でのクライアント VPN 接続」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。これには、ARM ベースのアーキテクチャが含まれます。ARM プロセッサを搭載したデバイス (Apple Silicon Mac や ARM ベースの Windows デバイスなど) を使用している場合は、OpenVPN クライアントではなく、

AWS 提供されたクライアントで SAML ベースの VPN エンドポイントを使用する必要があります。

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 AWS Client 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 AWS Client 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 AWS Client VPN エンドポイントに接続する
- AWS Client VPN Android および iOS アプリケーション上の 接続

Windows クライアントアプリケーションを使用して AWS Client 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済みであることを確認します。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

トラブルシューティング情報については、「Windows ベースの AWS 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、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。これには、ARM ベースのアーキテクチャが含まれます。ARM プロセッサを搭載したデバイス (Apple Silicon Mac や ARM ベースの Windows デバイスなど) を使用している場合は、OpenVPN クライアントではなく、AWS 提供されたクライアントで SAML ベースの VPN エンドポイントを使用する必要があります。

タスク

- 証明書を使用して Windows で AWS クライアント VPN 接続を確立する

証明書を使用して Windows で AWS クライアント VPN 接続を確立する

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。

証明書を使用して接続を確立するには

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 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 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"
   ```
5. 設定が完了したら、OpenVPN を使用して、以下のいずれかの方法で VPN 接続を確立します。

   - OpenVPN GUI クライアントアプリケーションを使用する

1. OpenVPN 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。[OpenVPN GUI] を右クリックし、[ファイルをインポート] 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 タスクバーで、[アイコンの表示/非表示] を選択します。[OpenVPN GUI] を右クリックし、[接続] を選択します。

- OpenVPN GUI Connect クライアントを使用する
  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。

macOS クライアントアプリケーションを使用して AWS Client 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、Tunnelblick、または AWS クライアント VPN 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済みであることを確認します。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

トラブルシューティング情報については、「macOS AWS 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、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。これには、ARM ベースのアーキテクチャが含まれます。ARM プロセッサを搭載したデバイス (Apple Silicon Mac や ARM ベースの Windows デバイスなど) を使用している場合は、OpenVPN クライアントではなく、AWS 提供されたクライアントで SAML ベースの VPN エンドポイントを使用する必要があります。

トピック

macOS で AWS Client VPN 接続を確立する

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 接続を確立できます。

> **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。

Tunnelblick を使用して 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。

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

このセクションでは、OpenVPN (Network Manager または OpenVPN) 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済みであることを確認します。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

トラブルシューティング情報については、「Linux ベースの AWS クライアントを使用したクライアント 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、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。これには、ARM ベースのアーキテクチャが含まれます。ARM プロセッサを搭載したデバイス (Apple Silicon Mac や ARM ベースの Windows デバイスなど) を使用している場合は、OpenVPN クライアントではなく、AWS 提供されたクライアントで SAML ベースの VPN エンドポイントを使用する必要があります。

トピック

- Linux で AWS Client VPN 接続を確立する

Linux で AWS Client VPN 接続を確立する

Ubuntu コンピュータでネットワークマネージャー GUI を使用するか、または OpenVPN アプリケーションを使用して VPN 接続を確立します。

OpenVPN - Network Manager を使用して 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、[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 を使用して 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
```

AWS Client VPN Android および iOS アプリケーション上の 接続

> **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。これには、ARM ベースのアーキテクチャが含まれます。ARM プロセッサを搭載したデバイス (Apple Silicon Mac や ARM ベースの Windows デバイスなど) を使用している場合は、OpenVPN クライアントではなく、AWS 提供されたクライアントで SAML ベースの VPN エンドポイントを使用する必要があります。

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**
>
> iOS または Android 向け 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に関する詳細については、OpenVPN ウェブサイトの「OpenVPN Connect User Guide」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。複数のプロファイルに同時に接続する場合は、プロファイルごとに設定ファイルが必要です。

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。

AWS 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 提供されたクライアントの AWS サポート 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り、トラブルシューティング AWS サポート のために 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 サポート。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、診断ログへのアクセス AWS サポート を に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 サポート できるように、 に付与できる参照番号が提供されます。

診断ログを送信するには

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

AWS 提供された 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. Site-to-Site 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 サポート、参照番号を指定する必要があります。

macOS 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. Site-to-Site 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 サポート、参照番号を指定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. Site-to-Site 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こともできます。

   に連絡するときは AWS サポート、参照番号を指定する必要があります。

Windows ベースの AWS 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

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。

AWS が提供するクライアントイベントログ

AWS 提供されたクライアントは、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 提供されたクライアントは 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
```

トラブルシューティングのトピック

- クライアントが接続できない
- 「TAP-Windows アダプタがありません」というログメッセージが表示されて、クライアントが接続できない
- 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に終了する
- 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
- VPN が切断され、ポップアップメッセージが出る

- Windows 10または11を使用している Dell PC でクライアントのクラッシュが発生する
- OpenVPN GUI
- OpenVPN 接続クライアント
- DNS を解決できない
- PKI エイリアスがない

クライアントが接続できない

問題

AWS 指定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 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。

ソリューション

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。

「TAP-Windows アダプタがありません」というログメッセージが表示されて、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ず、アプリケーションログに「このシステムに TAP-Windows アダプターはありません。[スタート] -> [すべてのプログラム] -> [TAP-Windows] -> [ユーティリティ] -> [新しい TAP-Windows 仮想イーサネットアダプタの追加] に移動すると、TAP-Windows アダプタを作成できます。

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 指定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、再接続状態のままです。

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。

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、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。VPN クライアントウィンドウで切断を選択して AWS VPN セッションを切断し、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に終了する

問題

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

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を再実行して、必要なすべての依存関係を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、クライアントを開いても、 AWS 提供されたクライアントは起動しません。

原因

.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。

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を再実行して、必要なすべての依存関係を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) ファイルにクライアント証明書とキーは含まれていません。

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。

VPN が切断され、ポップアップメッセージが出る

問題

VPN が切断され、以下のポップアップメッセージが出ます。「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たため、VPN 接続は終了しました。新しい VPN 接続を確立してください。」

原因

TAP-Windows アダプタには、必要な説明は含まれていません。

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
```

Windows 10または11を使用している Dell PC でクライアントの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 PC (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こと

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 DLLs と競合する可能性があります。

- 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 提供された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たく

ない場合は、別の方法として、DLL ファイルを削除するか、名前を変更することもできます。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 ファイルを削除するか、名前を変更します。

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

   ファイル名の末尾に「.bak」を追加することで、ファイルの名前を変更できます。例えば、dbroverlayiconbackuped.dll.bak。

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

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。

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 エイリアスがない

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 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。

ソリューション

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 AWS 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。

AWS が提供するクライアントイベントログ

AWS 提供されたクライアントは、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 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。

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

トラブルシューティングのトピック

- クライアントが接続できない
- クライアントが再接続状態でスタックしている
- クライアントがプロファイルを作成できない
- 「ヘルパーツールは必須です」エラー
- Tunnelblick
- 暗号アルゴリズム「AES-256-GCM」が見つからない
- 接続が応答を停止し、リセットされます。
- 拡張キー使用法 (EKU)
- 証明書が失効している
- OpenVPN
- DNS を解決できない

クライアントが接続できない

問題

AWS 指定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 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。

ソリューション

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

問題

AWS 指定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、再接続状態のままです。

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。

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、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。VPN クライアントウィンドウで切断を選択して AWS VPN セッションを切断し、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) ファイルにクライアント証明書とキーは含まれていません。

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

VPN に接続しようとすると、次のエラーが発生します。

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

ソリューション

AWS re:Post の次の記事を参照してください。AWS VPN Client - Helper tool is required error

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、[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」が見つからない

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-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。

ソリューション

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。

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要求します。

拡張キー使用法 (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。

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

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

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 接続はクライアント VPN DNS 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 AWS クライアントを使用したクライアント 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イベントログ
- DNS クエリはデフォルトのネームサーバーに移動します
- OpenVPN (コマンドライン)
- Network Manager (GUI) を介した OpenVPN

AWS が提供するクライアントイベントログ

AWS 提供されたクライアントは、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 提供されたクライアントデーモンプロセスは、システム上の次の場所にログファイルを保存します。

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

例えば、次のログファイルをチェックして、接続が失敗する原因となる DNS アップ/ダウンスクリプトのエラーを見つけることができます。

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

DNS クエリはデフォルトのネームサーバーに移動します

問題

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。

原因

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。

ソリューション

1. OpenVPN 設定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)

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

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

問題

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
```

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。

AWS クライアント VPN の一般的な問題のトラブルシューティング

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

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

次の表に、 AWS クライアント VPN ユーザーガイドの更新を示します。

変更	説明	日付
AWS が提供する Windows ARM64 および x64 用のクライアント (5.3.4) 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。	2026 年 3 月 26 日
AWS が提供する Windows ARM64 および x64 用のクライアント (5.3.3) 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。	2026 年 2 月 28 日
AWS macOS ARM64 および x64 用の 提供クライアント (5.3.4) 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。	2026 年 2 月 17 日
AWS が提供する Windows ARM64 および x64 用のクライアント (5.3.2) 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。	2026 年 2 月 17 日
AWS macOS ARM64 および x64 用の 提供クライアント (5.3.3) 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。	2025 年 12 月 26 日
AWS が提供する Ubuntu 用のクライアント (5.3.2) 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。	2025 年 12 月 17 日
AWS macOS x64 用の 提供クライアント (5.3.2) 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。	2025 年 10 月 27 日
AWS macOS ARM64 システム用に が提供するクライアント (5.3.2) をリリース	macOS ARM64 ベースのオペレーティングシステムのサポートが追加されました。これには、macOS ARM64 システム専用の AWS Client VPN	2025 年 10 月 27 日

	の新しいバージョンである 5.3.2 のダウンロードが含まれています。詳細については「macOS 向けクライアント VPN の要件」を、ダウンロードリンクについては「macOS 向けAWS Client VPN のリリースノート」を参照してください。	
AWS が提供する Windows x64 および Arm64 用のクライアント (5.3.1) 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。	2025 年 9 月 30 日
AWS macOS 用の が提供するクライアントが Tahoe (26.0) をサポートするようになりました	詳細については、「要件」を参照してください。	2025 年 9 月 25 日
AWS が提供する Ubuntu 用のクライアント (5.3.1) 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。	2025 年 9 月 25 日
AWS が提供する macOS 用クライアント (5.3.1) 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。	2025 年 9 月 9 日

AWS が提供する Windows Arm64 システム用のクライアント (5.3.0) をリリース	Windows Arm64 ベースのオペレーティングシステムのサポートが追加されました。これには、Windows Arm64 システム専用の AWS Client VPN の新しいバージョンである 5.3.0 のダウンロードが含まれます。詳細については「Windows 向けクライアント VPN の要件」を、ダウンロードリンクについては「Windows 向けAWS Client VPN のリリースノート」を参照してください。	2025 年 8 月 26 日
AWS が提供する macOS 用クライアント (5.3.0) 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。	2025 年 8 月 14 日
AWS が提供する Windows 用クライアント (5.3.0) 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。	2025 年 8 月 14 日
AWS が提供する Ubuntu 用のクライアント (5.3.0) 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。	2025 年 8 月 14 日
AWS が提供する macOS 用クライアント (5.2.1) 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。	2025 年 6 月 18 日
AWS が提供する Windows 用クライアント (5.2.2) 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。	2025 年 6 月 2 日
AWS が提供する Windows 用クライアント (5.2.1) 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。	2025 年 4 月 21 日

AWS が提供する macOS 用クライアント (5.2.0) 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。	2025 年 4 月 8 日
AWS が提供する Windows 用クライアント (5.2.0) 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。	2025 年 4 月 8 日
AWS が提供する Ubuntu 用のクライアント (5.2.0) 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。	2025 年 4 月 8 日
AWS が提供する macOS 用クライアント (5.1.0) 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。	2025 年 3 月 17 日
AWS が提供する Windows 用クライアント (5.1.0) 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。	2025 年 3 月 17 日
AWS が提供する Ubuntu 用のクライアント (5.1.0) 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。	2025 年 3 月 17 日
macOS Monterey のサポートを削除し、macOS Sonoma (14.0) のサポートを追加	詳細については、「macOS 向けクライアント VPN の要件」を参照してください。	2025 年 3 月 12 日
Ubuntu 18.0.4 (LTS) と Ubuntu 20.04 LTS (AMD64 のみ) の両方のサポートを削除	詳細については、「Linux 向けクライアント VPN の要件」を参照してください。	2025 年 3 月 12 日
AWS が提供する macOS 用クライアント (5.0.3) 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。	2025 年 3 月 6 日
AWS が提供する Windows 用クライアント (5.0.2) 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。	2025 年 2 月 24 日
AWS が提供する macOS 用クライアント (5.0.2) 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。	2025 年 2 月 17 日

AWS が提供する Windows 用クライアント (5.0.1) 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。	2025 年 1 月 30 日
AWS が提供する macOS 用クライアント (5.0.1) 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。	2025 年 1 月 22 日
AWS 提供されたクライアントが最大 5 つの同時接続をサポートするようになりました	詳細については、AWS「が提供するクライアントを使用した同時接続のサポート」を参照してください。	2025 年 1 月 21 日
AWS が提供する macOS 用クライアント (5.0.0) 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。	2025 年 1 月 21 日
AWS が提供する Windows 用クライアント (5.0.0) 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。	2025 年 1 月 21 日
AWS が提供する Ubuntu 用のクライアント (5.0.0) 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。	2024 年 11 月 12 日
AWS が提供する macOS 用クライアント (4.1.0) 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。	2024 年 11 月 12 日
AWS が提供する Windows 用クライアント (4.1.0) 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。	2024 年 11 月 12 日
AWS が提供する Ubuntu 用のクライアント (4.1.0) 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。	2024 年 11 月 12 日
AWS が提供する macOS 用クライアント (4.0.0) 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。	2024 年 9 月 25 日

AWS が提供する Windows 用クライアント (4.0.0) 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。	2024 年 9 月 25 日
AWS が提供する Ubuntu 用のクライアント (4.0.0) 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。	2024 年 9 月 25 日
AWS が提供する Ubuntu 用のクライアント (3.15.1) 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 9 月 4 日
AWS が提供する Windows 用クライアント (3.14.2) 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 9 月 4 日
AWS が提供する macOS 用クライアント (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 9 月 4 日
AWS が提供する Windows 用クライアント (3.14.1) 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 8 月 22 日
AWS が提供する Ubuntu 用のクライアント (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 用クライアント (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 用のクライアント (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 用クライアント (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 用クライアント (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 用クライアント (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 用のクライアント (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 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 5 月 21 日
AWS が提供する macOS 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。	2024 年 5 月 21 日
AWS が提供する macOS 用クライアント (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 用のクライアント (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 用のクライアント (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 用のクライアント (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 用クライアント (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 用クライアント (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 用のクライアント (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 用のクライアント (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 用のクライアント (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 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 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 用クライアント (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 用のクライアント (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 用クライアント (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 用クライアント (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 用のクライアント (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 用のクライアント (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 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 14 日

AWS が提供する Ubuntu 用のクライアント (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 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 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 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 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 用のクライアント (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 用クライアント (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 用クライアント (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 用クライアント (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 用クライアント (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 用のクライアント (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 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 Ubuntu 用のクライアント (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 用クライアント (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 用クライアント (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 用のクライアント (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 用クライアント (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) 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 用のクライアント (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 用のクライアント (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 LTS 用のクライアントをリリース	AWSが提供するクライアントは、Ubuntu 18.04 LTS および 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 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 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。	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 VPN が導入されました。	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。