管理者ガイド

AWS クライアント VPN

AWS クライアント VPN: 管理者ガイド

Table of Contents

AWS クライアント VPN とは

AWS クライアント VPN は、オンプレミスネットワーク内の AWS リソースとリソースに安全にアクセスできるマネージドクライアントベースの VPN サービスです。クライアント VPN を使用すると、OpenVPN ベースの VPN クライアントを使用して、どこからでもリソースにアクセスできます。

目次

クライアント VPN の機能

クライアント VPN には、以下の機能があります。

- 安全な接続 — OpenVPN クライアントを使用して、あらゆる場所から安全な TLS 接続を提供します。
- マネージドサービス — AWS マネージドサービスであるため、サードパーティーのリモートアクセス VPN ソリューションをデプロイして管理する運用上の負担が軽減されます。
- 高可用性と伸縮性 — AWS リソースとオンプレミスリソースに接続するユーザーの数に自動的にスケーリングされます。
- 認証 — Active Directory を使用したクライアント認証、フェデレーション認証、および証明書ベースの認証がサポートされます。
- きめ細かい制御 — ネットワークベースのアクセスルールを定義することで、カスタムセキュリティ管理を実装できます。これらのルールは、Active Directory グループの詳細度で設定できます。セキュリティグループを使用してアクセス制御を実装することもできます。
- 使いやすさ — 単一の VPN トンネルを使用して AWS リソースとオンプレミスリソースにアクセスできます。

- 管理性 — クライアントの接続試行に関する詳細を提供する接続ログを表示できます。アクティブなクライアント接続を終了する機能で、アクティブなクライアント接続を管理することもできます。
- ディープインテグレーション — や Amazon VPC などの既存の AWS サービスと統合 AWS Directory Service されます。

クライアント VPN のコンポーネント

クライアント VPN の主な概念は次のとおりです。

クライアント VPN エンドポイント

クライアント VPN エンドポイントは、クライアント VPN セッションを有効にして管理するために作成して設定するリソースです。これは、すべてのクライアント VPN セッションの終了ポイントです。

ターゲットネットワーク

ターゲットネットワークは、クライアント VPN エンドポイントに関連付けるネットワークです。VPC からのサブネットはターゲットネットワークです。サブネットをクライアント VPN エンドポイントに関連付けると、VPN セッションを確立できます。高可用性を実現するために、複数のサブネットをクライアント VPN エンドポイントに関連付けることができます。すべてのサブネットは同一の VPC に存在する必要があります。各サブネットは異なるアベイラビリティーゾーンに属している必要があります。

ルート

各クライアント VPN エンドポイントには、利用可能な送信先ネットワークルートを説明したルートテーブルがあります。ルートテーブル内の各ルートは、特定のリソースまたはネットワークへのトラフィックのパスを指定します。

承認ルール

承認ルールは、ネットワークにアクセスできるユーザーを制限します。指定のネットワークに対して、アクセスを許可する Active Directory または ID プロバイダー (IdP) グループを構成します。このグループに属するユーザーだけが、指定のネットワークにアクセスできます。デフォルトでは承認ルールはありません。ユーザーがリソースやネットワークにアクセスできるように承認ルールを設定する必要があります。

クライアント

VPN セッションを確立するためにクライアント VPN エンドポイントに接続するエンドユーザー。エンドユーザーは、OpenVPN クライアントをダウンロードし、作成した Client VPN 設定ファイルを使用して VPN セッションを確立する必要があります。

クライアント CIDR 範囲

クライアント IP アドレスの割り当て元となる IP アドレスの範囲。クライアント VPN エンドポイントへの各接続には、クライアント CIDR 範囲から固有の IP アドレスが割り当てられます。クライアント CIDR 範囲を選択します (例: `10.2.0.0/16`)。

クライアント VPN ポート

AWS クライアント VPN は、TCP と UDP の両方でポート 443 と 1194 をサポートします。デフォルトはポート 443 です。

クライアント VPN ネットワークインターフェイス

サブネットをクライアント VPN エンドポイントに関連付けると、そのサブネットにクライアント VPN ネットワークインターフェイスが作成されます。クライアント VPN エンドポイントから VPC に送信されるトラフィックは、クライアント VPN ネットワークインターフェイスを介して送信されます。次に、ソースネットワークアドレス変換 (SNAT) が適用され、クライアント CIDR 範囲からのソース IP アドレスがクライアント VPN ネットワークインターフェイス IP アドレスに変換されます。

接続ログ

クライアント VPN エンドポイントの接続ログを有効にして、接続イベントをログに記録できます。この情報を使用してフォレンジックを実行したり、クライアント VPN エンドポイントがどのように使用されているかを分析したり、接続の問題をデバッグしたりできます。

セルフサービスポータル

クライアント VPN は、エンドユーザーが AWS VPN Desktop 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するためのウェブページとなるセルフサービスポータルです。このファイルには、エンドポイントへの接続に必要な設定が含まれています。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有効または無効にすることができます。セルフサービスポータルは、米国東部 (バージニア北部) 、アジアパシフィック (東京) 、欧州 (アイルランド) 、 AWS GovCloud および (米国西部) の各リージョンのサービススタックに支えられたグローバルサービスです。

クライアント VPN の使用

クライアント VPN は、次のいずれかの方法で使用できます。

AWS Management Console

コンソールは、クライアント VPN 用のウェブベースのユーザーインターフェイスを提供します。にサインアップしている場合は AWS アカウント、Amazon VPC コンソールにサインインし、ナビゲーションペインでクライアント VPN を選択できます。

AWS Command Line Interface (AWS CLI)

AWS CLI は、クライアント VPN パブリック APIs。Windows、macOS、Linux でサポートされています。の使用開始の詳細については AWS CLI、「AWS Command Line Interface ユーザーガイド」を参照してください。クライアント VPN のコマンドの詳細については、AWS CLI コマンドリファレンスを参照してください。

AWS Tools for Windows PowerShell

AWS は、 PowerShell 環境でスクリプトを作成するユーザー向けに、幅広い AWS 製品セットのコマンドを提供します。 AWS Tools for Windows PowerShellの使用開始に関する詳細については、「AWS Tools for Windows PowerShell ユーザーガイド」を参照してください。クライアント VPN のコマンドレットの詳細については、「AWS Tools for Windows PowerShell コマンドレットリファレンス」を参照してください。

クエリ API

クライアント VPN HTTPS クエリ API は、クライアント VPN と へのプログラムによるアクセスを提供します AWS。HTTPS クエリ API を使用すると、HTTPS リクエストを直接サービスに発行できます。HTTPS API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、「AWS Client VPN アクション」を参照してください。

クライアント VPN の料金

それぞれのエンドポイントアソシエーションと各 VPN 接続について、時間単位で課金されます。詳細については、「AWS Client VPN 料金表」を参照してください。

Amazon EC2 からインターネットへのデータ転送に対して課金されます。詳細については、「Amazon EC2 オンデマンド料金」ページの「データ転送」を参照してください。

クライアント VPN エンドポイントの接続ログ記録を有効にする場合は、アカウントに CloudWatch ロググループを作成する必要があります。ロググループの使用には料金がかかります。詳細については、「Amazon の CloudWatch 料金」(「有料利用枠」で「ログ」を選択します) を参照してください。

クライアント VPN エンドポイントでクライアント接続ハンドラーを有効にする場合は、Lambda 関数を作成して呼び出す必要があります。Lambda 関数の呼び出しには料金がかかります。詳細については、「AWS Lambda 料金表」を参照してください。

クライアント VPN エンドポイントは、VPC 内のサブネットであるターゲットネットワークに関連付けられます。この VPC にインターネットゲートウェイがある場合、Elastic IP アドレスをクライアント VPN の Elastic Network Interface (ENIs。これらの Elastic IP アドレスは、使用中のパブリック IPv4 アドレスとして課金されます。詳細については、「VPC 料金表」ページの「パブリック IPv4 アドレス」タブを参照してください。

のルールとベストプラクティス AWS Client VPN

のルールとベストプラクティスは次のとおりです。 AWS Client VPN

- ユーザー接続ごとに 10 Mbps の最小帯域幅がサポートされています。ユーザー接続あたりの最大帯域幅は、クライアント VPN エンドポイントに対して行われる接続の数によって異なります。
- クライアント CIDR 範囲は、関連付けられたサブネットが配置されている VPC のローカル CIDR、またはクライアント VPN エンドポイントのルートテーブルに手動で追加されたルートと重複することはできません。
- クライアント CIDR 範囲は、ブロックサイズが /22 以上、/12 以下でなければなりません。
- クライアント CIDR 範囲内のアドレスの一部は、クライアント VPN エンドポイントの可用性モデルをサポートするために使用され、クライアントに割り当てることはできません。したがって、クライアント VPN エンドポイントでサポートする予定の同時接続の最大数を有効にするために必要な IP アドレスの数の 2 倍の数を含む CIDR ブロックを割り当てることをお勧めします。
- クライアント VPN エンドポイントの作成後にクライアント CIDR 範囲を変更することはできません。
- クライアント VPN エンドポイントに関連付けられているサブネットは、同じ VPC 内にある必要があります。
- 1 つのアベイラビリティーゾーンの複数のサブネットをクライアント VPN エンドポイントに関連付けることはできません。
- クライアント VPN エンドポイントは、専有テナント VPC でのサブネットの関連付けをサポートしていません。

- クライアント VPN は、IPv4 トラフィックのみをサポートしています。IPv6 の詳細については、「AWS クライアント VPN の IPv6 に関する考慮事項」を参照してください。
- クライアント VPN は、連邦情報処理規格 (FIPS) に準拠していません。
- セルフサービスポータルは、相互認証を使用して認証するクライアントでは利用できません。
- IP アドレスを使用して、クライアント VPN エンドポイントに接続することはお勧めしません。クライアント VPN はマネージドサービスであるため、DNS 名が解決する IP アドレスに変化が見られる場合があります。さらに、クライアント VPN ネットワークインターフェイスが削除され、CloudTrail ログに再作成されます。クライアント VPN エンドポイントへの接続には、提供された DNS 名を使用することをお勧めします。
- AWS Client VPN デスクトップアプリケーションを使用する場合、IP 転送は現在サポートされていません。IP 転送は他のクライアントからもサポートされています。
- クライアント VPN は、 AWS Managed Microsoft ADでのマルチリージョンレプリケーションをサポートしていません。クライアント VPN エンドポイントは、 AWS Managed Microsoft AD リソースと同じリージョンに存在する必要があります。
- Active Directory で多要素認証 (MFA) が無効になっている場合、ユーザーパスワードで次の形式を使用することはできません。

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- オペレーティングシステムに複数のユーザーがログインしている場合、このコンピュータから VPN 接続を確立することはできません。
- クライアント VPN サービスでは、クライアントが接続されている IP アドレスが、クライアント VPN エンドポイントの DNS 名が解決される IP と一致する必要があります。つまり、クライアント VPN エンドポイントにカスタム DNS レコードを設定し、エンドポイントの DNS 名が解決する実際の IP アドレスにトラフィックを転送すると、この設定は最近の AWSが提供するクライアントでは機能しません。このルールは、「」で説明されているように、サーバー IP 攻撃を軽減するために追加されましたTunnelCrack。
- クライアント VPN サービスでは、クライアントデバイスのローカルエリアネットワーク (LAN) IP アドレス範囲が、10.0.0.0/8、、172.16.0.0/12192.168.0.0/16、または の標準プライベート IP アドレス範囲内にある必要があります169.254.0.0/16。クライアント LAN アドレス範囲が上記の範囲外であることが検出された場合、クライアント VPN エンドポイントは OpenVPN ディレクティブ「redirect-gateway block-local」をクライアントに自動的にプッシュし、すべての LAN トラフィックを VPN に強制します。したがって、VPN 接続中に LAN アクセスが必要な場合は、上記の従来のアドレス範囲を LAN に使用することをお勧めします。このルー

ルは、「」で説明されているように、ローカルネット攻撃の可能性を軽減するために適用されますTunnelCrack。

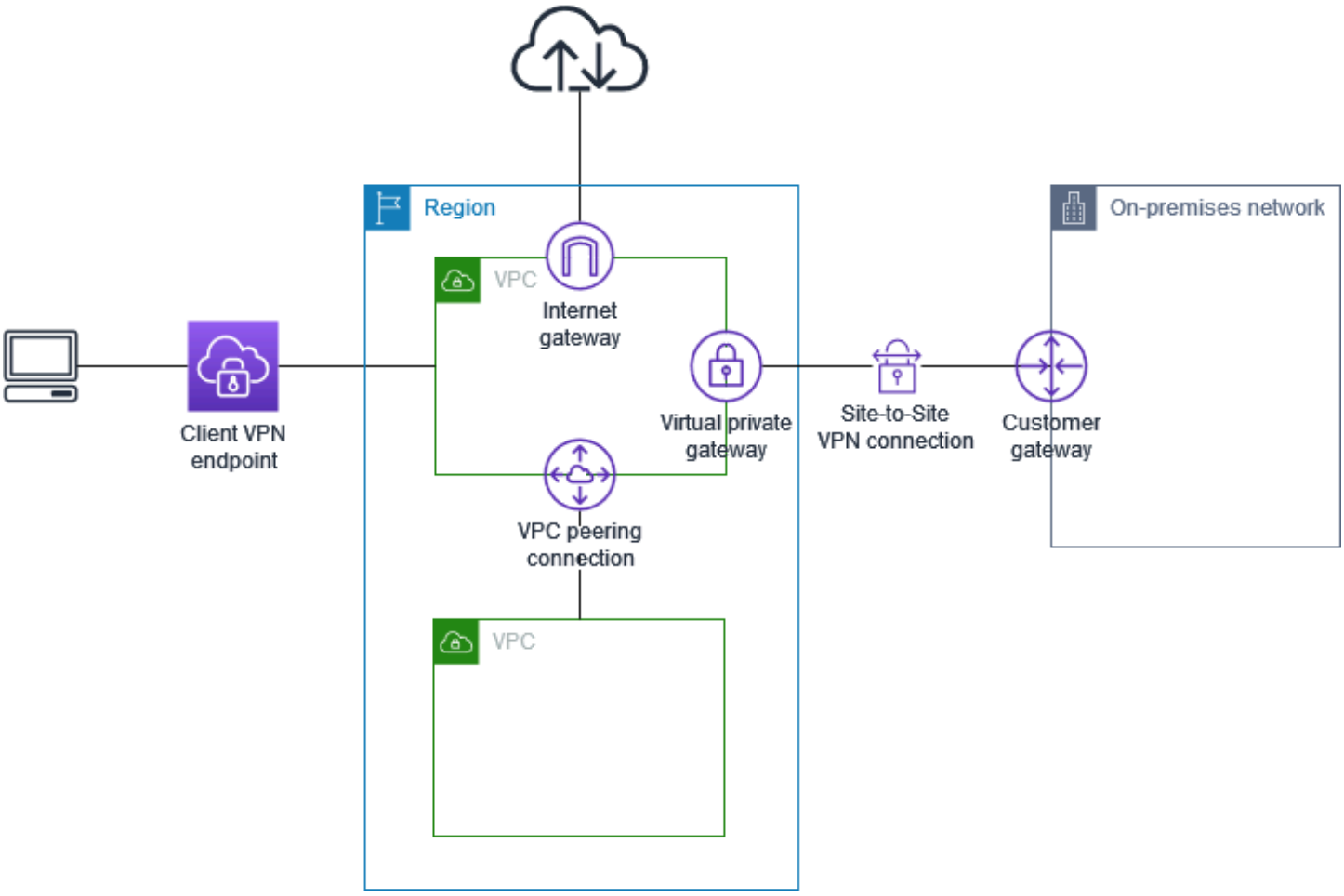
AWS クライアント VPN の仕組み

AWS クライアント VPN には、クライアント VPN エンドポイントの管理者およびクライアントとやり取りする 2 つのタイプのユーザーがいます。

管理者は、サービスの設定と設定を担当します。このプロセスには、クライアント VPN エンドポイントの作成、ターゲットネットワークの関連付け、認証ルールの設定、および追加のルート (必要な場合) の設定が含まれます。クライアント VPN エンドポイントを設定した後、管理者はクライアント VPN エンドポイント設定ファイルをダウンロードして、アクセスが必要なクライアントに配布します。クライアント VPN エンドポイント設定ファイルには、クライアント VPN エンドポイントの DNS 名と、VPN セッションを確立するために必要な認証情報が含まれています。サービス設定の詳細については、「AWS クライアント VPN の開始方法」を参照してください。

クライアントはエンドユーザーです。これは、VPN セッションを確立するためにクライアント VPN エンドポイントに接続する人です。クライアントは OpenVPN ベースの VPN クライアントアプリケーションを使用して、ローカルコンピュータまたはモバイルデバイスから VPN セッションを確立します。VPN セッションが確立されたら、関連付けられているサブネットが存在する VPC のリソースに安全にアクセスできます。必要なルートと認証ルールが設定されている場合は、AWS、オンプレミスネットワーク、または他のクライアントの他のリソースにもアクセスできます。VPN セッションを確立するためのクライアント VPN エンドポイントへの接続の詳細については、AWS クライアント VPN ユーザーガイドの「開始方法」を参照してください。

次の図は、基本的なクライアント VPN アーキテクチャを示しています。



クライアント承認

クライアント認証は、 AWS クラウドへの最初のエントリポイントで実装されます。クライアントがクライアント VPN エンドポイントへの接続を許可されているかどうかを判断するために使用されます。認証が成功すると、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て VPN セッションを確立します。認証が失敗すると、接続は拒否され、クライアントは VPN セッションを確立できなくなります。

クライアント VPN では、次のタイプのクライアント承認を使用できます。

- Active Directory 認証 (ユーザーベース)
- 相互認証 (証明書ベース)
- シングルサインオン (SAML ベースのフェデレーション認証) (ユーザーベース)

上記の方法のいずれかを単独で使用することも、次のようなユーザーベースの方法との相互認証を組み合わせて使用することもできます。

- 相互認証とフェデレーション認証
- 相互認証と Active Directory 認証

> **Important**
>
> クライアント VPN エンドポイントを作成するには、使用する認証のタイプに関係なく AWS Certificate Manager、 でサーバー証明書をプロビジョニングする必要があります。サーバー証明書の作成とプロビジョニングの詳細については、「相互認証」の手順を参照してください。

Active Directory 認証

クライアント VPN は、 と統合することで Active Directory サポートを提供します AWS Directory Service。Active Directory 認証では、クライアントは既存の Active Directory グループに対して認証されます。を使用すると AWS Directory Service、クライアント VPN は AWS またはオンプレミスネットワークでプロビジョニングされた既存の Active Directory に接続できます。これにより、既存のクライアント承認インフラストラクチャを使用することができます。オンプレミスの Active Directory を使用していて、既存の AWS Managed Microsoft AD がない場合は、Active Directory Connector (AD Connector) を設定する必要があります。1 つの Active Directory サーバーを使用してユーザーを認証できます。Active Directory 統合の詳細については、AWS Directory Service 管理ガイドを参照してください。

クライアント VPN は、 AWS Managed Microsoft AD または AD Connector で有効になっている場合、多要素認証 (MFA) をサポートします。MFA が有効になっている場合、クライアントはクライアント VPN エンドポイントに接続するときにユーザー名、パスワード、および MFA コードを入力する必要があります。MFA を有効にする詳細については、AWS Directory Service 管理ガイドの「AWS Managed Microsoft AD の多要素認証を有効にするには」および「AD Connector の多要素認証を有効にするには」を参照してください。

Active Directory でユーザーとグループを設定するためのクォータとルールについては、「ユーザーとグループのクォータ」を参照してください。

相互認証

相互認証では、クライアント VPN は証明書を使用してクライアントとサーバー間の認証を実行します。証明書とは、認証機関 (CA) によって発行された識別用デジタル形式です。クライアントがクライアント VPN エンドポイントに接続を試みると、サーバーはクライアント証明書を使用してクライアントを認証します。サーバー証明書とキー、および少なくとも 1 つのクライアント証明書とキーを作成する必要があります。

サーバー証明書を AWS Certificate Manager (ACM) にアップロードし、クライアント VPN エンドポイントを作成するときに指定する必要があります。サーバー証明書を ACM にアップロードするときは、認証局 (CA) も指定します。クライアント証明書を ACM にアップロードする必要があるのは、クライアント証明書の CA がサーバー証明書の CA と異なる場合だけです。ACM の詳細については、AWS Certificate Manager ユーザーガイドを参照してください。

クライアント VPN エンドポイントに接続するクライアントごとに、個別のクライアント証明書とキーを作成できます。これにより、ユーザーが組織を離れた場合に、特定のクライアント証明書を取り消すことができます。この場合、クライアント VPN エンドポイントを作成するときに、クライアント証明書がサーバー証明書と同じ CA によって発行されていれば、クライアント証明書のサーバー証明書 ARN を指定できます。

> **Note**
>
> クライアント VPN エンドポイントは、1024 ビットおよび 2048 ビットの RSA キーサイズのみサポートしています。また、クライアント証明書の [Subject (件名)] フィールドに CN 属性が含まれている必要があります。
> クライアント VPN サービスで使用している証明書を、ACM の自動ローテーション、新しい証明書の手動インポート、または IAM Identity Center へのメタデータの更新により更新すると、クライアント VPN サービスはクライアント VPN エンドポイントをより新しい証明書で自動更新します。これは、最長で 24 時間かかることがある自動プロセスです。

Linux/macOS

次の手順では、OpenVPN easy-rsa を使用してサーバーとクライアントの証明書とキーを生成してから、そのサーバーの証明書とキーを ACM にアップロードします。詳細については、「Easy-RSA 3 Quickstart README」を参照してください。

サーバーとクライアントの証明書とキーを生成し、それらを ACM にアップロードするには

1. OpenVPN easy-rsa リポジトリのクローンをローカルコンピュータに作成して、easy-rsa/easyrsa3 フォルダに移動します。

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. 新しい PKI 環境を初期化します。

```
$ ./easyrsa init-pki
```

3. 新しい認証局 (CA) を構築するには、このコマンドを実行し、プロンプトに従います。

```
$ ./easyrsa build-ca nopass
```

4. サーバー証明書とキーを生成します。

```
$ ./easyrsa --san=DNS:server build-server-full server nopass
```

5. クライアント証明書とキーを生成します。

   クライアント証明書とクライアントプライベートキーは、クライアントを設定するときに必要になるため、必ず保存してください。

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

   必要に応じて、クライアント証明書とキーを必要とするクライアント (エンドユーザー) ごとにこの手順を繰り返すことができます。

6. サーバー証明書とキー、およびクライアント証明書とキーをカスタムフォルダにコピーしてから、カスタムフォルダに移動します。

   証明書とキーをコピーする前に、mkdir コマンドを使用してカスタムフォルダを作成します。次の例では、ホームディレクトリにカスタムフォルダを作成します。

```
$ mkdir ~/custom_folder/
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
```

```
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. サーバー証明書とキー、およびクライアント証明書とキーを ACM にアップロードします。必ずクライアント VPN エンドポイントを作成する予定のリージョンと同じリージョンにアップロードしてください。以下のコマンドは、 AWS CLI を使用して証明書をアップロードします。代わりに ACM コンソールを使用して証明書をアップロードするには、AWS Certificate Manager ユーザーガイドの「証明書のインポート」を参照してください。

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

クライアント証明書を ACM にアップロードする必要はありません。サーバー証明書とクライアント証明書が同じ認証機関 (CA) によって発行されている場合、Client VPN エンドポイントを作成するときに、サーバーとクライアントの両方に対してサーバー証明書 ARN を使用することができます。上のステップで、同じ CA を使用して両方の証明書を作成しています。ただし、完全性を保証するために、クライアント証明書をアップロードするステップが含まれています。

Windows

次の手順では、Easy-RSA 3.x ソフトウェアをインストールし、それを使用してサーバーとクライアントの証明書およびキーを生成します。

サーバーとクライアントの証明書とキーを生成し、それらを ACM にアップロードするには

1. EasyRSA リリースページを開き、お使いの Windows のバージョン用の ZIP ファイルをダウンロードして抽出します。
2. コマンドプロンプトを開き、EasyRSA-3.x フォルダが抽出された場所に移動します。
3. 次のコマンドを実行して、EasyRSA 3 シェルを開きます。

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. 新しい PKI 環境を初期化します。

```
# ./easyrsa init-pki
```

5. 新しい認証局 (CA) を構築するには、このコマンドを実行し、プロンプトに従います。

```
# ./easyrsa build-ca nopass
```

6. サーバー証明書とキーを生成します。

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. クライアント証明書とキーを生成します。

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

必要に応じて、クライアント証明書とキーを必要とするクライアント (エンドユーザー) ごとにこの手順を繰り返すことができます。

8. EasyRSA 3 シェルを終了します。

```
# exit
```

9. サーバー証明書とキー、およびクライアント証明書とキーをカスタムフォルダにコピーしてから、カスタムフォルダに移動します。

証明書とキーをコピーする前に、mkdir コマンドを使用してカスタムフォルダを作成します。以下の例では、C:\ ドライブにカスタムフォルダを作成します。

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. サーバー証明書とキー、およびクライアント証明書とキーを ACM にアップロードします。必ずクライアント VPN エンドポイントを作成する予定のリージョンと同じリージョンにアップロードしてください。次のコマンドは AWS CLI 、 を使用して証明書をアップロー

ドします。代わりに ACM コンソールを使用して証明書をアップロードするには、AWS Certificate Manager ユーザーガイドの「証明書のインポート」を参照してください。

```
aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

クライアント証明書を ACM にアップロードする必要はありません。サーバー証明書とクライアント証明書が同じ認証機関 (CA) によって発行されている場合、Client VPN エンドポイントを作成するときに、サーバーとクライアントの両方に対してサーバー証明書 ARN を使用することができます。上のステップで、同じ CA を使用して両方の証明書を作成しています。ただし、完全性を保証するために、クライアント証明書をアップロードするステップが含まれています。

サーバー証明書の更新

有効期限が切れたサーバー証明書を更新して再インポートできます。使用している OpenVPN easy-rsa のバージョンに応じて、手順は異なります。詳細については、「Easy-RSA 3 証明書の更新と取り消しのドキュメント」を参照してください。

サーバー証明書の更新

1. 次のいずれかを実行します。
   - Easy-RSA バージョン 3.1.x
     - 証明書更新コマンドを実行します。

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA バージョン 3.2.x
     a. 期限切れコマンドを実行します。

        ```
        $ ./easyrsa expire server
        ```
     b. 新しい証明書に署名します。

```
$ ./easyrsa sign-req server server
```

2. カスタムフォルダを作成し、そのフォルダに新しいファイルをコピーして、フォルダに移動します。

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. 新しいファイルを ACM にインポートします。必ずクライアント VPN エンドポイントと同じリージョンにインポートしてください。

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

シングルサインオン (SAML 2.0 ベースのフェデレーション認証)

AWS Client VPN は、クライアント VPN エンドポイントの Security Assertion Markup Language 2.0 (SAML 2.0) との ID フェデレーションをサポートします。SAML 2.0 をサポートする ID プロバイダー (IdPs) を使用して、一元化されたユーザー ID を作成できます。その後、SAML ベースのフェデレーション認証が使用されるようにクライアント VPN エンドポイントを設定し、IdP に関連付けることができます。その後、ユーザーは、一元化された認証情報を使用してクライアント VPN エンドポイントに接続します。

SAML ベースの IdP をクライアント VPN エンドポイントに使用するには、次の操作を行う必要があります。

1. 選択した IdP に SAML ベースのアプリを作成して で使用するか AWS Client VPN、既存のアプリを使用します。
2. との信頼関係を確立するために IdP を設定します AWSリソースについては、「SAML ベースの IdP 設定リソース」を参照してください。
3. IdP で、組織を IdP として定義するフェデレーションメタデータドキュメントを生成し、ダウンロードします。この署名付き XML ドキュメントは、 AWS と IdP 間の信頼関係を確立するために使用されます。

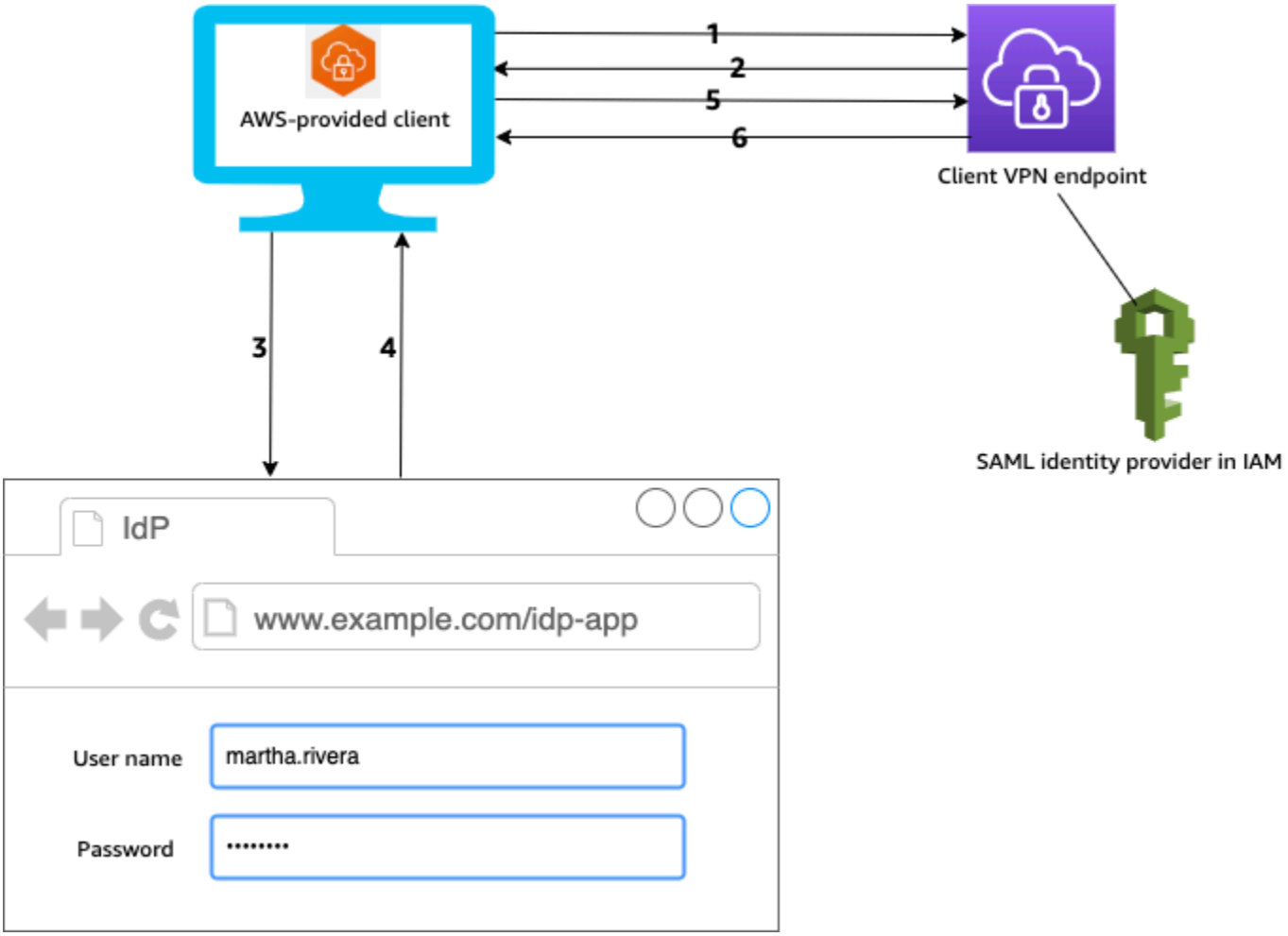
4. クライアント VPN エンドポイントと同じ AWS アカウントに IAM SAML ID プロバイダーを作成します。IAM SAML ID プロバイダーは、IdP によって生成されたメタデータドキュメントを使用して、組織の IdP とAWS 信頼の関係を定義します。詳細については、IAM ユーザーガイドの「SAML ID プロバイダーの作成」を参照してください。後で IdP のアプリ設定を更新する場合は、新しいメタデータドキュメントを生成し、IAM SAML ID プロバイダーを更新します。

   > **Note**
   >
   > IAM SAML ID プロバイダーを使用するために IAM ロールを作成する必要はありません。

5. クライアント VPN エンドポイントを作成します。認証タイプとしてフェデレーション認証を指定し、作成した IAM SAML ID プロバイダーを指定します。詳細については、「クライアント VPN エンドポイントを作成する」を参照してください。
6. クライアント設定ファイルをエクスポートし、ユーザーに配布します。AWS が提供するクライアントの最新バージョンをダウンロードし、これを使用して設定ファイルをロードして、クライアント VPN エンドポイントに接続するようにユーザーに指示します。または、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有効にした場合は、セルフサービスポータルに移動して設定ファイルと AWS 提供されたクライアントを取得するようにユーザーに指示します。詳細については、「セルフサービスポータルにアクセスする」を参照してください。

認証ワークフロー

次の図に、SAML ベースのフェデレーション認証を使用するクライアント VPN エンドポイントの認証ワークフローの概要を示します。クライアント VPN エンドポイントを作成および設定するときは、IAM SAML ID プロバイダーを指定します。



1. ユーザーは AWS 、提供されたクライアントをデバイスで開き、クライアント VPN エンドポイントへの接続を開始します。
2. クライアント VPN エンドポイントは、IAM SAML ID プロバイダーで提供された情報に基づいて IdP URL と認証リクエストをクライアントに送信します。
3. AWS 提供されたクライアントは、ユーザーのデバイスで新しいブラウザウィンドウを開きます。ブラウザは IdP にリクエストを送信し、ログインページを表示します。
4. ユーザーがログインページに認証情報を入力し、IdP は署名付き SAML アサーションをクライアントに返します。
5. AWS 提供されたクライアントは、SAML アサーションをクライアント VPN エンドポイントに送信します。
6. クライアント VPN エンドポイントはアサーションを検証し、ユーザーへのアクセスを許可または拒否します。

SAML ベースのフェデレーション認証の要件と考慮事項

SAML ベースのフェデレーション認証の要件と考慮事項を次に示します。

- SAML ベースの IdP でユーザーとグループを設定するためのクォータとルールについては、「ユーザーとグループのクォータ」を参照してください。
- SAML アサーションと SAML ドキュメントには署名が必要です。
- AWS Client VPN は、SAML アサーションのAudienceRestriction「」およびNotBefore NotOnOrAfter「」条件のみをサポートします。
- SAML 応答でサポートされる最大サイズは 128 KB です。
- AWS Client VPN は、署名付き認証リクエストを提供しません。
- SAML シングルログアウトはサポートされていません。ユーザーは、 AWS 提供されたクライアントから切断してログアウトすることも、接続を終了することもできます。
- 1 つのクライアント VPN エンドポイントでサポートされるのは、単一の IdP のみです。
- IdP で有効になっている場合は Multi-Factor Authentication (MFA) がサポートされます。
- ユーザーは、 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する必要があります。バージョン 1.2.0 以降を使用する必要があります。詳細については、AWS 「提供されたクライアント を使用して接続する」を参照してください。
- IdP 認証は、Apple Safari、Google Chrome、Microsoft Edge、Mozilla Firefox の各ブラウザでサポートされています。
- AWS が提供するクライアントは、SAML レスポンスのためにユーザーのデバイスに TCP ポート 35001 を予約します。
- 正しくない URL または悪意のある URL で IAM SAML ID プロバイダーのメタデータドキュメントが更新されると、ユーザーの認証の問題が発生したり、フィッシング攻撃につながる可能性があります。このため、IAM SAML ID プロバイダーに対して行われる更新は、 AWS CloudTrail を使用してモニタリングすることをお勧めします。詳細については、IAM ユーザーガイドの「AWS CloudTrailを使用した IAM および AWS STS 呼び出しのログ記録」を参照してください。
- AWS Client VPN は、HTTP リダイレクトバインディングを介して IdP に AuthN リクエストを送信します。このため、HTTP リダイレクトバインディングが IdP でサポートされ、IdP のメタデータドキュメントに存在する必要があります。
- SAML アサーションでは、`NameID` 属性に E メールアドレス形式を使用する必要があります。

SAML ベースの IdP 設定リソース

次の表に、 での使用をテスト IdPs した SAML ベースと AWS Client VPN、IdP の設定に役立つリソースを示します。

IdP	リソース
Okta	SAML で AWS Client VPN ユーザーを認証する
Microsoft Azure Active Directory (Azure AD)	詳細については、Microsoft ドキュメントウェブサイトの「チュートリアル: Azure Active Directory シングルサインオン (SSO) と AWS ClientVPN の統合」を参照してください。
JumpCloud	での Single Sign On (SSO) AWS Client VPN
AWS IAM Identity Center	での認証と認可 AWS Client VPN のための IAM Identity Center の使用

アプリを作成するためのサービスプロバイダー情報

前の表に示されていない IdP を使用して SAML ベースのアプリケーションを作成するには、次の情報を使用して AWS Client VPN サービスプロバイダー情報を設定します。

- Assertion Consumer Service (ACS) URL: `http://127.0.0.1:35001`
- Audience URI: `urn:amazon:webservices:clientvpn`

IdP からの SAML レスポンスには、少なくとも 1 つの属性が含まれている必要があります。以下は属性の例です。

属性	説明
`FirstName`	ユーザーの名。
`LastName`	ユーザーの姓。
`memberOf`	ユーザーが属するグループ (複数も可)。

> **Note**
>
> `memberOf` 属性は、Active Directory または SAML IdP グループベースの承認ルールを使用する場合に必要です。また、属性は大文字と小文字を区別し、指定どおりに設定する必要があります。詳細については、「ネットワークベースの承認」と「承認ルール」を参照してください。

セルフサービスポータルのサポート

クライアント VPN エンドポイントでセルフサービスポータルを有効にした場合、ユーザーは SAML ベースの IdP 認証情報を使用してポータルにログインします。

IdP が複数の Assertion Consumer Service (ACS) URL をサポートしている場合は、次の ACS URL をアプリに追加します。

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

GovCloud リージョンでクライアント VPN エンドポイントを使用している場合は、代わりに次の ACS URL を使用します。同じ IDP アプリを使用して標準と GovCloud リージョンの両方を認証する場合は、両方の URLsを追加できます。

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

IdP が複数の ACS URL をサポートしていない場合は、以下を実行します。

1. IdP に追加の SAML ベースのアプリを作成し、次の ACS URL を指定します。

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. フェデレーションメタデータドキュメントを生成し、ダウンロードします。
3. クライアント VPN エンドポイントと同じ AWS アカウントに IAM SAML ID プロバイダーを作成します。詳細については、IAM ユーザーガイドの「SAML ID プロバイダーの作成」を参照してください。

> **Note**
>
> メインアプリ用に作成したプロバイダーに加えて、この IAM SAML ID プロバイダーを作成します。

4. クライアント VPN エンドポイントを作成し、作成した IAM SAML ID プロバイダーを両方指定します。

クライアント認可

クライアント VPN では 2 種類のクライアント認可がサポートされています。セキュリティグループとネットワークベースの承認 (承認ルールを使用) です。

セキュリティグループ

クライアント VPN エンドポイントを作成するときに、特定の VPC からセキュリティグループを指定して、クライアント VPN エンドポイントに適用できます。サブネットをクライアント VPN エンドポイントに関連付けると、VPC のデフォルトセキュリティグループが自動的に適用されます。クライアント VPN エンドポイントを作成した後で、セキュリティグループを変更できます。詳細については、「」を参照してくださいセキュリティグループをターゲットネットワークに適用する セキュリティグループはクライアント VPN ネットワークインターフェイスに関連付けられます。

アプリケーションのセキュリティグループにルールを追加して、関連付けに適用されたセキュリティグループからのトラフィックを許可することで、クライアント VPN ユーザーが VPC 内のアプリケーションにアクセスできるようにすることができます。

クライアント VPN エンドポイントセキュリティグループからのトラフィックを許可するルールを追加するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Security Groups] を選択します。
3. リソースまたはアプリケーションに関連付けられているセキュリティグループを選択し、[アクション]、[インバウンドルールの編集] の順に選択します。
4. [Add rule] を選択します。
5. [Type] で、[All traffic] を選択します。または、特定のタイプのトラフィック (SSH など) へのアクセスを制限することもできます。

[Source (ソース)] に、クライアント VPN エンドポイントのターゲットネットワーク (サブネット) に関連付けられているセキュリティグループの ID を指定します。

6. [Save Rules (ルールの保存)] を選択します。

逆に、関連付けに適用されたセキュリティグループを指定しないか、クライアント VPN エンドポイントセキュリティグループを参照するルールを削除することで、クライアント VPN ユーザーのアクセスを制限できます。必要なセキュリティグループルールは、設定する VPN アクセスの種類によっても異なる場合があります。詳細については、「」を参照してくださいAWS クライアント VPN のシナリオと例

VPC セキュリティグループの詳細については、Amazon VPC ユーザーガイドの「VPC のセキュリティグループ」を参照してください。

ネットワークベースの承認

ネットワークベースの承認は承認ルールを使用して実装されます。アクセスを有効にするネットワークごとに、アクセス権を持つユーザーを制限する承認ルールを設定する必要があります。指定のネットワークに対して、アクセスを許可する Active Directory グループまたは SAML ベースの IdP グループを構成します。指定されたグループに属するユーザーのみが、指定されたネットワークにアクセスできます。Active Directory または SAML ベースのフェデレーション認証を使用していない場合、またはすべてのユーザーにアクセスを許可したい場合は、すべてのクライアントにアクセスを許可するルールを指定できます。詳細については、「承認ルール」を参照してください。

接続承認

クライアント VPN エンドポイントのクライアント接続ハンドラーを設定できます。ハンドラーを使用すると、デバイス、ユーザー、および接続属性に基づいて、新しい接続を許可するカスタムロジックを実行できます。クライアント接続ハンドラーは、クライアント VPN サービスがデバイスとユーザーを認証した後に実行されます。

クライアント VPN エンドポイントのクライアント接続ハンドラーを設定するには、デバイス、ユーザー、および接続属性を入力として受け取り、新しい接続を許可または拒否する決定をクライアント VPN サービスに返す AWS Lambda 関数を作成します。クライアント VPN エンドポイントで Lambda 関数を指定します。デバイスがクライアント VPN エンドポイントに接続すると、クライアント VPN サービスはユーザーに代わって Lambda 関数を呼び出します。Lambda 関数によって承認された接続に対して、クライアント VPN エンドポイントへの接続が許可されます。

> **Note**
>
> 現在、サポートされているクライアント接続ハンドラーのタイプは Lambda 関数だけです。

要件と考慮事項

クライアント接続ハンドラーの要件と考慮事項を次に示します。

- Lambda 関数の名前は、 `AWSClientVPN-` プレフィックスで始まる必要があります。
- 認定済みの Lambda 関数がサポートされています。
- Lambda 関数は、Client VPN AWS AWS エンドポイントと同じリージョンと同じアカウントにある必要があります。
- Lambda 関数は 30 秒後にタイムアウトします。この値は変更できません。
- Lambda 関数は同期的に呼び出されます。これは、デバイスとユーザーの認証後、および承認ルールが評価される前に呼び出されます。
- 新しい接続に対して Lambda 関数が呼び出され、クライアント VPN サービスが関数から期待されるレスポンスを取得しない場合、クライアント VPN サービスは接続要求を拒否します。これは、Lambda 関数がスロットルされた、タイムアウトした、またはその他の予期しないエラーが発生した場合、関数のレスポンスが有効な形式でない場合などに発生します。
- Lambda 関数にプロビジョニングされた同時実行数を設定して、レイテンシーの変動なしに関数をスケーリングできるようにすることをお勧めします。
- Lambda 関数を更新しても、クライアント VPN エンドポイントへの既存の接続は影響を受けません。既存の接続を終了してから、新しい接続を確立するようクライアントに指示できます。詳細については、「クライアント接続の終了」を参照してください。
- AWS クライアントが提供されたクライアントを使用してClient VPN エンドポイントに接続する場合、Windows ではバージョン 1.2.6 以降、macOS ではバージョン 1.2.4 以降を使用する必要があります。詳細については、「AWS が提供するクライアントを使用して接続する」「を参照してください。

Lambda インターフェイス

Lambda 関数は、クライアント VPN サービスからの入力として、デバイス属性、ユーザー属性、および接続属性を受け取ります。その後、クライアント VPN サービスに接続を許可または拒否するかどうかを決定する必要があります。

リクエストスキーマ

Lambda 関数は、次のフィールドを含む JSON BLOB を入力として受け取ります。

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id` — クライアント VPN エンドポイントへのクライアント接続の ID。
- `endpoint-id` — クライアント VPN エンドポイントの ID。
- `common-name` — デバイス識別子。デバイス用に作成するクライアント証明書では、共通名によってデバイスが一意に識別されます。
- `username` — ユーザー ID (該当する場合)。Active Directory 認証の場合、これはユーザー名です。SAML ベースのフェデレーション認証の場合、これは `NameID` です。相互認証の場合、このフィールドは空です。
- `platform` — クライアントのオペレーティングシステムプラットフォーム。
- `platform-version` — オペレーティングシステムのバージョン。クライアント VPN サービスは、クライアントがクライアント VPN エンドポイントに接続するとき、およびクライアントが Windows プラットフォームを実行しているときに `--push-peer-info` ディレクティブが OpenVPN クライアント設定に存在する場合に値を提供します。
- `public-ip` — 接続デバイスのパブリック IP アドレス。
- `client-openvpn-version` — クライアントが使用している OpenVPN バージョン。
- `aws-client-version`— クライアントバージョン。 AWS
- `groups` — グループ ID (該当する場合)。Active Directory 認証の場合、これはActive Directory グループの一覧になります。SAML ベースのフェデレーション認証の場合、これは ID プロバイダー (IdP) グループの一覧になります。相互認証の場合、このフィールドは空です。
- `schema-version` — スキーマバージョン。デフォルト: v3。

レスポンススキーマ

Lambda 関数は次のフィールドを返す必要があります。

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `allow` — 必須。新しい接続を許可または拒否するかどうかを示すブール値 (`true` | `false`)。
- `error-msg-on-denied-connection` — 必須。Lambda 関数によって接続が拒否された場合に、クライアントにステップとガイダンスを提供するために使用できる最大 255 文字の文字列。Lambda 関数の実行中に障害が発生した場合 (スロットリングなどの理由で)、次のデフォルトメッセージがクライアントに返されます。

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses` — 必須。体制評価に Lambda 関数を使用する場合、これは接続デバイスのステータスのリストです。デバイスの体制評価カテゴリ (`compliant`、`quarantined`、`unknown` など) に従って、ステータス名を定義します。各名前の最大長は 255 文字です。最大 10 個のステータスを指定できます。
- `schema-version` — 必須。スキーマバージョン。デフォルト: v3。

同じリージョン内の複数のクライアント VPN エンドポイントに対して、同じ Lambda 関数を使用できます。

Lambda 関数の作成の詳細については、AWS Lambda デベロッパーガイドの「AWS Lambdaの開始方法」を参照してください。

体制評価のためのクライアント接続ハンドラーの使用

クライアント接続ハンドラーを使用して、クライアント VPN エンドポイントを既存のデバイス管理ソリューションと統合し、接続デバイスの体制コンプライアンスを評価できます。Lambda 関数がデバイス承認ハンドラーとして機能するには、クライアント VPN エンドポイントに相互認証を使用します 。クライアント VPN エンドポイントに接続するクライアント (デバイス) ごとに、一意のクライアント証明書とキーを作成します。Lambda 関数は、クライアント証明書の一意の共通名 (クライアント VPN サービスから渡される) を使用して、デバイスを識別し、デバイス管理ソリューション

から体制コンプライアンスステータスを取得できます。相互認証をユーザーベースの認証と組み合わせることができます。

または、Lambda 関数自体で基本的な体制評価を行うこともできます。たとえば、クライアント VPN サービスによって Lambda 関数に渡される `platform` および `platform-version` フィールドを評価できます。

> **Note**
>
> AWS Client VPN 接続ハンドラーを使用して最低限のアプリケーションバージョンを適用することもできますが、`aws-client-version` AWS Client VPN 接続ハンドラーのフィールドはアプリケーションにのみ適用され、ユーザーデバイス上の環境変数から入力されます。

クライアント接続ハンドラーの有効化

クライアント接続ハンドラーを有効にするには、クライアント VPN エンドポイントを作成または変更し、Lambda 関数の Amazon リソースネーム (ARN) を指定します。詳細については、「クライアント VPN エンドポイントを作成する」および「クライアント VPN エンドポイントを変更する」を参照してください。

サービスにリンクされたロール

AWS Client VPN というサービスにリンクされたロールがアカウントに自動的に作成されます。AWSServiceRoleForClientVPNConnectionsロールには、クライアント VPN エンドポイントへの接続が行われたときに Lambda 関数を呼び出すアクセス許可があります。詳細については、「クライアント VPN のサービスにリンクされたロールの使用」を参照してください。

接続承認失敗のモニタリング

クライアント VPN エンドポイントへの接続の接続承認ステータスを表示できます。詳細については、「クライアント接続の表示」を参照してください。

体制評価にクライアント接続ハンドラーを使用すると、クライアント VPN エンドポイントに接続するデバイスの体制コンプライアンスステータスを接続ログに表示することもできます。詳細については、「接続ログ」を参照してください。

デバイスが接続承認に失敗した場合、接続ログの `connection-attempt-failure-reason` フィールドから次の失敗理由のいずれかが返されます。

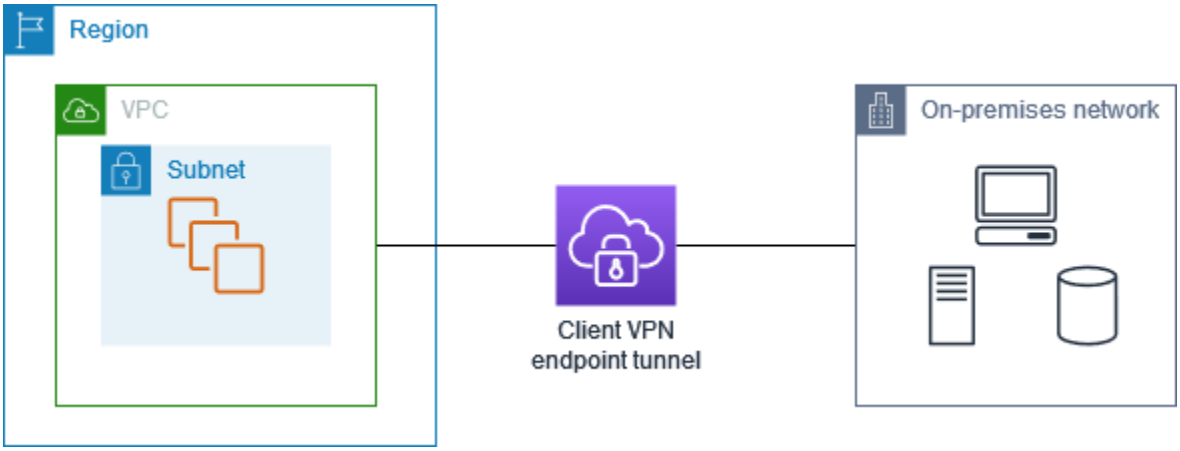
- `client-connect-failed` — Lambda 関数によって接続が確立されませんでした。
- `client-connect-handler-timed-out` — Lambda 関数がタイムアウトしました。
- `client-connect-handler-other-execution-error` — Lambda 関数で予期しないエラーが発生しました。
- `client-connect-handler-throttled` — Lambda 関数がスロットルされました。
- `client-connect-handler-invalid-response` — Lambda 関数が無効なレスポンスを返しました。
- `client-connect-handler-service-error` — 接続試行中にサービス側のエラーが発生しました。

AWS クライアント VPN エンドポイントの分割トンネル

デフォルトでは、クライアント VPN エンドポイントがある場合、クライアントからのすべてのトラフィックはクライアント VPN トンネル経由でルーティングされます。クライアント VPN エンドポイントで分割トンネルを有効にすると、クライアント VPN エンドポイントルートテーブル上のルートがクライアント VPN エンドポイントに接続されているデバイスにプッシュされます。これにより、クライアント VPN エンドポイントルートテーブルからのルートと一致するネットワークへの送信先を持つトラフィックだけがクライアント VPN トンネル経由でルーティングされます。

すべてのユーザートラフィックがクライアント VPN エンドポイントを通過しないようにする場合は、分割トンネルクライアント VPN エンドポイントを使用できます。

次の例では、クライアント VPN エンドポイントで分割トンネルが有効になっています。VPC (172.31.0.0/16) 宛てのトラフィックのみがクライアント VPN トンネル経由でルーティングされます。オンプレミスリソース宛てのトラフィックは、クライアント VPN トンネル経由でルーティングされません。



分割トンネルの利点

クライアント VPN エンドポイントの分割トンネルには、次の利点があります。

- AWS 宛てのトラフィックだけが VPN トンネルを通過できるようにすることで、クライアントからのトラフィックのルーティングを最適化できます。
- AWS からの送信トラフィックの量を減らして、データ転送コストを削減できます。

ルーティングに関する考慮事項

- 分割トンネルを有効化する場合、VPN 接続が確立されると、クライアント VPN エンドポイントのルートテーブル内のすべてのルートがクライアントのルートテーブルに追加されます。このオペレーションは、デフォルトの動作とは異なります。デフォルトの動作では、クライアントのルートテーブルがエントリ `0.0.0.0/0` で上書きされ、すべてのトラフィックが VPN 経由でルーティングされます。

  > **Note**
  >
  > 分割トンネルモードを使用する場合、クライアント VPN エンドポイントのルートテーブルに `0.0.0.0/0` ルートを追加することはお勧めしません。

- スプリットトンネルモードが有効な場合、クライアント VPN エンドポイントのルートテーブルを変更すると、すべてのクライアント接続がリセットされます。

分割トンネルの有効化

新規または既存のクライアント VPN エンドポイントで分割トンネルを有効にできます。詳細については、次のトピックを参照してください。

- クライアント VPN エンドポイントを作成する
- クライアント VPN エンドポイントを変更する

接続ログ

接続ログは、クライアント VPN エンドポイントの接続ログをキャプチャできる AWS Client VPN の機能です。

接続ログには、接続ログエントリが含まれます。各接続ログエントリには、クライアント (エンドユーザー) が接続するタイミング、接続を試行するタイミング、クライアント VPN エンドポイントから切断するタイミングなどの接続イベントに関する情報が含まれます。この情報を使用してフォレンジックを実行したり、クライアント VPN エンドポイントがどのように使用されているかを分析したり、接続の問題をデバッグしたりできます。

接続ログは、AWS クライアント VPN が使用可能なすべてのリージョンで使用できます。接続ログは、アカウントの CloudWatch Logs ロググループに発行されます。

> **Note**
>
> 失敗した相互認証の試行は記録されません。

接続ログエントリ

接続ログエントリは、キーと値のペアの JSON 形式の BLOB です。次に、接続ログエントリの例を示します。

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

接続ログエントリには、次のキーが含まれます。

- connection-log-type — 接続ログエントリのタイプ (connection-attempt または connection-reset)。
- connection-attempt-status — 接続リクエストのステータス (successful、failed、waiting-for-assertion、または NA)。
- connection-reset-status — 接続リセットイベントのステータス (NA または assertion-received)。
- connection-attempt-failure-reason — 接続エラーの理由 (該当する場合)。
- connection-id — 接続の ID。
- client-vpn-endpoint-id — 接続が行われたクライアント VPN エンドポイントの ID。
- transport-protocol — 接続に使用されたトランスポートプロトコル。
- connection-start-time — 接続の開始時刻。
- connection-last-update-time — 接続の最終更新時刻。この値は、ログ内で定期的に更新されます。
- client-ip — クライアントの IP アドレス。クライアント VPN エンドポイントのクライアント IPv4 CIDR 範囲から割り当てられます。
- common-name — 証明書ベースの認証に使用される証明書の共通名。
- device-type — エンドユーザーが接続に使用するデバイスのタイプ。
- device-ip — デバイスのパブリック IP アドレス。
- port — 接続のポート番号。
- ingress-bytes — 接続の受信 (インバウンド) バイト数。この値は、ログ内で定期的に更新されます。
- egress-bytes — 接続の送信 (アウトバウンド) バイト数。この値は、ログ内で定期的に更新されます。
- ingress-packets — 接続の受信 (インバウンド) パケット数。この値は、ログ内で定期的に更新されます。
- egress-packets — 接続の送信 (アウトバウンド) パケット数。この値は、ログ内で定期的に更新されます。
- connection-end-time — 接続の終了時刻。この値は、接続がまだ進行中の場合や接続の試行が失敗した場合は NA です。
- posture-compliance-statuses — クライアント接続ハンドラーによって返される体制コンプライアンスステータス (該当する場合)。

- `username` - ユーザー名は、エンドポイントにユーザーベースの認証 (AD または SAML) を使用するときに記録されます。
- `connection-duration-seconds` - 接続の継続時間 (秒)。「接続開始時間」と「接続終了時間」の差に等しくなります。

接続ログの有効化の詳細については、「接続ログの操作」を参照してください。

クライアント VPN スケーリングに関する考慮事項

クライアント VPN エンドポイントを作成するときは、サポートする予定の同時 VPN 接続の最大数を考慮してください。現在サポートしているクライアントの数と、必要に応じてクライアント VPN エンドポイントが追加需要を満たすことができるかどうかを考慮する必要があります。

以下の要因は、クライアント VPN エンドポイントでサポートできる同時 VPN 接続の最大数に影響します。

クライアント CIDR 範囲のサイズ

クライアント VPN エンドポイントを作成するときは、クライアント CIDR 範囲を指定する必要があります。これは、/12 と /22 ネットマスクの間の IPv4 CIDR ブロックです。クライアント VPN エンドポイントへのそれぞれの VPN 接続には、クライアント CIDR 範囲から固有の IP アドレスが割り当てられます。クライアント CIDR 範囲内のアドレスの一部は、クライアント VPN エンドポイントの可用性モデルをサポートするためにも使用され、クライアントに割り当てることはできません。クライアント VPN エンドポイントの作成後にクライアント CIDR 範囲を変更することはできません。

一般に、クライアント VPN エンドポイントでサポートする予定の IP アドレス (つまり同時接続) の 2 倍の数を含むクライアント CIDR 範囲を指定することをお勧めします。

関連付けられたサブネットの数

サブネットをクライアント VPN エンドポイントに関連付けると、ユーザーはクライアント VPN エンドポイントへの VPN セッションを確立できるようになります。複数のサブネットを 1 つのクライアント VPN エンドポイントに関連付けると、高可用性を実現し、追加の接続キャパシティを有効にできます。

クライアント VPN エンドポイントのサブネットの関連付けの数に基づく、サポートされる同時 VPN 接続の数を次に示します。

サブネットの関連付け	サポートされる接続数
1	7,000
2	36,500
3	66,500
4	96,500
5	126,000

1 つのアベイラビリティーゾーンの複数のサブネットをクライアント VPN エンドポイントに関連付けることはできません。したがって、サブネットの関連付けの数は、AWS リージョンで使用可能なアベイラビリティーゾーンの数にも依存します。

例えば、クライアント VPN エンドポイントへの 8,000 の VPN 接続をサポートすることが予想される場合は、クライアント CIDR 範囲の最小サイズ /18 (16,384 IP アドレス) を指定し、少なくとも 2 つのサブネットをクライアント VPN エンドポイントに関連付けます。

クライアント VPN エンドポイントで予想される VPN 接続の数がわからない場合は、/16 CIDR ブロックのサイズ以上を指定することをお勧めします。

クライアント CIDR 範囲とターゲットネットワークの操作に関する規則と制限の詳細については、「のルールとベストプラクティス AWS Client VPN」を参照してください 。

クライアント VPN エンドポイントのクォータの詳細については、「AWS クライアント VPN クォータ」を参照してください 。

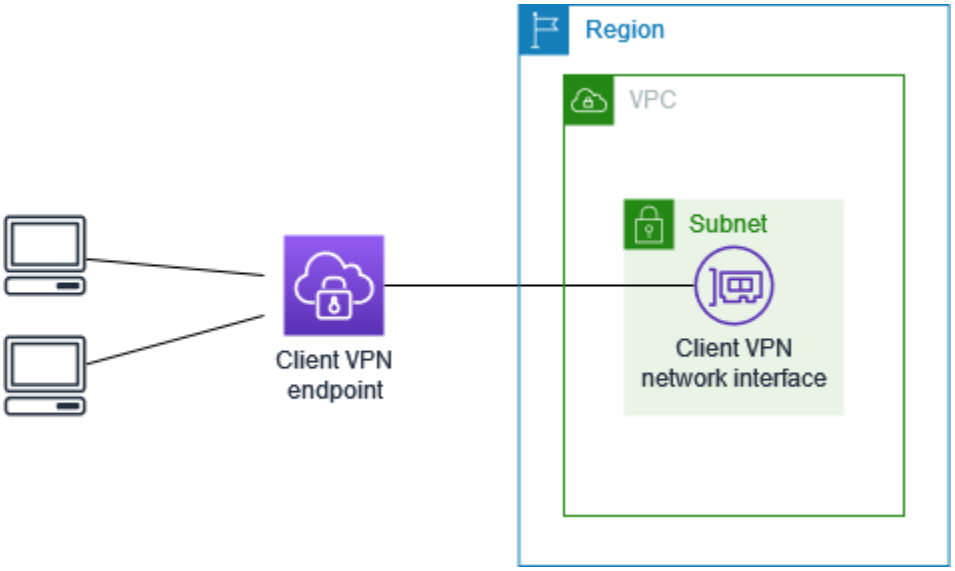
AWS クライアント VPN のシナリオと例

このセクションでは、クライアントの VPN アクセスを作成して設定するための例について説明します。

内容

AWS クライアント VPN を使用した VPC へのアクセス

このシナリオの設定には、単一のターゲット VPC が含まれています。クライアントに単一の VPC 内のリソースへのアクセスのみを許可する必要がある場合は、この設定をお勧めします。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントと関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。

- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- のルールとベストプラクティス AWS Client VPN のクライアント VPN エンドポイントのルールと制限を確認します。

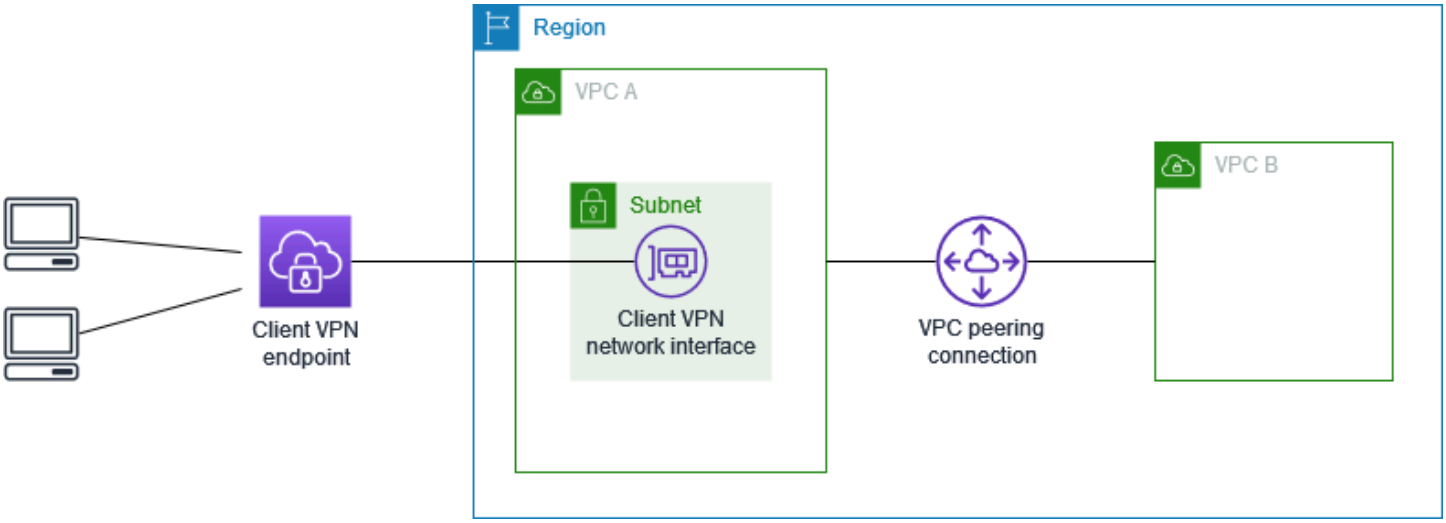
この設定を実装するには

1. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する」で説明されているステップを実行します。
2. サブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける」で説明されているステップを実行し、先ほど確認した VPC およびサブネットを選択します。
3. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行し、[Destination network (送信先ネットワーク)] で、VPC の IPv4 CIDR 範囲を入力します。
4. リソースのセキュリティグループにルールを追加して、ステップ 2 でサブネットの関連付けに適用されたセキュリティグループからのトラフィックを許可します。詳細については、「セキュリティグループ」を参照してください。

AWS クライアント VPN を使用したピア接続 VPC へのアクセス

このシナリオの設定には、追加の VPC (VPC B) とピア接続されているターゲット VPC (VPC A) が含まれます。クライアントにターゲット VPC およびそれとピア接続されている他の VPC (VPC B など) にあるリソースへのアクセスを許可する必要がある場合は、この設定をお勧めします。

> **Note**
>
> 以下に示すピアリングされた VPC へのアクセスを許可する手順は、Client VPN エンドポイントがスプリットトンネルモードに設定されている場合にのみ必要です。フルトンネルモードでは、ピアリングされた VPC へのアクセスがデフォルトで許可されます。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントと関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- のルールとベストプラクティス AWS Client VPN のクライアント VPN エンドポイントのルールと制限を確認します。

この設定を実装するには

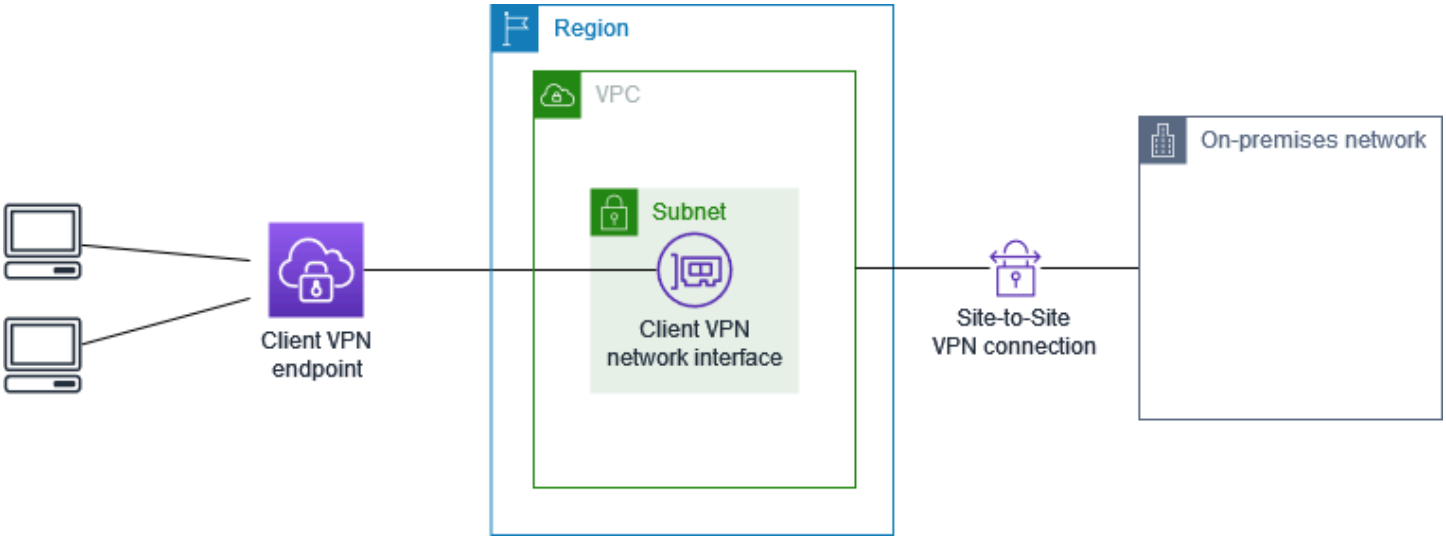
1. VPC 間の VPC ピア接続を確立します。Amazon VPC ピアリングガイドの「VPC ピア接続の作成と承認」のステップに従います。VPC A のインスタンスがピア接続を介して VPC B のインスタンスと通信できることを確認します。
2. ターゲット VPC と同じリージョンに、クライアント VPN エンドポイントを作成します。これは、前の図では VPC A です。「クライアント VPN エンドポイントを作成する」に説明されている手順を実行します。
3. 特定したサブネットを、作成したクライアント VPN エンドポイントと関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける」で説明している手順を実行し、VPC とサブネットを選択します。デフォルトでは、VPC のデフォルトセキュリティグループをクライアント VPN エンドポイントに関連付けます。「the section called “セキュリティグループをターゲットネットワークに適用する”」で説明している手順を使用して、別のセキュリティグループを関連付けることができます。
4. 許可ルールを追加して、クライアントにターゲット VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているス

テップを実行します。[Destination network to enable (有効にする宛先ネットワーク)] に、VPC の IPv4 CIDR 範囲を入力します。

5. ピア VPC にトラフィックを送信するルートを追加します。これは、図では VPC B です。これを行うには、「エンドポイントルートの作成」で説明している手順を実行します。[ルート送信先] に、ピアリングされた VPC の IPv4 CIDR 範囲を入力します。[ターゲット VPC サブネット ID] で、クライアント VPN エンドポイントに関連付けたサブネットを選択します。
6. クライアントにピア接続 VPC へのアクセスを許可するための承認ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行します。[送信先ネットワーク] に、ピアリングされた VPC の IPv4 CIDR 範囲を入力します。
7. VPC A および VPC B でインスタンスのセキュリティグループにルールを追加し、ステップ 3 でクライアント VPN エンドポイントに適用したセキュリティグループからのトラフィックを許可します。詳細については、「セキュリティグループ」を参照してください。

AWS クライアント VPN を使用したオンプレミスネットワークへのアクセス

このシナリオの設定には、オンプレミスネットワークへのアクセスのみが含まれています。クライアントにオンプレミスネットワーク内のリソースへのアクセスのみを許可する必要がある場合は、この設定をお勧めします。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントと関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- のルールとベストプラクティス AWS Client VPN のクライアント VPN エンドポイントのルールと制限を確認します。

この設定を実装するには

1. AWS Site-to-Site VPN 接続を介した VPC と独自のオンプレミスネットワーク間の通信を有効にします。これを行うには、AWS Site-to-Site VPN ユーザーガイドの「開始方法」で説明されているステップを実行します。

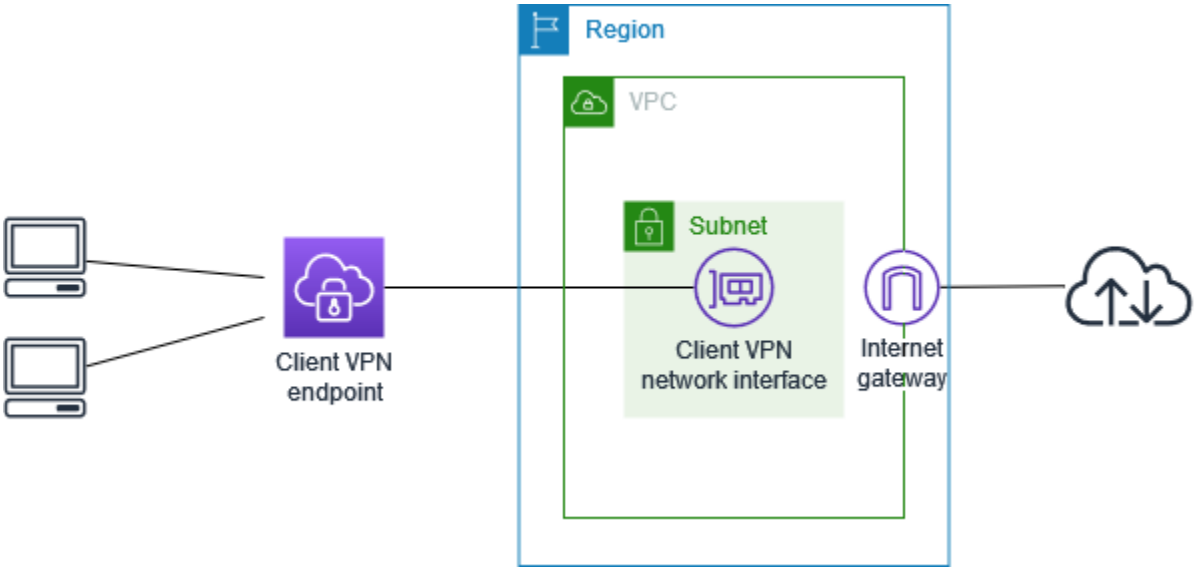
   > **Note**
   >
   > または、VPC とオンプレミスネットワーク間の AWS Direct Connect 接続を使用して、このシナリオを実装することもできます。詳細については、AWS Direct Connect ユーザーガイドを参照してください。

2. 前のステップで作成した AWS Site-to-Site VPN 接続をテストします。これを行うには、AWS Site-to-Site VPN ユーザーガイドの「Site-to-Site VPN 接続のテスト」で説明されているステップを実行します。VPN 接続が正常に機能する場合は、次のステップに進みます。
3. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する」で説明されているステップを実行します。
4. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける」で説明されているステップを実行し、VPC とサブネットを選択します。
5. AWS Site-to-Site VPN 接続へのアクセスを許可するルートを追加します。これを行うには、「エンドポイントルートの作成」で説明されているステップを実行します。[Route destination] (ルートの送信先) には、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力し、[Target VPC Subnet ID,] (ターゲット VPC サブネット ID) には、クライアント VPN エンドポイントに関連付けたサブネットを選択します。
6. クライアントに、AWS Site-to-Site VPN 接続へのアクセス権を付与する許可ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行します。[Destination network] (送信先ネットワーク) で、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力します。

AWS クライアント VPN を使用したインターネットへのアクセス

このシナリオの設定には、単一のターゲット VPC とインターネットへのアクセスが含まれています。クライアントに単一のターゲット VPC 内のリソースへのアクセスを許可し、インターネットへのアクセスを許可する必要がある場合は、この設定をお勧めします。

AWS クライアント VPN の開始方法 チュートリアルが完了している場合、このシナリオはすでに実装されていることになります。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントと関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- のルールとベストプラクティス AWS Client VPN のクライアント VPN エンドポイントのルールと制限を確認します。

この設定を実装するには

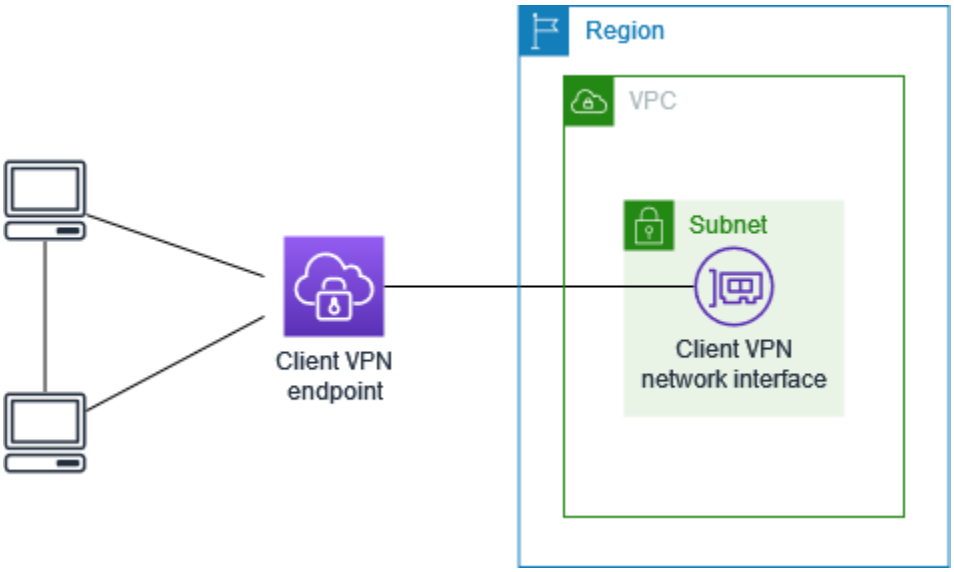
1. クライアント VPN エンドポイントに使用するセキュリティグループで、インターネットへのアウトバウンドトラフィックが許可されていることを確認します。このためには、HTTP および HTTPS トラフィックについて、0.0.0.0/0 へのトラフィックを許可するアウトバウンドルールを追加します。

2. インターネットゲートウェイを作成して VPC にアタッチします。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイの作成とアタッチ」を参照してください。
3. インターネットゲートウェイへのルートをそのルートテーブルに追加して、サブネットを公開します。[VPC コンソール] で、[サブネット] を選択し、クライアント VPN エンドポイントに関連付ける予定のサブネットを選択します。[Route Table (ルートテーブル)] を選択し、次にルートテーブル ID を選択します。[アクション] を選択し、[Edit routes (ルートの編集)] を選択して、[Add route (ルートの追加)] を選択します。[送信先] に、`0.0.0.0/0` を入力し、[ターゲット] で、前のステップからインターネットゲートウェイを選択します。
4. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する」で説明されているステップを実行します。
5. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける」で説明されているステップを実行し、VPC とサブネットを選択します。
6. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行します。[Destination network to enable (有効にする送信先ネットワーク)] で、VPC の IPv4 CIDR 範囲を入力します。
7. インターネットへのトラフィックを可能にするルートを追加します。これを行うには、「エンドポイントルートの作成」で説明されているステップを実行します。[Route destination (ルートの送信先)] に `0.0.0.0/0` を入力し、[Target VPC Subnet ID (ターゲット VPC サブネット ID)] でクライアント VPN エンドポイントに関連付けたサブネットを選択してください。
8. 承認ルールを追加して、クライアントにインターネットへのアクセスを許可します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行し、送信先ネットワークとして「`0.0.0.0/0`」と入力します。
9. VPC 内のリソースのセキュリティグループに、クライアント VPN エンドポイントに関連付けられたセキュリティグループからのアクセスを許可するルールがあることを確認します。これにより、クライアントが VPC 内のリソースにアクセスできるようになります。

AWS クライアント VPN を使用した C lient-to-client アクセス

このシナリオの設定では、クライアントは単一の VPC にアクセスでき、クライアントが相互にトラフィックをルーティングできます。同じクライアント VPN エンドポイントに接続するクライアントも相互に通信する必要がある場合は、この設定をお勧めします。クライアントは、クライアント

VPN エンドポイントに接続するときに、クライアントの CIDR 範囲から割り当てられた一意の IP アドレスを使用して相互に通信できます。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントと関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- のルールとベストプラクティス AWS Client VPN のクライアント VPN エンドポイントのルールと制限を確認します。

> **Note**
>
> Active Directory グループまたは SAML ベースの IdP グループを使用するネットワークベースの承認規則は、このシナリオではサポートされません。

この設定を実装するには

1. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する」で説明されているステップを実行します。
2. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける」で説明されているステップを実行し、VPC とサブネットを選択します。

3. ルートテーブルのローカルネットワークにルートを追加します。これを行うには、「エンドポイントルートの作成」で説明されているステップを実行します。[Route destination (ルート送信先)] に、クライアントの CIDR 範囲を入力し、[Target VPC Subnet ID (ターゲット VPC サブネット ID)] で `local` を指定します。
4. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行します。[Destination network to enable (有効にする宛先ネットワーク)] に、VPC の IPv4 CIDR 範囲を入力します。
5. クライアントにクライアントの CIDR 範囲へのアクセスを許可するための承認ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加」で説明されているステップを実行します。[Destination network to enable (有効にする宛先ネットワーク)] に、クライアントの CIDR 範囲を入力します。

AWS クライアント VPN を使用したネットワークへのアクセス制限

クライアント VPN エンドポイントを設定して、VPC 内の特定のリソースへのアクセスを制限することができます。ユーザーベースの認証の場合、クライアント VPN エンドポイントにアクセスするユーザーグループに基づいて、ネットワークの一部へのアクセスを制限することもできます。

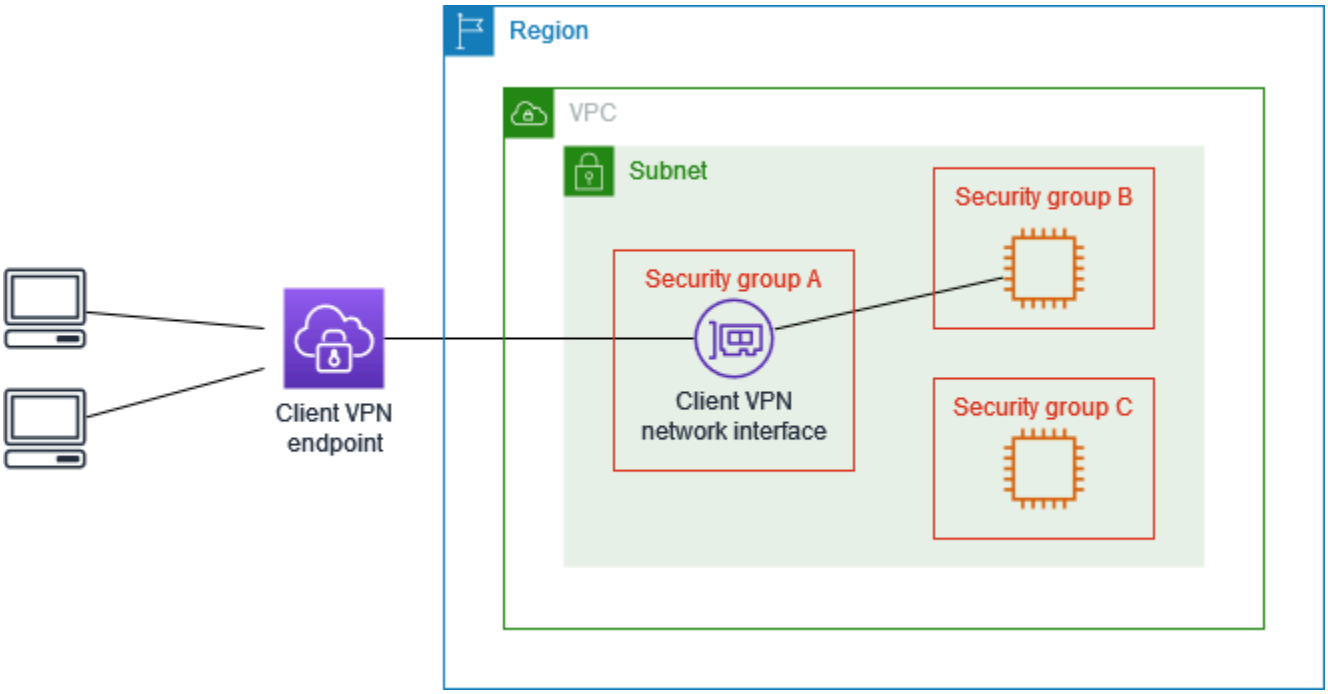
セキュリティグループを使用してアクセスを制限する

ターゲットネットワーク関連付けに適用されたセキュリティグループ (クライアント VPN セキュリティグループ) を参照するセキュリティ グループルールを追加または削除することで、VPC 内の特定のリソースへのアクセスを許可または拒否することができます。この設定は「AWS クライアント VPN を使用した VPC へのアクセス」で説明されているシナリオに拡張します。この設定は、そのシナリオで設定された認証ルールに加えて適用されます。

特定のリソースへのアクセスを許可するには、リソースが実行されているインスタンスに関連付けられているセキュリティグループを特定します。次に、クライアント VPN セキュリティグループからのトラフィックを許可するルールを作成します。

以下の図では、セキュリティグループ A はクライアント VPN セキュリティグループで、セキュリティグループ B は EC2 インスタンスに関連付けられ、セキュリティグループ C は EC2 インスタンスに関連付けられています。セキュリティグループ A からのアクセスを許可するルールをセキュリティグループ B に追加すると、クライアントはセキュリティグループ B に関連付けられているインスタンスにアクセスできます。セキュリティグループ C に、セキュリティグループ A からのアクセ

スを許可するルールがない場合、クライアントはセキュリティグループ C に関連付けられたインスタンスにアクセスできません。



開始する前に、クライアント VPN セキュリティグループが VPC 内の他のリソースに関連付けられているかどうかを確認します。クライアント VPN セキュリティグループを参照するルールを追加または削除すると、他の関連するリソースへのアクセスを許可または拒否することができます。これを防ぐには、クライアント VPN エンドポイント専用として使用するために作成されたセキュリティグループを使用します。

セキュリティグループルールを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、セキュリティグループ] を選択します。
3. リソースが実行されているインスタンスに関連付けられているセキュリティグループを選択します。
4. [アクション]、[Edit inbound rules (インバウンドルールの編集)] の順に選択します。
5. [ルールの追加] を選択し、次の操作を行います。
   - [タイプ] で、[すべてのトラフィック]、または許可する特定のタイプのトラフィックを選択します。
   - [ソース] で [カスタム] を選択し、クライアント VPN セキュリティグループの ID を入力または選択します。

6. [Save Rules (ルールの保存)] を選択します。

特定のリソースへのアクセスを削除するには、リソースが実行されているインスタンスに関連付けられているセキュリティグループを確認します。クライアント VPN セキュリティグループからのトラフィックを許可するルールがある場合は、それを削除します。

セキュリティグループルールを確認するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、セキュリティグループ] を選択します。
3. [Inbound Rules (インバウンドルール)] を選択します。
4. ルールのリストを確認します。[ソース] がクライアント VPN セキュリティグループであるルールがある場合は、[Edit Rules (ルールの編集)] を選択し、そのルールの [削除] (x アイコン) を選択します。[Save Rules] (ルールの保存) を選択します。

ユーザーグループに基づいてアクセスを制限する

クライアント VPN エンドポイントがユーザーベースの認証用に設定されている場合は、特定のユーザーグループにネットワークの特定の部分へのアクセスを許可できます。そのためには、以下のステップを完了します。

1. AWS Directory Service または IdP でユーザーとグループを設定します。詳細については、次のトピックを参照してください。
   - Active Directory 認証
   - SAML ベースのフェデレーション認証の要件と考慮事項
2. クライアント VPN エンドポイントの許可ルールを作成して、指定したグループがネットワークの全部または一部に アクセスできるようにします。詳細については、「承認ルール」を参照してください。

クライアント VPN エンドポイントが相互認証用に設定されている場合は、ユーザーグループを設定できません。承認ルールを作成するときは、すべてのユーザーにアクセスを許可する必要があります。特定のユーザーグループがネットワークの特定の部分にアクセスできるようにするには、複数のクライアント VPN エンドポイントを作成します。たとえば、ネットワークにアクセスするユーザーグループごとに、次の操作を実行します。

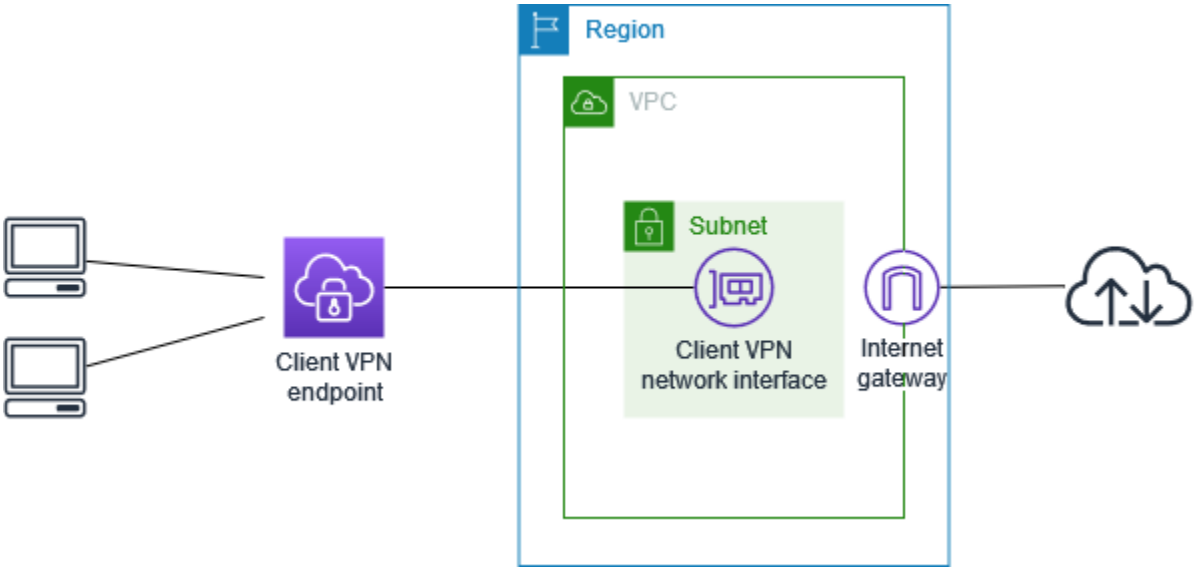
1. そのユーザーグループに対して、サーバー証明書、クライアント証明書、およびキーのセットを作成します。詳細については、「相互認証」を参照してください。
2. クライアント VPN エンドポイントを作成します。詳細については、「クライアント VPN エンドポイントを作成する」を参照してください。
3. ネットワークのすべてまたは一部へのアクセスを許可する承認ルールを作成します。たとえば、管理者が使用するクライアント VPN エンドポイントの場合、ネットワーク全体へのアクセスを許可する許可ルールを作成できます。詳細については、「クライアント VPN エンドポイントへの承認ルールの追加」を参照してください。

AWS クライアント VPN の開始方法

このチュートリアルでは、次の処理を実行するクライアント VPN エンドポイントを作成します。

- すべてのクライアントが 1 つの VPC にアクセスできるようにします。
- すべてのクライアントがインターネットにアクセスできるようにします。
- 相互認証を使用します。

次の図は、このチュートリアルを完了した後の VPC とクライアント VPN エンドポイントの設定を示しています。



ステップ

- 前提条件
- ステップ 1: サーバーおよびクライアント証明書とキーの生成
- ステップ 2: クライアント VPN エンドポイントを作成する
- ステップ 3: ターゲットネットワークを関連付ける
- ステップ 4: VPC の認可ルールを追加する
- ステップ 5: インターネットへのアクセスを提供する
- ステップ 6: セキュリティグループの要件を検証する
- ステップ 7: クライアント VPN エンドポイント設定ファイルをダウンロードする
- ステップ 8: クライアント VPN エンドポイントに接続する

前提条件

このチュートリアルを開始する前に、以下の要件を満たしていることを確認してください。

- クライアント VPN エンドポイントを操作するために必要な許可。
- AWS Certificate Manager に証明書をインポートするために必要な許可。
- 少なくとも 1 つのサブネットとインターネットゲートウェイを持つ VPC。サブネットに関連付けられているルートテーブルには、インターネットゲートウェイへのルートが必要です。

ステップ 1: サーバーおよびクライアント証明書とキーの生成

このチュートリアルでは、相互認証が使用されます。相互認証では、クライアント VPN は証明書を使用してクライアントとクライアント VPN エンドポイント間の認証を実行します。サーバー証明書とキー、および少なくとも 1 つのクライアント証明書とキーが必要です。少なくとも、サーバー証明書を AWS Certificate Manager (ACM) にインポートする必要があり、クライアント VPN エンドポイントを作成するときに指定する必要があります。ACM へのクライアント証明書のインポートはオプションです。

この目的で使用する証明書をまだ持っていない場合は、OpenVPN easy-rsa ユーティリティを使用して作成できます。OpenVPN easy-RSA ユーティリティを使用してサーバーおよびクライアント証明書とキーを生成し、ACM にインポートするステップの詳細については、「相互認証」を参照してください。

> **Note**
>
> サーバー証明書は、クライアント VPN エンドポイントを作成するのと同じ AWS リージョンの AWS Certificate Manager (ACM) でプロビジョニングするか、インポートする必要があります。

ステップ 2: クライアント VPN エンドポイントを作成する

クライアント VPN エンドポイントは、クライアント VPN セッションを有効にして管理するために作成して設定するリソースです。これは、すべてのクライアント VPN セッションの終了ポイントです。

クライアント VPN エンドポイントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Client VPN Endpoint] (クライアント VPN エンドポイント) を選択し、[Create Client VPN Endpoint] (クライアント VPN エンドポイントの作成) を選択します。
3. (オプション) クライアント VPN エンドポイントの名前タグと説明を入力します。
4. [Client IPv4 CIDR] (クライアント IPv4 CIDR) に、クライアント IP アドレスを割り当てる IP アドレス範囲を CIDR 表記で指定します。

   > **Note**
   >
   > IP アドレス範囲は、ターゲットネットワークのアドレス範囲、VPC のアドレス範囲、またはクライアント VPN エンドポイントに関連付けられるルートと重複できません。クライアントアドレス範囲は /22 以上で、/12 CIDR ブロックサイズを超えないようにする必要があります。クライアント VPN エンドポイントの作成後にクライアントのアドレス範囲を変更することはできません。

5. [Server certificate ARN] (サーバー証明書 ARN) として、ステップ 1 で生成したサーバー証明書の ARN を選択します。
6. [Authentication options] (認証オプション) で、[Use mutual authentication] (相互認証を使用する) を選択してから、[Client certificate ARN] (クライアント証明書 ARN) で、使用するクライアント証明書の ARN を選択します。

   サーバー証明書とクライアント証明書が同じ認証機関 (CA) によって署名されている場合、サーバーとクライアントの両方の証明書についてサーバー証明書 ARN を指定することができます。この状況では、サーバー証明書に対応するすべてのクライアント証明書を使用して認証できます。
7. 残りはデフォルト設定のままにして、[Create Client VPN Endpoint] (クライアント VPN エンドポイントの作成) を選択します。

クライアント VPN エンドポイントを作成すると、その状態は `pending-associate` になります。クライアントは、少なくとも 1 つのターゲットネットワークを関連付けた後でのみ、VPN 接続を確立できます。

クライアント VPN エンドポイントに指定できるオプションの詳細については、「クライアント VPN エンドポイントを作成する」を参照してください。

ステップ 3: ターゲットネットワークを関連付ける

クライアントが VPN セッションを確立するには、ターゲットネットワークをクライアント VPN エンドポイントに関連付ける必要があります。ターゲットネットワークは、VPC のサブネットです。

ターゲットネットワークをクライアント VPN エンドポイントに関連付けるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 前の手順で作成したクライアント VPN エンドポイントを選択してから、[Target network associations] (ターゲットネットワークの関連付け)、[Associate target network] (ターゲットネットワークを関連付ける) を選択します。
4. [VPC] で、サブネットがある VPC を選択します。
5. [Choose a subnet to associate] (関連付けるサブネットを選択する) で、クライアント VPN エンドポイントに関連付けるサブネットを選択します。
6. [Associate target network] (ターゲットネットワークを関連付ける) を選択します。
7. 認可ルールで許可されている場合、クライアントが VPC のネットワーク全体にアクセスするには、1 つのサブネットの関連付けで十分です。アベイラビリティーゾーンに障害が発生した場合に高可用性を提供するために、追加のサブネットを関連付けることができます。

最初のサブネットをクライアント VPN エンドポイントに関連付けると、次の処理が実行されます。

- クライアント VPN エンドポイントの状態が `available` に変わります。これで、クライアントは VPN 接続を確立できるようになりましたが、認証ルールを追加するまで VPC 内のリソースにアクセスすることはできません。
- VPC のローカルルートが、クライアント VPN エンドポイントルートテーブルに自動的に追加されます。
- VPC のデフォルトのセキュリティグループが、クライアント VPN エンドポイントに自動的に適用されます。

ステップ 4: VPC の認可ルールを追加する

クライアントが VPC にアクセスするには、クライアント VPN エンドポイントのルートテーブルに VPC へのルートと認可ルールが存在する必要があります。ルートは、前のステップで既に自動的に

追加されています。このチュートリアルでは、すべてのユーザーに VPC へのアクセスを付与します。

VPC の認可ルールを追加するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 認可ルールを追加するクライアント VPN エンドポイントを選択します。[Authorization rules] (認可ルール) を選択してから、[Add authorization rule] (認可ルールを追加する) を選択します。
4. [Destination network to enable] (有効にする送信先ネットワーク) に、アクセスを許可するネットワークの CIDR を入力します。例えば、VPC 全体へのアクセスを許可するには、VPC の IPv4 CIDR ブロックを指定します。
5. [Grant access to] (アクセスを付与する対象) で、[Allow access to all users] (すべてのユーザーにアクセスを許可する) を選択します。
6. [Description] (説明) に、認可ルールの簡単な説明を入力します。
7. [Add authorization rule] (認可ルールを追加する) を選択します。

ステップ 5: インターネットへのアクセスを提供する

AWS サービス、ピア接続 VPC、オンプレミスネットワークなど、VPC に接続されている追加のネットワークとインターネットへのアクセスを提供できます。追加のネットワークごとに、クライアント VPN エンドポイントのルートテーブルにネットワークへのルートを追加し、クライアントアクセスに付与する認可ルールを設定します。

このチュートリアルでは、すべてのユーザーにインターネットと VPC へのアクセスを付与します。VPC へのアクセスは既に設定したため、このステップではインターネットへのアクセスを設定します。

インターネットへのアクセスを提供するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. このチュートリアル用に作成したクライアント VPN エンドポイントを選択します。[Route Table] (ルートテーブル) を選択してから、[Create Route] (ルートの作成) を選択します。

4. [Route destination] (ルートの宛先) に「`0.0.0.0/0`」と入力します。[Subnet ID for target network association] (ターゲットネットワーク関連付けのサブネット ID) で、トラフィックをルーティングするサブネットの ID を指定します。
5. [Create Route] (ルートの作成) を選択します。
6. [Authorization rules] (認可ルール) を選択してから、[Add authorization rule] (認可ルールを追加する) を選択します。
7. [Destination network to enable access] (アクセスを有効にする送信先ネットワーク) で、「`0.0.0.0/0`」と入力し、[Allow access to all users] (すべてのユーザーにアクセスを許可する) を選択します。
8. [Add authorization rule] (認可ルールを追加する) を選択します。

ステップ 6: セキュリティグループの要件を検証する

このチュートリアルでは、ステップ 2 でのクライアント VPN エンドポイントの作成時にセキュリティグループが指定されていません。つまり、VPC のデフォルトのセキュリティグループが、ターゲットネットワークが関連付けられるときにクライアント VPN エンドポイントに自動的に適用されます。その結果、VPC のデフォルトのセキュリティグループがクライアント VPN エンドポイントに関連付けられているはずです。

次のセキュリティグループの要件を確認します。

- トラフィックをルーティングするサブネットに関連付けられているセキュリティグループ (この場合はデフォルトの VPC セキュリティグループ) によって、インターネットへのアウトバウンドトラフィックが許可されること。このためには、宛先 `0.0.0.0/0` へのすべてのトラフィックを許可するアウトバウンドルールを追加します。
- VPC 内のリソースのセキュリティグループに、クライアント VPN エンドポイントに適用されるセキュリティグループ (この場合はデフォルトの VPC セキュリティグループ) からのアクセスを許可するルールがあること。これにより、クライアントが VPC 内のリソースにアクセスできるようになります。

詳細については、「セキュリティグループ」を参照してください。

ステップ 7: クライアント VPN エンドポイント設定ファイルをダウンロードする

次のステップでは、クライアント VPN エンドポイント設定ファイルをダウンロードして準備します。設定ファイルには、クライアント VPN エンドポイントの詳細と VPN 接続を確立するために必要な証明書情報が含まれています。このファイルを、クライアント VPN エンドポイントに接続する必要があるエンドユーザーに提供します。エンドユーザーは、このファイルを使用して VPN クライアントアプリケーションを設定します。

クライアント VPN エンドポイント設定ファイルをダウンロードして準備するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. このチュートリアル用に作成したクライアント VPN エンドポイントを選択し、[Download client configuration] (クライアント設定のダウンロード) を選択します。
4. ステップ 1 で生成されたクライアント証明書とキーを見つけます。クライアント証明書とキーは、クローンされた OpenVPN easy-rsa repo の次の場所にあります。
   - クライアント証明書 — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - クライアントキー — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. 任意のテキストエディタを使用して、クライアント VPN エンドポイント設定ファイルを開きます。`<cert></cert>` および `<key></key>` タグをファイルに追加します。次のように、クライアント証明書の内容とプライベートキーの内容を、対応するタグ間に配置します。

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. クライアント VPN エンドポイント設定ファイルを保存して閉じます。
7. クライアント VPN エンドポイント設定ファイルをエンドユーザーに配信します。

クライアント VPN エンドポイント設定ファイルの詳細については、「クライアント設定ファイルをエクスポートして設定する」を参照してください。

ステップ 8: クライアント VPN エンドポイントに接続する

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と、作成したばかりの設定ファイルを使用して、クライアント VPN エンドポイントに接続できます。詳細については、『AWS Client VPN ユーザーガイド』を参照してください。

AWS クライアント VPN の使用

次のトピックでは、Client VPN の操作方法を説明します。

内容

セルフサービスポータルにアクセスする

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有効にした場合、セルフサービスポータルの URL をクライアントに提供できます。クライアントは、ウェブブラウザでポータルにアクセスし、ユーザーベースの認証情報を使用してログインできます。ポータルでは、クライアントはクライアント VPN エンドポイント設定ファイルをダウンロードし、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することができます。

以下のルールが適用されます。

- セルフサービスポータルは、相互認証を使用して認証するクライアントでは利用できません。
- セルフサービスポータルで利用できる設定ファイルは、Amazon VPC コンソールまたは AWS CLI を使用してエクスポートする設定ファイルと同じです。クライアントへの配信前に設定ファイルをカスタマイズする必要がある場合は、カスタマイズしたファイルを自分自身でクライアントに配信する必要があります。

- 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オプションを有効にする必要があります。有効にしないと、クライアントはポータルにアクセスできません。このオプションが有効になっていない場合は、クライアント VPN エンドポイントを変更して有効にすることができます。

セルフサービスポータルオプションを有効にした後、次の URL のいずれかをクライアントに提供します。

- `https://self-service.clientvpn.amazonaws.com/`

  クライアントがこの URL を使用してポータルにアクセスする場合、クライアントは、ログインする前にクライアント VPN エンドポイントの ID を入力する必要があります。
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  上記の URLの *<endpoint-id>* をクライアント VPN エンドポイントの ID (たとえば、`cvpn-endpoint-0123456abcd123456`) に置き換えます。

セルフサービスポータルの URL は、describe-client-vpn-endpoints AWS CLI コマンドの出力にも表示できます。または、URL は Amazon VPC コンソールの [Client VPN Endpoints] (クライアント VPN エンドポイント) ページの [Details] (詳細) タブに表示されます。

フェデレーション認証で使用するためのセルフサービスポータルの設定の詳細については、「セルフサービスポータルのサポート」を参照してください。

承認ルール

承認ルールは、ネットワークへのアクセス許可を与えるファイアウォールルールとして機能します。承認ルールを追加することで、特定のクライアントに対し、特定のネットワークへのアクセス許可を与えます。アクセス許可の対象となるネットワークそれぞれに、承認ルールが必要となります。コンソールと AWS CLI を使用して、クライアント VPN エンドポイントに承認ルールを追加できます。

> **Note**
>
> クライアント VPN は、承認ルールを評価するときに、最長プレフィックスマッチングを使用します。詳細については、Amazon VPC ユーザーガイドの「トピックActive Directory グループの承認ルールが想定どおりに機能しない のトラブルシューティング」および「ルーティングの優先度」を参照してください。

目次

クライアント VPN エンドポイントへの承認ルールの追加

AWS Management Console を使用して、クライアント VPN エンドポイントに承認ルールを追加するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 認可ルールを追加するクライアント VPN エンドポイントを選択し、[Authorization rules] (認可ルール) を選択し、[Add authorization rule] (認可ルールを追加する) を選択します。
4. [Destination network to enable access] (アクセスを有効にする送信先ネットワーク) に、ユーザーがアクセスするネットワークの IP アドレスを CIDR 表記で入力します (VPC の CIDR ブロックなど)。
5. 指定したネットワークにアクセスしてもよいクライアントを指定します。[For grant access to (アクセス権の付与対象)] で、以下のいずれかを行います。

   - すべてのクライアントにアクセス許可を与えるには、[Allow access to all users (すべてのユーザーにアクセスを許可する)] を選択します。
   - 特定のクライアントへのアクセスを制限するには、[特定のアクセスグループのユーザーへのアクセスを許可する] を選択し、[アクセスグループ ID] に、アクセス権限を付与するグループの ID を入力します。たとえば、Active Directory グループのセキュリティ識別子 (SID) か、SAML ベースの ID プロバイダー (IdP) で定義されたグループの ID/名前を指定します。
     - (Active Directory) SID を取得するには、たとえば次のように、Microsoft Powershell の Get-ADGroup コマンドレットを使用できます。

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

       または、[Active Directory Users and Computers (Active Directory ユーザーとコンピュータ)] ツールを開き、グループのプロパティを表示します。続いて、[Attribute Editor (属性エディ

タ)] タブに移動し、objectSID の値を取得します。必要に応じて、まず [View (表示)]、[Advanced Features (高度な機能)] の順に選択して、[Attribute Editor (属性エディタ)] タブを有効にします。

- (SAML ベースのフェデレーション認証) グループの ID/名前は、SAML アサーションで返されるグループ属性情報と一致する必要があります。

6. [説明] に承認ルールの簡単な説明を入力します。
7. [Add authorization rule (承認ルールを追加する)] を選択します。

クライアント VPN エンドポイントに承認ルールを追加するには (AWS CLI)

authorize-client-vpn-ingress コマンドを使用します。

クライアント VPN エンドポイントから承認ルールを削除する

承認ルールを削除すると、指定のネットワークへのアクセス許可が削除されます。

クライアント VPN エンドポイントから承認ルールを削除するには、コンソールまたは AWS CLI を使用します。

クライアント VPN エンドポイントから承認ルールを削除するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 認可ルールが追加されているクライアント VPN エンドポイントを選択し、[Authorization rules] (認可ルール) を選択します。
4. 削除する認可ルールを選択し、[Remove authorization rule] (認可ルールの削除) を選択し、[Remove authorization rule] (認可ルールを削除する) を選択します。

クライアント VPN エンドポイントから承認ルールを削除するには (AWS CLI)

revoke-client-vpn-ingress コマンドを使用します。

承認ルールの表示

特定のクライアント VPN エンドポイントの承認ルールを表示するには、コンソールまたは AWS CLI を使用します。

承認ルールを表示するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 認可ルールを表示するクライアント VPN エンドポイントを選択し、[Authorization rules] (認可ルール) を選択します。

承認ルールを表示するには (AWS CLI)

describe-client-vpn-authorization-rules コマンドを使用します。

承認ルールのシナリオ例

このセクションでは、AWS Client VPN の承認ルールの仕組みについて説明します。承認ルールを理解するための重要なポイント、アーキテクチャの例、およびアーキテクチャの例に対応するシナリオ例の説明が含まれています。

目次

承認ルールを理解するための重要なポイント

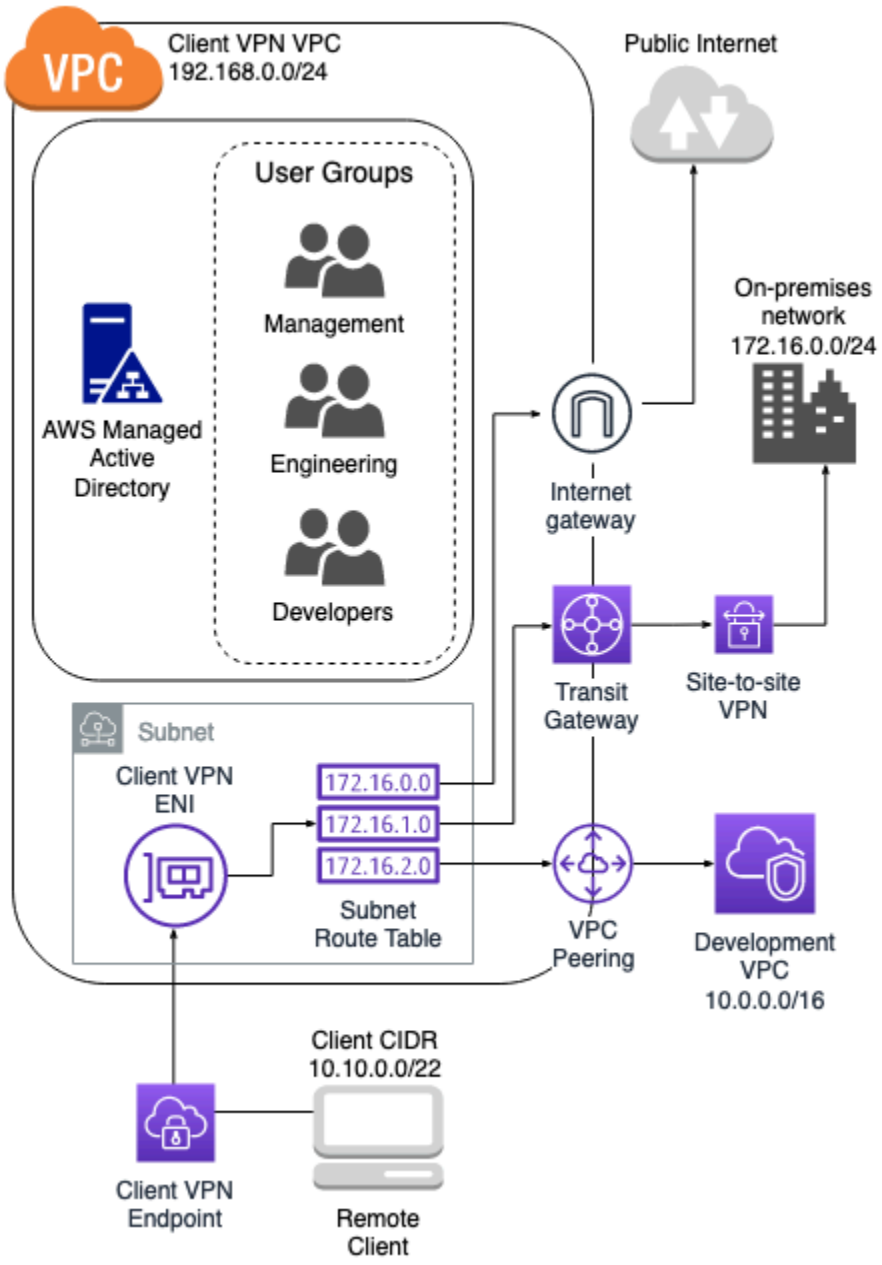
次のポイントは、承認ルールの動作の一部を説明しています。

- 送信先ネットワークへのアクセスを許可するには、許可ルールを明示的に追加する必要があります。デフォルトの動作では、アクセスは拒否されます。

- 送信先ネットワークへのアクセスを制限する承認ルールを追加することはできません。
- 0.0.0.0/0 CIDR は特殊なケースとして扱われます。これは承認ルールの作成順序に関係なく、最後に扱われます。
- 0.0.0.0/0 CIDR は「任意の送信先」または「他の承認ルールで定義されていない任意の送信先」と考えることができます。
- 最も長いプレフィックス一致が、優先されるルールです。

承認ルールシナリオのアーキテクチャの例

次の図は、このセクションのシナリオ例に使用されているアーキテクチャの例を示しています。



シナリオ 1: 単一の送信先へのアクセス

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミ	s-xxxxx14	False	172.16.0.0/24

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
スネットワークへのアクセスを提供する			
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループにクライアント VPN VPC へのアクセスを提供する	s-xxxxx16	False	192.168.0.0/24

結果として生じる動作

- エンジニアリンググループは 172.16.0.0/24 にのみアクセスできます。
- 開発グループは 10.0.0.0/16 にのみアクセスできます。
- マネージャーグループは 192.168.0.0/24 にのみアクセスできます。
- 他のすべてのトラフィックは、クライアント VPN エンドポイントによって削除されます。

> **Note**
>
> このシナリオでは、どのユーザーグループもパブリックインターネットにアクセスできません。

シナリオ 2: 任意の送信先 (0.0.0.0/0) CIDR の使用

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
	s-xxxxx14	False	172.16.0.0/24

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する			
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へのアクセスを提供する	s-xxxxx16	False	0.0.0.0/0

結果として生じる動作

- エンジニアリンググループは 172.16.0.0/24 にのみアクセスできます。
- 開発グループは 10.0.0.0/16 にのみアクセスできます。
- マネージャーグループはパブリックインターネットおよび 192.168.0.0/24 にアクセスできますが、172.16.0.0/24 または 10.0.0/16 にはアクセスできません。

> **Note**
>
> このシナリオでは、どのルールも 192.168.0.0/24 を参照していないため、そのネットワークへのアクセスも 0.0.0.0/0 ルールによって提供されます。0.0.0.0/0 を含むルールは、ルールが作成された順序に関係なく、常に最後に評価されます。このため、0.0.0.0/0 以前に評価されたルールが、0.0.0.0/0 によってアクセス権が付与されるネットワークを決定するうえで役割を果たすことを覚えておいてください。

シナリオ 3: 長い IP プレフィックスの一致

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する	s-xxxxx14	False	172.16.0.0/24
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へのアクセスを提供する	s-xxxxx16	False	0.0.0.0/0
マネージャーグループに開発 VPC 内の単一ホストへのアクセスを提供する	s-xxxxx16	False	10.0.1.66/32

結果として生じる動作

- エンジニアリンググループは 172.16.0.0/24 にのみアクセスできます。
- 開発グループは単一ホスト 10.0.2.119/32 の場合を除き、10.0.0.0/16 にアクセスできます。
- マネージャーグループはパブリックインターネット、192.168.0.0/24、および開発 VPC 内の単一ホスト (10.0.2.119/32) にアクセスできますが、172.16.0.0/24 または開発 VPC 内のその他のホストにはアクセスできません。

> **Note**
>
> ここでは、長い IP プレフィックスを持つルールが、短い IP プレフィックスを持つルールよりも優先されることがわかります。開発グループに 10.0.2.119/32 へのアクセスを許可する場合は、開発チームに 10.0.2.119/32 へのアクセスを許可するルールを追加する必要があります。

シナリオ 4: 重複する CIDR (同じグループ)

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する	s-xxxxx14	False	172.16.0.0/24
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へのアクセスを提供する	s-xxxxx16	False	0.0.0.0/0
マネージャーグループに開発 VPC 内の単一ホストへのアクセスを提供する	s-xxxxx16	False	10.0.1.66/32
エンジニアリンググループがオンプレミ	s-xxxxx14	False	172.16.0.128/25

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
スネットワーク内のより小さなサブネットにアクセスできるようにする			

結果として生じる動作

- 開発グループは単一ホスト 10.0.2.119/32 の場合を除き、10.0.0.0/16 にアクセスできます。
- マネージャーグループはパブリックインターネット、192.168.0.0/24、および 10.0.0.0/16 ネットワーク内の単一ホスト (10.0.2.119/32) にアクセスできますが、172.16.0.0/24 または 10.0.0.0/16 ネットワーク内のその他のホストにはアクセスできません。
- エンジニアリンググループは、より具体的なサブネット 172.16.0.128/25 を含めて、172.16.0.0/24 にアクセスできます。

シナリオ 5: 追加の 0.0.0.0/0 ルール

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する	s-xxxxx14	False	172.16.0.0/24
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へ	s-xxxxx16	False	0.0.0.0/0

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
のアクセスを提供する			
マネージャーグループに開発 VPC 内の単一ホストへのアクセスを提供する	s-xxxxx16	False	10.0.1.66/32
エンジニアリンググループがオンプレミスネットワーク内のより小さなサブネットにアクセスできるようにする	s-xxxxx14	False	172.16.0.128/25
エンジニアリンググループに任意の送信先へのアクセスを提供する	s-xxxxx14	False	0.0.0.0/0

結果として生じる動作

- 開発グループは単一ホスト 10.0.2.119/32 の場合を除き、10.0.0.0/16 にアクセスできます。
- マネージャーグループはパブリックインターネット、192.168.0.0/24、および 10.0.0.0/16 ネットワーク内の単一ホスト (10.0.2.119/32) にアクセスできますが、172.16.0.0/24 または 10.0.0.0/16 ネットワーク内のその他のホストにはアクセスできません。
- エンジニアリンググループは、より具体的なサブネット 172.16.0.128/25 を含めて、パブリックインターネット、192.168.0.0/24、および 172.16.0.0/24 にアクセスできます。

> **Note**
>
> エンジニアリンググループとマネージャーグループの両方が 192.168.0.0/24 にアクセスできるようになりました。これは、どちらのグループも 0.0.0.0/0 (任意の送信先) にアクセスでき、さらに他のどのルールも 192.168.0.0/24 を参照していないためです。

シナリオ 6: 192.168.0.0/24 のルールの追加

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する	s-xxxxx14	False	172.16.0.0/24
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へのアクセスを提供する	s-xxxxx16	False	0.0.0.0/0
マネージャーグループに開発 VPC 内の単一ホストへのアクセスを提供する	s-xxxxx16	False	10.0.1.66/32
エンジニアリンググループにオンプレミスネットワークのサ	s-xxxxx14	False	172.16.0.128/25

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
ブネットへのアクセスを提供する			
エンジニアリンググループに任意の送信先へのアクセスを提供する	s-xxxxx14	False	0.0.0.0/0
マネージャーグループにクライアント VPN VPC へのアクセスを提供する	s-xxxxx16	False	192.168.0.0/24

結果として生じる動作

- 開発グループは単一ホスト 10.0.2.119/32 の場合を除き、10.0.0.0/16 にアクセスできます。
- マネージャーグループはパブリックインターネット、192.168.0.0/24、および 10.0.0.0/16 ネットワーク内の単一ホスト (10.0.2.119/32) にアクセスできますが、172.16.0.0/24 または 10.0.0.0/16 ネットワーク内のその他のホストにはアクセスできません。
- エンジニアリンググループは、パブリックインターネット、172.16.0.0/24、および 172.16.0.128/25 にアクセスできます。

> **Note**
>
> マネージャーグループが 192.168.0.0/24 にアクセスするルールを追加する方法によって、開発グループはその送信先ネットワークにアクセスできなくなることに注意してください。

シナリオ 7: すべてのユーザーグループのアクセス

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
エンジニアリンググループにオンプレミスネットワークへのアクセスを提供する	s-xxxxx14	False	172.16.0.0/24
開発グループに開発 VPC へのアクセスを提供する	s-xxxxx15	False	10.0.0.0/16
マネージャーグループに任意の送信先へのアクセスを提供する	s-xxxxx16	False	0.0.0.0/0
マネージャーグループに開発 VPC 内の単一ホストへのアクセスを提供する	s-xxxxx16	False	10.0.1.66/32
エンジニアリンググループにオンプレミスネットワークのサブネットへのアクセスを提供する	s-xxxxx14	False	172.16.0.128/25
エンジニアリンググループにすべてのネットワークへのアクセスを提供する	s-xxxxx14	False	0.0.0.0/0

ルールの説明	グループ ID	すべてのユーザーにアクセスを許可する	送信先 CIDR
マネージャーグループにクライアント VPN VPC へのアクセスを提供する	s-xxxxx16	False	192.168.0.0/24
すべてのグループへのアクセスを提供する	該当なし	True	0.0.0.0/0

結果として生じる動作

- 開発グループは単一ホスト 10.0.2.119/32 の場合を除き、10.0.0.0/16 にアクセスできます。
- マネージャーグループはパブリックインターネット、192.168.0.0/24、および 10.0.0.0/16 ネットワーク内の単一ホスト (10.0.2.119/32) にアクセスできますが、172.16.0.0/24 または 10.0.0.0/16 ネットワーク内のその他のホストにはアクセスできません。
- エンジニアリンググループは、パブリックインターネット、172.16.0.0/24、および 172.16.0.128/25 にアクセスできます。
- 他のユーザーグループ (「管理者グループ」など) は、パブリックインターネットにアクセスできますが、他のルールで定義された他の送信先ネットワークにはアクセスできません。

クライアント証明書失効リスト

クライアント証明書失効リストを使用して、特定のクライアント証明書のクライアント VPN エンドポイントへのアクセスを取り消すことができます。

> **Note**
>
> サーバーとクライアント証明書の生成の詳細については、「相互認証」を参照してください。

クライアント証明書失効リストに追加できるエントリ数の詳細については、「クライアント VPN クォータ」を参照してください。

目次

クライアント証明書失効リストの生成

Linux/macOS

次の手順では、クライアント証明書失効リストの生成に OpenVPN の Easy-RSA というコマンドラインユーティリティを使用してください。

OpenVPN Easy-RSA を使ってクライアント証明書失効リストを生成するには

1. 証明書の生成に使用した easyrsa インストールをホストしているサーバーにログインします。
2. ローカルリポジトリの `easy-rsa/easyrsa3` フォルダに移動します。

```
$ cd easy-rsa/easyrsa3
```

3. クライアント証明書を取り消し、クライアント失効リストを生成します。

```
$ ./easyrsa revoke client1.domain.tld
$ ./easyrsa gen-crl
```

プロンプトが表示されたら、「`yes`」と入力します。

Windows

次の手順では、OpenVPN ソフトウェアを使用してクライアント失効リストを生成します。ここでは、OpenVPN ソフトウェアを使用してクライアントとサーバーの証明書およびキーを生成するステップに従っていることを前提としています。

EasyRSA version 3.x.x を使ってクライアント証明書失効リストを生成するには

1. コマンドプロンプトを開き、EasyRSA-3.x.x ディレクトリに移動します。これは、お使いのシステムにインストールされている場所に依存します。

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. 「EasyRSA-Start.bat」ファイルを実行して EasyRSA シェルを実行します。

```
C:\> .\EasyRSA-Start.bat
```

3. EasyRSA シェルで、クライアント証明書を取り消します。

```
# ./easyrsa revoke client_certificate_name
```

4. プロンプトが表示されたら、「yes」(はい) と入力します。
5. クライアント証明書失効リストを生成します。

```
# ./easyrsa gen-crl
```

6. クライアント失効リストは、次の場所に作成されます。

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

以前の EasyRSA バージョンを使用してクライアント証明書失効リストを生成するには

1. コマンドプロンプトを開き、OpenVPN ディレクトリに移動します。

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. `vars.bat` ファイルを実行します。

```
C:\> vars
```

3. クライアント証明書を取り消し、クライアント失効リストを生成します。

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

クライアント証明書失効リストのインポート

インポートするクライアント証明書失効リストを持っている必要があります。クライアント証明書失効リストの生成の詳細については、「クライアント証明書失効リストの生成」を参照してください。

クライアント証明書失効リストのインポートには、コンソールと AWS CLI が使用できます。

クライアント証明書失効リストをインポートするには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアント証明書失効リストをインポートするクライアント VPN エンドポイントを選択します。
4. [Actions] を選択し、[Import Client Certificate CRL (クライアント証明書 CRL のインポート)] を選択します。
5. [Certificate Revocation List] (証明書失効リスト) で、クライアント証明書失効リストファイルの内容を入力し、[Import client certificate CRL] (クライアント証明書 CRL のインポート) を選択します。

クライアント証明書失効リストをインポートするには (AWS CLI)

import-client-vpn-client-certificate-revocation-list コマンドを使用します。

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

クライアント証明書失効リストのエクスポート

クライアント証明書失効リストのエクスポートには、コンソールと AWS CLI が使用できます。

クライアント証明書失効リストをエクスポートするには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。

3. クライアント証明書失効リストをエクスポートするクライアント VPN エンドポイントを選択します。
4. [Actions] (アクション) を選択し、[Export Client Certificate CRL] (クライアント証明書 CRL のエクスポート) を選択し、[Export Client Certificate CRL] (クライアント証明書 CRL をエクスポートする) を選択します。

クライアント証明書失効をエクスポートするには (AWS CLI)

export-client-vpn-client-certificate-revocation-list コマンドを使用します。

クライアント接続

接続とは、クライアントによって確立された VPN セッションを指します。クライアントがクライアント VPN エンドポイントに正常に接続したとき、接続が確立されたことになります。

目次

クライアント接続の表示

コンソールの表示には、コンソールと AWS CLI が使用できます。接続情報には、クライアント CIDR 範囲から割り当てられた IP アドレスが含まれます。

クライアント接続を表示するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアント接続を表示するクライアント VPN エンドポイントを選択します。
4. [Connections (接続)] タブを選択します。[Connections (接続)] タブに、すべてのアクティブなクライアント接続と終了されたクライアント接続が一覧表示されます。

クライアント接続を表示するには (AWS CLI)

describe-client-vpn-connections コマンドを使用します。

クライアント接続の終了

クライアント接続を終了すると、VPN セッションが終了します。

クライアント接続の終了には、コンソールと AWS CLI が終了できます。

クライアント接続を終了するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアントが接続しているクライアント VPN エンドポイントを選択し、[Connections] を選択します。
4. 終了する接続を選択し、 [Terminate Connection (接続の終了)] 、続いて [Terminate Connection (接続の終了)] を選択します。

クライアント接続を終了するには (AWS CLI)

terminate-client-vpn-connections コマンドを使用します。

クライアントログインバナー

AWS Client VPN は、VPN セッションの確立時に、AWS が提供する Client VPN デスクトップアプリケーションにテキストバナーを表示するオプションを提供します。規制およびコンプライアンスのニーズを満たすために、テキストバナーのコンテンツを定義できます。最大 1400 の UTF-8 エンコード文字が使用できます。

> **Note**
>
> クライアントログインバナーが有効になっている場合、新しく作成された VPN セッションでのみ表示されます 既存の VPN セッションは中断されませんが、既存のセッションが再確立されるとバナーが表示されます。

クライアントデスクトップアプリケーションの詳細については、AWS Client VPN ユーザーガイドの「AWS が提供するクライアントのリリースノート」を参照してください。

目次

Client VPN エンドポイント作成時のクライアントログインバナーを設定する

Client VPN エンドポイントの作成時にクライアントログインバナーを有効にする詳細手順については、「クライアント VPN エンドポイントを作成する」を参照してください。

既存の Client VPN エンドポイントにクライアントログインバナーを設定する

既存の Client VPN エンドポイントにクライアントログインバナーを設定するには、以下のステップを実行します。

Client VPN エンドポイント (コンソール)でクライアントログインバナーを有効にする

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN Endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. ページを下にスクロールして、[Other parameters] (その他のパラメータ) セクションに移動します。
5. [Enable client login banner] (クライアントログインバナーを有効にする) をオンにします。
6. [Client login banner text] (クライアントログインバナーテキスト) で、VPN セッションの確立時に AWS 提供のクライアントのバナーに表示されるテキストを入力します。UTF-8 でエンコードされた文字のみ、最大 1400 文字を使用できます。
7. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

Client VPN エンドポイントでクライアントログインバナーを有効にする (AWS CLI)

modify-client-vpn-endpoint コマンドを使用します。

既存のクライアント VPN エンドポイントのクライアントログインバナーを無効にする

以下のステップを実行して、既存のクライアント VPN エンドポイントのクライアントログインバナーを無効にします。

クライアント VPN エンドポイントのクライアントログインバナーを無効にする (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. ページを下にスクロールして、[Other parameters] (その他のパラメータ) セクションに移動します。
5. [Enable client login banner?] (クライアントログインバナーを有効にしますか) をオフにします。
6. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

クライアント VPN エンドポイントのクライアントログインバナーを無効にする (AWS CLI)

modify-client-vpn-endpoint コマンドを使用します。

Client VPN エンドポイントで使用している既存のバナーテキストを変更する

次のステップを実行して、既存のクライアントログインバナーのテキストを変更します。

Client VPN エンドポイントで使用している既存のバナーテキストを変更する (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN Endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。

4. [Enable client login banner?] (クライアントログインバナーを有効にしますか?) がオンになっていることを確認します。
5. [Client login banner text] (クライアントログインバナーテキスト) で、VPN セッションが確立されたときに、AWS が提供するクライアントのバナーに表示する既存のテキストを新しいテキストで置き換えます。最大 1400 の UTF-8 エンコード文字のみ使用できます。
6. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

Client VPN エンドポイントのクライアントログインバナーを変更する (AWS CLI)

modify-client-vpn-endpoint コマンドを使用します。

現在設定されているログインバナーを表示する

現在設定されているログインバナーを表示するには、次のステップを実行します。

Client VPN エンドポイントで使用している現在のログインバナーを表示する (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 表示する Client VPN エンドポイントを選択します。
4. [Details] (詳細) タブが選択されていることを確認します。
5. [Client login banner text] (クライアントログインバナーテキスト) の横に、現在設定されているログインバナーテキストが表示されます。

Client VPN エンドポイントで、現在設定されているログインバナーを表示する (AWS CLI)

describe-client-vpn-endpoints コマンドを使用します。

クライアント VPN エンドポイント

すべてのクライアント VPN セッションは、クライアント VPN エンドポイントで終了します。クライアント VPN エンドポイントによってすべてのクライアント VPN セッションが管理、制御されるよう設定を行います。

内容

- クライアント VPN エンドポイントを変更する
- クライアント VPN エンドポイントを表示する
- クライアント VPN エンドポイントを削除する

クライアント VPN エンドポイントを作成する

クライアントが VPN セッションを確立できるようにするには、クライアント VPN エンドポイントを作成します。

クライアント VPN は、該当するターゲットネットワークがプロビジョニングされているのと同じ AWS アカウントに作成する必要があります。

前提条件

作業を開始する前に、次のことを必ず実行してください。

- のルールとベストプラクティス AWS Client VPN のルールと制限を確認します。
- サーバー証明書を生成し、必要に応じてクライアント証明書を取得します。詳細については、「クライアント承認」を参照してください。

クライアント VPN エンドポイントを作成するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Client VPN Endpoint (クライアント VPN エンドポイント)] を選択し、[Create Client VPN Endpoint (クライアント VPN エンドポイントの作成)] を選択します。
3. (オプション) クライアント VPN エンドポイントの名前タグと説明を入力します。
4. [Client IPv4 CIDR] (クライアント IPv4 CIDR) に、クライアント IP アドレスを割り当てる IP アドレス範囲を CIDR 表記で指定します。たとえば、`10.0.0.0/22` と指定します。

> **Note**
>
> IP アドレス範囲は、ターゲットネットワークのアドレス範囲、VPC のアドレス範囲、またはクライアント VPN エンドポイントに関連付けられるルートと重複できません。クライアントアドレス範囲は /22 以上で、/12 CIDR ブロックサイズを超えないようにする必要があります。クライアント VPN エンドポイントの作成後にクライアントのアドレス範囲を変更することはできません。

5. [Server certificate ARN (サーバー証明書 ARN)] に、サーバーによって使用される TLS 証明書の ARN を指定します。クライアントは、接続先のクライアント VPN エンドポイントを認証するためにサーバー証明書を使用します。

> **Note**
>
> サーバー証明書は、クライアント VPN エンドポイントを作成しているリージョンの AWS Certificate Manager (ACM) に存在する必要があります。証明書は ACM でプロビジョニングするか、ACM にインポートすることができます。

6. VPN 接続を確立するとき、クライアントを認証するために使用する認証方法を指定します。認証方法を選択する必要があります。

- ユーザーベースの認証を使用するには、[ユーザーベースの認証を使用] を選択し、次のいずれかを選択します。
  - Active Directory 認証: Active Directory 認証の場合はこのオプションを選択します。[ディレクトリ ID] には、使用する Active Directory の ID を指定します。
  - フェデレーション認証: SAML ベースのフェデレーション認証の場合は、このオプションを選択します。

    [SAML プロバイダー ARN] には、IAM SAML ID プロバイダーの ARN を指定します。

    (オプション) [Self-service SAML provider ARN (セルフサービス SAML プロバイダー ARN)] で、セルフサービスポータルをサポートするために作成した IAM SAML ID プロバイダーの ARN を指定します (該当する場合)。
- 相互証明書認証を使用するには、[Use mutual authentication] (相互認証の使用) を選択し、[Client certificate ARN] (クライアント証明書 ARN) で AWS Certificate Manager (ACM) でプロビジョニングしたクライアント証明書の ARN を指定します。

> **Note**
>
> サーバー証明書とクライアントの証明書が同じ認証機関 (CA) によって発行されている場合、サーバーとクライアントの両方に対してサーバー証明書 ARN を使用できます。クライアント証明書が別の CA によって発行された場合は、クライアント証明書 ARN を指定する必要があります。

7. (オプション) 接続ログ記録 で、Amazon CloudWatch Logs を使用してクライアント接続に関するデータをログに記録するかどうかを指定します。[Enable log details on client connections] (ク

ライアント接続の詳細のログを有効にする) をオンにします。CloudWatch Logs ロググループ名に、使用するロググループの名前を入力します。CloudWatch Logs ログストリーム名 には、使用するログストリームの名前を入力するか、このオプションを空白のままにしてログストリームを作成できるようにします。

8. (オプション) クライアント VPN エンドポイントへの新しい接続を許可または拒否するカスタムコードを実行するには、[Client Connect Handler] (クライアント接続ハンドラー) で、[Enable client connect handler] (クライアント接続ハンドラーを有効にする) をオンにします。[Client Connect Handler ARN (クライアント接続ハンドラー ARN)] で、接続を許可または拒否するロジックを含む Lambda 関数の Amazon リソースネーム (ARN) を指定します。
9. (オプション) DNS 解決に使用する DNS サーバーを指定します。カスタム DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] と [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] に、使用する DNS サーバーの IP アドレスを指定します。VPC DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] または [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] のいずれかに IP アドレスを指定し、VPC DNS サーバー IP アドレスを追加します。

> **Note**
>
> クライアントが DNS サーバーに到達できることを確認します。

10. (オプション) デフォルトでは、クライアント VPN エンドポイントは UDP 転送プロトコルを使用します。代わりに TCP トランスポートプロトコルを使用するには、[Transport Protocol (トランスポートプロトコル)] の [TCP] を選択します。

> **Note**
>
> UDP は通常、TCP よりも優れたパフォーマンスが得られます。クライアント VPN エンドポイントを作成した後で、トランスポートプロトコルを変更することはできません。

11. (オプション) エンドポイントをスプリットトンネルクライアント VPN エンドポイントにするには、[Enable split-tunnel] (スプリットトンネルを有効にする) をオンにします。デフォルトでは、Client VPN エンドポイントの分割トンネルは無効になっています。
12. (オプション) [VPC ID] で、クライアント VPN エンドポイントに関連付ける VPC を選択します。[セキュリティグループ ID] で、クライアント VPN エンドポイントに適用する VPC のセキュリティグループを 1 つ以上選択します。
13. (オプション) [VPN port (VPN ポート)] で、VPN ポート番号を選択します。デフォルトは 443 です。

14. (オプション) クライアントのセルフサービスポータルの URL を生成するには、[Enable self-service portal] (セルフサービスポータルを有効にする) を選択します。
15. (オプション) [Session timeout hours] (セッションタイムアウト時間) で、使用可能なオプションから希望する最大 VPN セッション継続時間を時間単位で選択するか、デフォルトの 24 時間のままにしておきます。
16. (オプション) クライアントログインバナーテキストを有効にするか指定します。[Enable client login banner] (クライアントログインバナーを有効にする) をオンにします。[Client login banner text] (クライアントログインバナーテキスト) に、VPN セッションが確立されたときに AWS が提供するクライアントのバナーに表示されるテキストを入力します。UTF-8 でエンコードされた文字のみ。最大 1400 文字。
17. [Create Client VPN endpoint] (クライアント VPN エンドポイントの作成) を選択します。

クライアント VPN エンドポイントを作成したら、次の手順を実行して設定を完了し、クライアントが接続できるようにします。

- クライアント VPN エンドポイントの初期状態は `pending-associate` です。最初のターゲットネットワークを関連付けて初めて、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るようになります。
- 承認ルールを作成して、ネットワークにアクセスできるクライアントを指定します。
- クライアントに配布するクライアント VPN エンドポイント設定ファイルをダウンロードして準備します。
- AWS 提供の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、クライアント VPN エンドポイントに接続するようクライアントに指定します。詳細については、『AWS Client VPN ユーザーガイド』を参照してください。

クライアント VPN エンドポイントを作成するには (AWS CLI)

create-client-vpn-endpointコマンドを実行します。

クライアント VPN エンドポイントを変更する

クライアント VPN を作成した後、次の設定を変更できます。

- 説明
- サーバー証明書
- クライアント接続ログオプション

- クライアント接続ハンドラーのオプション
- DNS サーバー
- スプリットトンネルオプション
- ルート (分割トンネルオプションを使用する場合)
- 証明書失効リスト (CRL)
- 承認ルール
- VPC とセキュリティグループの関連付け
- VPN ポート番号
- セルフサービスポータルオプション
- VPN セッションの最大継続時間
- クライアントログインバナーテキストを有効または無効にする
- クライアントログインバナーテキスト

> **Note**
>
> Client VPN エンドポイントへの変更 (証明書失効リスト (CRL) の変更を含む) は、Client VPN サービスによってリクエストが受け入れられてから 4 時間以内に有効になります。
> クライアント VPN エンドポイントの作成後に、クライアントの IPv4 CIDR 範囲、認証オプション、クライアント証明書またはトランスポートプロトコルを変更することはできません。

クライアント VPN エンドポイントで次のいずれかのパラメータを変更すると、接続がリセットされます。

- サーバー証明書
- DNS サーバー
- スプリットトンネルオプション (サポートをオンまたはオフ)
- ルート (スプリットトンネルオプションを使用する場合)
- 証明書失効リスト (CRL)
- 承認ルール
- VPN ポート番号

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントを変更できます。

クライアント VPN エンドポイントを変更するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. (オプション) [Description] (説明) で、クライアント VPN エンドポイントの簡単な説明を入力します。
5. [Server certificate ARN (サーバー証明書 ARN)] に、サーバーによって使用される TLS 証明書の ARN を指定します。クライアントは、接続先のクライアント VPN エンドポイントを認証するためにサーバー証明書を使用します。

   > **Note**
   >
   > サーバー証明書は、クライアント VPN エンドポイントを作成しているリージョンの AWS Certificate Manager (ACM) に存在する必要があります。証明書は ACM でプロビジョニングするか、ACM にインポートすることができます。

6. Amazon CloudWatch Logs を使用してクライアント接続に関するデータをログに記録するかどうかを指定します。[Enable log details on client connections] (クライアント接続の詳細のログを有効にする) で、次のいずれかの操作を行います。

   - クライアント接続のログを有効にするには、[Enable log details on client connections] (クライアント接続の詳細なログを有効にする) をオンにします。CloudWatch Logs ロググループ名 で、使用するロググループの名前を選択します。CloudWatch Logs ログストリーム名 で、使用するログストリームの名前を選択するか、このオプションを空白のままにしてログストリームを作成できるようにします。
   - クライアント接続のログを無効にするには、[Enable log details on client connections] (クライアント接続の詳細なログを有効にする) をオフにします。

7. [Client connect handler] (クライアント接続ハンドラー) で、クライアント接続ハンドラーを有効にするには、[Enable client connect handler] (クライアント接続ハンドラーを有効にする) をオンにします。[Client Connect Handler ARN (クライアント接続ハンドラー ARN)] で、接続を許可または拒否するロジックを含む Lambda 関数の Amazon リソースネーム (ARN) を指定します。

8. [Enable DNS servers] (DNS サーバーを有効にする) をオンまたはオフにします。カスタム DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] と [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] に、使用する DNS サーバーの IP アドレスを指定します。VPC DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] または [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] のいずれかに IP アドレスを指定し、VPC DNS サーバー IP アドレスを追加します。

   > **Note**
   >
   > クライアントが DNS サーバーに到達できることを確認します。

9. [Enable split-tunnel] (分割トンネルを有効にする) をオンまたはオフにします。デフォルトでは、VPN エンドポイントの分割トンネルは無効です。
10. [VPC ID] で、クライアント VPN エンドポイントに関連付ける VPC を選択します。[セキュリティグループ ID] で、クライアント VPN エンドポイントに適用する VPC のセキュリティグループを 1 つ以上選択します。
11. [VPN port] (VPN ポート) で、VPN ポート番号を選択します。デフォルトは 443 です。
12. クライアントのセルフサービスポータルの URL を生成するには、[Enable self-service portal] (セルフサービスポータルを有効にする) をオンにします。
13. [Session timeout hours] (セッションタイムアウト時間) で、使用可能なオプションから目的の最大 VPN セッション継続時間 (時間単位) を選択するか、デフォルトの 24 時間のままに設定しておきます。
14. [Enable client login banner] (クライアントログインバナーを有効にする) をオンまたはオフにします。クライアントログインバナーを使用する場合は、VPN セッションが確立されたときに AWS が提供するクライアントのバナーに表示されるテキストを入力します。UTF-8 でエンコードされた文字のみ。最大 1400 文字。
15. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

クライアント VPN エンドポイントを変更するには (AWS CLI)

modify-client-vpn-endpointコマンドを実行します。

クライアント VPN エンドポイントを表示する

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントに関する情報を表示できます。

クライアント VPN エンドポイントルートを表示するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 表示するクライアント VPN エンドポイントを選択します。
4. [Details] (詳細)、[Target network associations] (ターゲットネットワーク関連付け)、[Security groups] (セキュリティグループ)、[Authorization rules] (認可ルール)、[Route table] (ルートテーブル)、[Connections] (接続)、および [Tags] (タグ) タブを使用して、既存のクライアント VPN エンドポイントに関する情報を表示します。

   フィルターを使用して、検索を絞り込むこともできます。

クライアント VPN エンドポイントを表示するには (AWS CLI)

describe-client-vpn-endpointsコマンドを実行します。

クライアント VPN エンドポイントを削除する

クライアント VPN エンドポイントを削除する前に、すべてのターゲットネットワークの関連付けを解除する必要があります。クライアント VPN エンドポイントを削除すると、そのステータスは `deleting` に変わり、クライアントが接続できなくなります。

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントを削除できます。

クライアント VPN エンドポイントを削除するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 削除するクライアント VPN エンドポイントを選択します。[Actions] (アクション)、[Delete Client VPN endpoint] (クライアント VPN エンドポイントの削除) の順に選択します。
4. 確認ウィンドウに delete と入力して、[Delete] (削除) を選択します。

クライアント VPN エンドポイントを削除するには (AWS CLI)

delete-client-vpn-endpointコマンドを実行します。

接続ログの操作

新規または既存のクライアント VPN エンドポイントの接続ログを有効にして、接続ログのキャプチャを開始できます。

開始する前に、アカウントに CloudWatch Logs ロググループが必要です。詳細については、Amazon CloudWatch Logs ユーザーガイドの「ロググループとログストリームの操作」を参照してください。CloudWatch Logs の使用には料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

接続ログを有効にすると、ロググループ内のログストリームの名前を指定できます。ログストリームを指定しない場合、クライアント VPN サービスによって自動的に作成されます。

新しいクライアント VPN エンドポイントの接続ログを有効にする

コンソールまたはコマンドラインを使用して新しいクライアント VPN エンドポイントを作成するときに、接続ログを有効にできます。

コンソールを使用して新しいクライアント VPN エンドポイントの接続ログを有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Client VPN Endpoints] (クライアント VPN エンドポイント) を選択し、[Create Client VPN endpoint] (クライアント VPN エンドポイントの作成) を選択します。
3. [接続ログ] セクションが表示されるまでオプションを完了します。オプションの詳細については、「クライアント VPN エンドポイントを作成する」を参照してください。
4. [Connection logging] (接続ログ) の [Enable log details on client connections] (クライアント接続の詳細なログを有効にする) をオンにします。
5. [CloudWatch Logs ロググループ名] で、CloudWatch Logs ロググループの名前を選択します。
6. (オプション) [CloudWatch Logs ログストリーム名] で、CloudWatch Logs ログストリームの名前を選択します。
7. [Create Client VPN endpoint] (クライアント VPN エンドポイントの作成) を選択します。

AWS CLI を使用して新しいクライアント VPN エンドポイントの接続ログを有効にするには

create-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。次の例に示すように、接続ログ情報を JSON 形式で指定できます。

```
{
```

```
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

既存のクライアント VPN エンドポイントの接続ログを有効にする

コンソールまたはコマンドラインを使用して、既存のクライアント VPN エンドポイントの接続ログを有効にできます。

コンソールを使用して既存のクライアント VPN エンドポイントの接続ログを有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. [Connection logging] (接続ログ) の [Enable log details on client connections] (クライアント接続の詳細なログを有効にする) をオンにします。
5. [CloudWatch Logs ロググループ名] で、CloudWatch Logs ロググループの名前を選択します。
6. (オプション) [CloudWatch Logs ログストリーム名] で、CloudWatch Logs ログストリームの名前を選択します。
7. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

AWS CLI を使用して既存のクライアント VPN エンドポイントの接続ログを有効にするには

modify-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。次の例に示すように、接続ログ情報を JSON 形式で指定できます。

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

接続ログの表示

CloudWatch Logs コンソールを使用して、接続ログを表示できます。

コンソールを使用して接続ログを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[ロググループ] を選択し、接続ログを含むロググループを選択します。
3. クライアント VPN エンドポイントのログストリームを選択します。

> **Note**
>
> [タイムスタンプ] 列には、接続の時刻ではなく、接続ログが CloudWatch Logs にパブリッシュされた時刻が表示されます。

ログデータの検索の詳細については、『Amazon CloudWatch Logs ユーザーガイド』の「フィルターパターンを使用したログデータ検索」を参照してください。

接続ログを無効にする

コンソールまたはコマンドラインを使用して、クライアント VPN エンドポイントの接続ログを無効にできます。接続ログを無効にしても、CloudWatch Logs の既存の接続ログは削除されません。

コンソールを使用して接続ログを無効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. [Connection logging] (接続ログ) の [Enable log details on client connections] (クライアント接続の詳細なログを有効にする) をオフにします。
5. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

AWS CLI を使用して接続ログを無効にするには

modify-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。`Enabled` が `false` に設定されていることを確認します。

クライアント設定ファイルをエクスポートして設定する

クライアント VPN エンドポイント設定ファイルは、クライアント (ユーザー) がクライアント VPN エンドポイントとの VPN 接続を確立するために使用するファイルです。このファイルをダウンロード (エクスポート) し、VPN へのアクセスを必要とするすべてのクライアントに配布する必要があります。または、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有効にした場合、クライアントはポータルにログインして、構成ファイルを自身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にアクセスする」を参照してください。

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は、ダウンロードする .ovpn 設定ファイルにクライアント証明書とクライアントプライベートキーを追加する必要があります。お客様が情報を追加した後、クライアントは .ovpn ファイルを OpenVPN クライアントソフトウェアにインポートできます。

> **Important**
>
> クライアント証明書とクライアントプライベートキー情報をファイルに追加しない場合、相互認証を使用して認証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。

デフォルトでは、OpenVPN クライアント設定のremote-random-hostname「」オプションはワイルドカード DNS を有効にします。ワイルドカード DNS が有効になっているため、クライアントはエンドポイントの IP アドレスをキャッシュしません。そのため、エンドポイントの DNS 名に ping を実行することはできません。

クライアント VPN エンドポイントが Active Directory 認証を使用しており、クライアント設定ファイルの配布後にディレクトリで Multi-Factor Authentication (MFA) を有効にした場合は、新しいファイルをダウンロードしてクライアントに再配布する必要があります。クライアントは、以前の設定ファイルを使用してクライアント VPN エンドポイントに接続することはできません。

クライアント設定ファイルをエクスポートする

コンソールまたは AWS CLI を使用して、クライアント設定をエクスポートできます。

クライアント設定をエクスポートするには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. クライアント設定をダウンロードするクライアント VPN エンドポイントを選択し、[クライアント設定のダウンロード] を選択します。

クライアント設定をエクスポートするには (AWS CLI)

export-client-vpn-client-configuration コマンドを使用して、出力ファイル名を指定します。

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

クライアント証明書とキー情報を追加する (相互認証)

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は、ダウンロードする .ovpn 設定ファイルにクライアント証明書とクライアントプライベートキーを追加する必要があります。

相互認証を使用する場合は、クライアント証明書を変更できません。

クライアント証明書とキー情報を追加するには (相互認証)

次のオプションの 1 つを使用できます。

(オプション 1) クライアント証明書とキーを、クライアント VPN エンドポイント設定ファイルとともにクライアントに配布します。この場合、設定ファイルで証明書とキーへのパスを指定します。任意のテキストエディタを使用して設定ファイルを開き、以下をファイルの最後に追加します。*/path/* をクライアント証明書とキーの場所に置き換えます (この場所は、エンドポイントに接続しているクライアントから見た相対的な位置です)。

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(オプション 2) <cert></cert> タグ間のクライアント証明書の内容と、<key></key> タグ間のプライベートキーの内容を設定ファイルに追加します。このオプションを選択した場合、設定ファイルのみをクライアントに配布します。

クライアント VPN エンドポイントに接続するユーザーごとに個別のクライアント証明書とキーを生成した場合は、ユーザーごとにこのステップを繰り返します。

クライアント証明書とキーを含むクライアント VPN 設定ファイルの形式の例を次に示します。

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

ルート

各クライアント VPN エンドポイントには、利用可能な送信先ネットワークルートを説明したルートテーブルがあります。ルートテーブルのルートによって、ネットワークトラフィックの振り分け先が決まります。送信先ネットワークにどのクライアントがアクセスできるかを指定するため、各クライアント VPN エンドポイントルートに対して承認ルールを設定する必要があります。

VPC のサブネットをクライアント VPN エンドポイントに関連付けると、クライアント VPN エンドポイントのルートテーブルにその VPC 用のルートが自動的に追加されます。ピア接続 VPC、オンプレミスネットワーク、ローカルネットワーク (クライアントが相互に通信できるようにする場合)、インターネットなど、追加のネットワークへのアクセスを有効にするには、クライアント VPN エンドポイントのルートテーブルにルートを手動で追加する必要があります。

> **Note**
>
> クライアント VPN エンドポイントに複数のサブネットを関連付ける場合は、ここで説明するように、サブネットごとにルートを作成する必要があります ピア接続 VPC、Amazon S3、またはインターネットへのアクセスが断続的である。関連する各サブネットには、同一のルートセットが必要です。

目次

クライアント VPN エンドポイントの分割トンネルに関する考慮事項

クライアント VPN エンドポイントで分割トンネルを使用する場合、VPN が確立されると、クライアント VPN ルートテーブル内のすべてのルートがクライアントルートテーブルに追加されます。VPN の確立後にルートを追加する場合は、新しいルートがクライアントに送信されるように接続をリセットする必要があります。

クライアント VPN エンドポイントルートテーブルを変更する前に、クライアントデバイスが処理できるルート数を考慮することをお勧めします。

エンドポイントルートの作成

ルートを作成する際、送信先ネットワークへのトラフィックをどのように振り分けるかを指定します。

クライアントがインターネットにアクセスできるようにするには、送信先 `0.0.0.0/0` ルートを追加します。

コンソールと AWS CLI を使用して、クライアント VPN エンドポイントにルートを追加できます。

クライアント VPN エンドポイントルートを作成するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. ルートを追加するクライアント VPN エンドポイントを選択し、[Route table] (ルートテーブル)、[Create route] (ルートの作成) の順に選択します。
4. [Route destination (ルートの送信先)] で、送信先ネットワークの IPv4 CIDR 範囲を指定します。例:
   - クライアント VPN エンドポイントの VPC 用のルートを追加するには、VPC の IPv4 CIDR 範囲を入力します。
   - インターネット接続用のルートを追加するには、「`0.0.0.0/0`」を入力します。
   - ピア接続 VPC 用のルートを追加するには、ピア接続 VPC の IPv4 CIDR 範囲を入力します。
   - オンプレミスネットワーク用のルートを追加するには、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力します。
5. [[Subnet ID for target network association] (ターゲットネットワーク関連付けのサブネット ID) で、クライアント VPN エンドポイントに関連付けられているサブネットを選択します。

   または、ローカルクライアント VPN エンドポイントネットワークのルートを追加する場合は、`local` を選択します。
6. (オプション) [Description] (説明) に、ルートの簡単な説明を入力します。
7. [ルートの作成] を選択します。

クライアント VPN エンドポイントルートを作成するには (AWS CLI)

create-client-vpn-route コマンドを使用します。

エンドポイントルートの表示

コンソールまたは AWS CLI を使用して、特定のクライアント VPN エンドポイントのルートを表示できます。

クライアント VPN エンドポイントルートを表示するには (コンソール)

1. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
2. ルートを表示するクライアント VPN エンドポイントを選択し、[Route table] (ルートテーブル) を選択します。

クライアント VPN エンドポイントルートを表示するには (AWS CLI)

describe-client-vpn-routes コマンドを使用します。

エンドポイントルートの削除

削除できるのは、手動で追加したルートに限られます。クライアント VPN エンドポイントにサブネットを関連付けた際に自動的に追加されたルートは、削除できません。自動的に追加されたルートを削除するには、その作成のきっかけとなったサブネットのクライアント VPN エンドポイントへの関連付けを解除する必要があります。

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントからルートを削除できます。

クライアント VPN エンドポイントルートを削除するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. ルートを削除するクライアント VPN エンドポイントを選択し、[Route table] (ルートテーブル) を選択します。
4. 削除するルートを選択し、[Delete route] (ルートの削除)、[Delete route] (ルートを削除する) の順に選択します。

クライアント VPN エンドポイントルートを削除するには (AWS CLI)

delete-client-vpn-route コマンドを使用します。

ターゲットネットワーク

ターゲットネットワークは、VPC のサブネットです。クライアントがクライアント VPN エンドポイントに接続し、VPN 接続を確立するためには、クライアント VPN エンドポイントに少なくとも 1 つのターゲットネットワークが必要です。

設定できるアクセスの種類 (クライアントからインターネットへのアクセスなど) の詳細については、「AWS クライアント VPN のシナリオと例」を参照してください。

目次

- セキュリティグループをターゲットネットワークに適用する
- ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除する
- ターゲットネットワークの表示

ターゲットネットワークをクライアント VPN エンドポイントに関連付ける

1 つ以上のターゲットネットワーク (サブネット) をクライアント VPN エンドポイントに関連付けることができます。

以下のルールが適用されます。

- サブネットには、少なくとも /27 ビットマスク (10.0.0.0/27 など) を持つ CIDR ブロックが必要です。サブネットには、常に最低 20 個の利用可能な IP アドレスも必要です。
- サブネットの CIDR ブロックは、クライアント VPN エンドポイントのクライアント CIDR 範囲と重複できません。
- 複数のサブネットをクライアント VPN エンドポイントに関連付ける場合、各サブネットは異なるアベイラビリティーゾーンに存在する必要があります。アベイラビリティーゾーンの冗長性を提供するために、少なくとも 2 つのサブネットを関連付けることをお勧めします。
- クライアント VPN エンドポイントの作成時に VPC を指定した場合、サブネットは同じ VPC 内にある必要があります。VPC をクライアント VPN エンドポイントにまだ関連付けていない場合、任意の VPC 内のサブネットを選択できます。

  それ以降のすべてのサブネットの関連付けは、同じ VPC から行う必要があります。別の VPC からのサブネットを関連付けるには、まずクライアント VPN エンドポイントを変更し、それに関連付けられている VPC を変更する必要があります。詳細については、「クライアント VPN エンドポイントを変更する」を参照してください。

サブネットをクライアント VPN エンドポイントに関連付けると、そのサブネットがプロビジョニングされたところの VPC のローカルルートが自動的にクライアント VPN エンドポイントのルートテーブルに追加されます。

> **Note**
>
> ターゲットネットワークが関連付けられた後に、アタッチされた VPC に CIDR をさらに追加したり、削除したりする場合は、次のいずれかの操作を実行して、クライアント VPN エンドポイントルートテーブルのローカルルートを更新する必要があります。

- クライアント VPN エンドポイントの関連付けをターゲットネットワークから解除してから、クライアント VPN エンドポイントをターゲットネットワークに関連付けます。
- クライアント VPN エンドポイントルートテーブルにルートを手動で追加するか、クライアント VPN エンドポイントルートテーブルからルートを削除します。

最初のサブネットをクライアント VPN エンドポイントに関連付けると、クライアント VPN エンドポイントのステータスが `pending-associate` から `available` に変わり、クライアントが VPN 接続を確立できるようになります。

ターゲットネットワークをクライアント VPN エンドポイントに関連付けるには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. ターゲットネットワークを関連付けるクライアント VPN エンドポイントを選択し、[Target network associations] (ターゲットネットワーク関連付け) を選択し、[Associate target network] (ターゲットネットワークを関連付ける) を選択します。
4. [VPC] で、サブネットがある VPC を選択します。クライアント VPN エンドポイントの作成時に VPC を指定した場合、または以前のサブネットの関連付けがある場合は、同じ VPC である必要があります。
5. [Choose a subnet to associate] (関連付けるサブネットを選択する) で、クライアント VPN エンドポイントに関連付けるサブネットを選択します。
6. [Associate target network] (ターゲットネットワークを関連付ける) を選択します。

ターゲットネットワークをクライアント VPN エンドポイントに関連付けるには (AWS CLI)

associate-client-vpn-target-network コマンドを使用します。

セキュリティグループをターゲットネットワークに適用する

クライアント VPN エンドポイントを作成するときに、ターゲットネットワークに適用するセキュリティグループを指定できます。1 つ目のターゲットネットワークをクライアント VPN エンドポイントに関連付けると、関連付けられたサブネットが位置している VPC のデフォルトのセキュリティグループが自動的に適用されます。詳細については、「セキュリティグループ」を参照してください。

クライアント VPN エンドポイントのセキュリティグループを変更できます。必要なセキュリティグループルールは、設定する VPN アクセスの種類によって異なります。詳細については、「AWS クライアント VPN のシナリオと例」を参照してください。

ターゲットネットワークにセキュリティグループを適用するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. セキュリティグループを適用するクライアント VPN エンドポイントを選択します。
4. [Security Groups] (セキュリティグループ) を選択して、[Apply Security Groups] (セキュリティグループの適用) を選択します。
5. [Security group IDs] (セキュリティグループ ID) から適切なセキュリティグループを選択します。
6. [Assign Security Groups] (セキュリティグループの適用) を選択します。

ターゲットネットワークにセキュリティグループを適用するには (AWS CLI)

apply-security-groups-to-client-vpn-target-network コマンドを使用します。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除する

ターゲットネットワークの関連付けを解除すると、クライアント VPN エンドポイントのルートテーブルに手動で追加されたすべてのルートと、ターゲットネットワークの関連付けが行われたときに自動的に作成されたルート (VPC のローカルルート) が削除されます。すべてのターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除すると、クライアントは VPN 接続を確立できなくなります。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. ターゲットネットワークが関連付けられているクライアント VPN エンドポイントを選択し、[Target network associations] (ターゲットネットワーク関連付け) を選択します。

4. 関連付けを解除するターゲットネットワークを選択し、[Disassociate] (関連付け解除)、[Disassociate target network] (ターゲットネットワークの関連付け解除) の順に選択します。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除するには (AWS CLI)

disassociate-client-vpn-target-network コマンドを使用します。

ターゲットネットワークの表示

クライアント VPN エンドポイントに関連付けられたターゲットを表示するには、コンソールまたは AWS CLI を使用します。

ターゲットネットワークを表示するには (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 適切なクライアント VPN エンドポイントを選択し、[Target network associations] (ターゲットネットワーク関連付け) を選択します。

AWS CLI を使用してターゲットネットワークを表示するには

describe-client-vpn-target-networks コマンドを使用します。

VPN セッションの最大継続時間

AWS Client VPN は、VPN セッションの最大継続時間に対して、いくつかのオプションを提供しています。セキュリティおよびコンプライアンス要件を満たすために、VPN セッションの最大継続時間を短く設定することができます。デフォルトでは、セッションの最大継続時間は 24 時間です。

> **Note**
>
> VPN セッションの最大継続時間値が減少すると、新しいタイムアウト値よりも古いアクティブな VPN セッションが切断されます。

クライアントデスクトップアプリケーションの詳細については、AWS Client VPN ユーザーガイドの「AWS が提供するクライアントのリリースノート」を参照してください。

目次

Client VPN エンドポイント作成時の最大 VPN セッションを設定する

Client VPN エンドポイントの作成時に最大 VPN セッションを設定するために詳細なステップについては、「クライアント VPN エンドポイントを作成する」を参照してください。

現在の VPN セッションの最大継続時間を表示

現在の VPN セッションの最大継続期間を表示するには、以下のステップを実行します。

Client VPN エンドポイントの現在の VPN セッション最大継続期間を表示する (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints] (クライアント VPN エンドポイント) を選択します。
3. 表示する Client VPN エンドポイントを選択します。
4. [Details] (詳細) タブが選択されていることを確認します。
5. [Session timeout hours] (セッションタイムアウト時間) の横にある、現在のVPNセッションの最大継続時間を表示します。

Client VPN エンドポイントの現在の VPN セッション最大継続時間を表示する (AWS CLI)

describe-client-vpn-endpoints コマンドを使用します。

VPN セッションの最大継続時間の変更

既存の VPN セッションの最大継続時間を変更するには、次のステップを実行します。

Client VPN エンドポイントの既存の VPN セッションの最大継続時間を変更する (コンソール)

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで、[Client VPN endpoints] (クライアント VPN エンドポイント) を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[Action] (アクション)、[Modify Client VPN Endpoint] (クライアント VPN エンドポイントの変更) の順に選択します。
4. [Session timeout hours] (セッションタイムアウト時間) を使用する場合、VPN セッションの最大継続時間を時間単位で選択します。
5. [Modify Client VPN endpoint] (クライアント VPN エンドポイントの変更) を選択します。

Client VPN エンドポイントの既存の VPN セッションの最大継続期間を変更する (AWS CLI)

modify-client-vpn-endpoint コマンドを使用します。

AWS Client VPN でのセキュリティ

AWS では、クラウドセキュリティを最優先事項としています。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは、AWS とユーザーの間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Client VPN に適用するコンプライアンスプログラムの詳細については、コンプライアンスプログラムによる対象範囲内の AWS のサービスをご参照ください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、ユーザーは、データの機密性、企業要件、および適用法令と規制などのその他要因に対する責任も担います。

AWS Client VPN は Amazon VPC サービスの一部です。Amazon VPC のセキュリティの詳細については、Amazon VPC ユーザーガイドの「セキュリティ」を参照してください。

このドキュメントは、クライアント VPN を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するようクライアント VPN を設定する方法を示します。また、クライアント VPN リソースのモニタリングや保護に役立つその他の AWS のサービスを利用する方法についても説明します。

目次

AWS Client VPN でのデータ保護

AWS 責任共有モデルは、AWS クライアント VPN におけるデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラストラクチャを保護する責任を負います。顧客は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。ご利用の AWS のサービス のセキュリティ設定と管理タスクについてもご自身の責任となります。データプライバシーの詳細については、データプライバシーのよくある質問を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、次の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 および TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS のサービス 内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや名前フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で Client VPN または他の AWS のサービス を使用する場合も同様です。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへ URL を供給する場合は、そのサーバーへのリクエストを検証するために、認証情報を URL に含めないことを強くお勧めします。

転送中の暗号化

AWS Client VPN では、Transport Layer Security (TLS) 1.2 以降を使用して任意の場所から安全な接続が提供されます。

インターネットトラフィックのプライバシー

ネットワーク間アクセスの有効化

クライアントが、クライアント VPN エンドポイントを介して VPC および他のネットワークに接続できるようにすることができます。詳細な説明と例については、「AWS クライアント VPN のシナリオと例」を参照してください。

ネットワークへのアクセスを制限する

クライアント VPN エンドポイントを設定して、VPC 内の特定のリソースへのアクセスを制限することができます。ユーザーベースの認証の場合、クライアント VPN エンドポイントにアクセスするユーザーグループに基づいて、ネットワークの一部へのアクセスを制限することもできます。詳細については、「AWS クライアント VPN を使用したネットワークへのアクセス制限」を参照してください。

クライアントの認証

認証は AWS クラウドへの最初のエントリポイントで実装されます。クライアントがクライアント VPN エンドポイントへの接続を許可されているかどうかを判断するために使用されます。認証が成功すると、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て VPN セッションを確立します。認証が失敗すると、接続は拒否され、クライアントは VPN セッションを確立できなくなります。

クライアント VPN では、次のタイプのクライアント承認を使用できます。

- Active Directory 認証 (ユーザーベース)
- 相互認証 (証明書ベース)
- シングルサインオン (SAML ベースのフェデレーション認証) (ユーザーベース)

AWS クライアント VPN の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰にクライア

ント VPN リソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、クライアント VPN で行う作業によって異なります。

サービスユーザー – ジョブを実行するために クライアント VPN サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。作業を実行するためにさらに多くのクライアント VPN の機能を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。クライアント VPN の特徴にアクセスできない場合は、「AWS クライアント VPN アイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内のクライアント VPN リソースを担当している場合は、通常、クライアント VPN へのフルアクセスがあります。サービスのユーザーがどのクライアント VPN 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社でクライアント VPN で IAM を利用する方法の詳細については、「AWS クライアント VPN と IAM の連携方法」をご参照ください。

IAM 管理者 - IAM 管理者は、クライアント VPN へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できるクライアント VPN アイデンティティベースのポリシーの例を表示するには、「AWS クライアント VPN のアイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center とは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイド の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリー

ムサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーで IAM の AWS マネージドポリシーを使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

AWS クライアント VPN と IAM の連携方法

IAM を使用してクライアント VPN へのアクセスを管理する前に、クライアント VPN で利用できる IAM の機能について学びます。

AWS クライアント VPN で使用できる IAM 機能

IAM 機能	Client VPN のサポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	No
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	Yes
プリンシパル権限	Yes
サービスロール	あり
サービスリンクロール	はい

クライアント VPN およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS と連携する のサービス」を参照してください。

クライアント VPN のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

クライアント VPN のアイデンティティベースのポリシーの例

クライアント VPN アイデンティティベースのポリシーの例を表示するには、「AWS クライアント VPN のアイデンティティベースのポリシーの例」を参照してください。

クライアント VPN 内のリソースベースのポリシー

リソースベースのポリシーのサポート	No

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーに

よって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

Client VPN のポリシーアクション

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

クライアント VPN アクションのリストを確認するには、「サービス認証リファレンス」のAWS「クライアント VPN で定義されるアクション」を参照してください。

クライアント VPN のポリシーアクションは、アクションの前に以下のプレフィックスを使用します。

```
ec2
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

クライアント VPN アイデンティティベースのポリシーの例を表示するには、「AWS クライアント VPN のアイデンティティベースのポリシーの例」を参照してください。

Client VPN のポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

クライアント VPN リソースタイプとその ARNs」のAWS 「クライアント VPN で定義されるリソース」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、AWS 「クライアント VPN で定義されるアクション」を参照してください。

クライアント VPN アイデンティティベースのポリシーの例を表示するには、「AWS クライアント VPN のアイデンティティベースのポリシーの例」を参照してください。

クライアント VPN 向けのポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

クライアント VPN 条件キーのリストを確認するには、「サービス認証リファレンス」の AWS 「クライアント VPN の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、AWS 「クライアント VPN で定義されるアクション」を参照してください。

クライアント VPN アイデンティティベースのポリシーの例を表示するには、「AWS クライアント VPN のアイデンティティベースのポリシーの例」を参照してください。

クライアント VPN での ACL

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ABAC とクライアント VPN

ABAC (ポリシー内のタグ) のサポート	いいえ

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイド の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

クライアント VPN での一時的な認証情報の使用

一時的な認証情報のサポート	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセ

スすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。この際、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

クライアント VPN のクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

クライアント VPN のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、クライアント VPN の機能が破損する可能性があります。クライアント VPN が指示する場合以外は、サービスロールを編集しないでください。

クライアント VPN のサービスにリンクされたロール

サービスリンクロールのサポート	はい

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、Service-linked role (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

AWS クライアント VPN のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、クライアント VPN リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARNs」のAWS 「クライアント VPN のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス

- ユーザーが自分の権限を表示できるようにする

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かがクライアント VPN リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素: 条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティベストプラクティス」を参照してください。

ユーザーが自分の権限を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS クライアント VPN アイデンティティとアクセスのトラブルシューティング

次の情報は、クライアント VPN と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

クライアント VPN でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なec2:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

この場合、ec2:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新してクライアント VPN にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用してクライアント VPN でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーにクライアント VPN リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- クライアント VPN でこれらの特徴がサポートされるかどうかを確認するには、「AWS クライアント VPN と IAM の連携方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

クライアント VPN のサービスにリンクされたロールの使用

AWS クライアント VPN は、AWS Identity and Access Management (IAM) のサービスにリンクされたロールを使用します。サービスにリンクされたロールは、クライアント VPN に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールはクライアント VPN によって事前に定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要な、すべてのアクセス許可が含まれています。

トピック

クライアント VPN のロールの使用

AWS クライアント VPN は、AWS Identity and Access Management (IAM) のサービスにリンクされたロールを使用します。サービスにリンクされたロールは、クライアント VPN に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールはクライアント VPN によって事前に定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要な、すべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用することで、必要な許可を手動で追加する必要がなくなるため、クライアント VPN の設定が簡単になります。クライアント VPN は、サービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、クライアント VPN のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティにアタッチすることはできません。

サービスにリンクされたロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへの意図しないアクセスによる許可の削除が防止され、クライアント VPN リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動する AWS のサービス」を参照し、[Service-linked roles] (サービスにリンクされたロール) の列内で [Yes] (はい) と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

クライアント VPN のサービスにリンクされたロールのアクセス許可

クライアント VPN は、AWSServiceRoleForClientVPN という名前のサービスにリンクされたロールを使用します。これにより、クライアント VPN は、ユーザーの VPN 接続に関連するリソースを作成および管理できます。

AWSServiceRoleForClientVPN のサービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `clientvpn.amazonaws.com`

ClientVPNServiceRolePolicy という名前のロール許可ポリシーは、クライアント VPN が次のアクションを指定されたリソースで完了することを許可します。

- アクション: `Resource: "*"` 上で `ec2:CreateNetworkInterface`
- アクション: `Resource: "*"` 上で `ec2:CreateNetworkInterfacePermission`
- アクション: `Resource: "*"` 上で `ec2:DescribeSecurityGroups`
- アクション: `Resource: "*"` 上で `ec2:DescribeVpcs`
- アクション: `Resource: "*"` 上で `ec2:DescribeSubnets`
- アクション: `Resource: "*"` 上で `ec2:DescribeInternetGateways`
- アクション: `Resource: "*"` 上で `ec2:ModifyNetworkInterfaceAttribute`
- アクション: `Resource: "*"` 上で `ec2:DeleteNetworkInterface`
- アクション: `Resource: "*"` 上で `ec2:DescribeAccountAttributes`
- アクション: `Resource: "*"` 上で `ds:AuthorizeApplication`
- アクション: `Resource: "*"` 上で `ds:DescribeDirectories`
- アクション: `Resource: "*"` 上で `ds:GetDirectoryLimits`
- アクション: `Resource: "*"` 上で `ds:UnauthorizeApplication`
- アクション: `Resource: "*"` 上で `logs:DescribeLogStreams`
- アクション: `Resource: "*"` 上で `logs:CreateLogStream`
- アクション: `Resource: "*"` 上で `logs:PutLogEvents`
- アクション: `Resource: "*"` 上で `logs:DescribeLogGroups`
- アクション: `Resource: "*"` 上で `acm:GetCertificate`

- アクション: `Resource: "*"` 上で `acm:DescribeCertificate`
- アクション: `Resource: "*"` 上で `iam:GetSAMLProvider`
- アクション: `lambda:GetFunctionConfiguration` 上で `Resource: "*"`

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

クライアント VPN のサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS Management Console、AWS CLI、または AWS API を使用してアカウントで最初のクライアント VPN を作成にリンクされたロールを作成すると、クライアント VPN によってサービスにリンクされたロールが作成されます。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。アカウントに最初のクライアント VPN エンドポイントを作成すると、クライアント VPN によってサービスにリンクされたロールが再度作成されます。

クライアント VPN のサービスにリンクされたロールの編集

クライアント VPN では、AWSServiceRoleForClientVPN のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

クライアント VPN のサービスにリンクされたロールの削除

クライアント VPN を使用する必要がなくなった場合は、AWSServiceRoleForClientVPN のサービスにリンクされたリンクロールを削除することをお勧めします。

まず、関連するクライアント VPN リソースを削除する必要があります。これにより、リソースに対するアクセス許可を誤って削除することがなくなります。

サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

クライアント VPN のサービスにリンクされたロールをサポートするリージョン

クライアント VPN では、このサービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、「AWS リージョンとエンドポイント」を参照してください。

接続認証へのロールの使用

AWS クライアント VPN は、AWS Identity and Access Management (IAM) のサービスにリンクされたロールを使用します。サービスにリンクされたロールは、クライアント VPN に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールはクライアント VPN によって事前に定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要な、すべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用することで、必要な許可を手動で追加する必要がなくなるため、クライアント VPN の設定が簡単になります。クライアント VPN は、サービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、クライアント VPN のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティにアタッチすることはできません。

サービスにリンクされたロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへの意図しないアクセスによる許可の削除が防止され、クライアント VPN リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動する AWS のサービス」を参照し、[Service-linked roles] (サービスにリンクされたロール) の列内で [Yes] (はい) と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

クライアント VPN のサービスにリンクされたロールのアクセス許可

クライアント VPN は、AWSServiceRoleForClientVPNConnections (クライアント VPN 接続用のサービスにリンクされたロール) という名前のサービスにリンクされたロールを使用します。

AWSServiceRoleForClientVPNConnections のサービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `clientvpn-connections.amazonaws.com`

ClientVPNServiceConnectionsRolePolicy という名前のロール許可ポリシーは、クライアント VPN が次のアクションを指定されたリソースで完了することを許可します。

- アクション: `arn:aws:lambda:*:*:function:AWSClientVPN-*` 上で `lambda:InvokeFunction`

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

クライアント VPN のサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS Management Console、AWS CLI、または AWS API を使用してアカウントで最初のクライアント VPN を作成にリンクされたロールを作成すると、クライアント VPN によってサービスにリンクされたロールが作成されます。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。アカウントに最初のクライアント VPN エンドポイントを作成すると、クライアント VPN によってサービスにリンクされたロールが再度作成されます。

クライアント VPN のサービスにリンクされたロールの編集

クライアント VPN では、AWSServiceRoleForClientVPNConnections のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

クライアント VPN のサービスにリンクされたロールの削除

クライアント VPN を使用する必要がなくなった場合は、AWSServiceRoleForClientVPNConnections のサービスにリンクされたリンクロールを削除することをお勧めします。

まず、関連するクライアント VPN リソースを削除する必要があります。これにより、リソースに対するアクセス許可を誤って削除することがなくなります。

サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

クライアント VPN のサービスにリンクされたロールをサポートするリージョン

クライアント VPN では、このサービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートしています。詳細については、「AWS リージョンとエンドポイント」を参照してください。

AWS Client VPN での耐障害性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心として構築されます。AWS リージョンには、低レイテンシー、高スループット、そして高冗長性のネットワークで接続されている複数の物理的に独立· 隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS Client VPN では、AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応するための機能を提供しています。

高可用性対応の複数のターゲットネットワーク

クライアントが VPN セッションを確立できるようにするには、ターゲットネットワークをクライアント VPN エンドポイントに関連付けます。ターゲットネットワークは、VPC のサブネットです。クライアント VPN エンドポイントに関連付ける各サブネットは、異なるアベイラビリティーゾーンに属している必要があります。高可用性を実現するために、複数のサブネットをクライアント VPN エンドポイントに関連付けることができます。

AWS Client VPN でのインフラストラクチャセキュリティ

マネージドサービスである AWS クライアント VPN は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWS クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 - AWS Well-Architected Framework」の「インフラストラクチャ保護」を参照してください。

AWS が公開した API 呼び出しを使用して、ネットワーク経由で Client VPN にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Client VPN のセキュリティのベストプラクティス

AWS Client VPN には、独自のセキュリティポリシーを開発および実装する際に考慮する必要のあるいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な検討事項とお考えください。

承認ルール

承認ルールを使用して、ネットワークにアクセスできるユーザーを制限します。詳細については、「承認ルール」を参照してください。

セキュリティグループ

セキュリティグループを使用して、VPC でユーザーがアクセスできるリソースを制御します。詳細については、「セキュリティグループ」を参照してください。

クライアント証明書失効リスト

クライアント証明書失効リストを使用して、特定のクライアント証明書のクライアント VPN エンドポイントへのアクセスを取り消すことができます。たとえば、ユーザーが組織を離れた場合です。詳細については、「クライアント証明書失効リスト」を参照してください。

モニタリングツール

モニタリングツールを使用して、クライアント VPN エンドポイントの可用性とパフォーマンスを追跡します。詳細については、「AWS クライアント VPN のモニタリング」を参照してください。

Identity and Access Management

IAM ユーザーおよび IAM ロールの IAM ポリシーを使用して、クライアント VPN リソースと API へのアクセスを管理します。詳細については、「AWS クライアント VPN の Identity and Access Management」を参照してください。

AWS クライアント VPN の IPv6 に関する考慮事項

現在、クライアント VPN サービスは、VPN トンネルを経由する IPv6 トラフィックのルーティングをサポートしていません。ただし、IPv6 のリークを防ぐために、IPv6 トラフィックを VPN トンネルにルーティングする必要がある場合があります。IPv6 リークは、IPv4 と IPv6 の両方が有効で VPN に接続されているが、VPN が IPv6 トラフィックをトンネルにルーティングしない場合に発生する可能性があります。この場合、IPv6 が有効な送信先に接続したときに、ISP から提供された IPv6 アドレスを使用して接続していることになります。これにより、実際の IPv6 アドレスがリークします。次の手順では、IPv6 トラフィックを VPN トンネルにルーティングする方法について説明します。

IPv6 リークを防ぐために、次の IPv6 関連のディレクティブをクライアント VPN 設定ファイルに追加する必要があります。

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

次の例のようになります。

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

この例では、`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` によって、ローカルトンネルデバイスの IPv6 アドレスが `fd15:53b6:dead::2` に設定され、リモート VPN エンドポイント IPv6 アドレスが `fd15:53b6:dead::1` に設定されます。

次のコマンド `route-ipv6 2000::/4` は、`2000:0000:0000:0000:0000:0000:0000:0000` から `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` の IPv6 アドレスを VPN 接続にルーティングします。

> **Note**
>
> 例えば、Windows の「TAP」デバイスルーティングの場合、`ifconfig-ipv6` の 2 つ目のパラメータが `--route-ipv6` のルートターゲットとして使用されます。

Organizations では、`ifconfig-ipv6` の 2 つのパラメータを自身で設定する必要があり、`100::/64` (`0100:0000:0000:0000:0000:0000:0000:0000` から `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) または `fc00::/7` (`fc00:0000:0000:0000:0000:0000:0000:0000` から `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`) のアドレスを使用できます。`100::/64` は破棄専用アドレスブロックであり、`fc00::/7` は一意ローカルです。

別の例を紹介します。

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

この例では、設定により、現在割り当てられているすべての IPv6 トラフィックが VPN 接続にルーティングされます。

検証

ご自身の組織で独自のテストを実施することになるでしょう。基本的な検証は、フルトンネル VPN 接続を設定してから、IPv6 アドレスを使用して IPv6 サーバーに対して ping6 を実行することです。サーバーの IPv6 アドレスは、`route-ipv6` コマンドによって指定された範囲内にある必要があります。この ping テストは失敗します。ただし、将来的に IPv6 サポートがクライアント VPN サービスに追加された場合は変わる可能性があります。ping が成功し、フルトンネルモードで接続しているときにパブリックサイトにアクセスできる場合は、さらにトラブルシューティングを行う必要があります。また、ipleak.org などの公開されているツールを使ってテストすることもできます。

AWS クライアント VPN のモニタリング

モニタリングは、AWS クライアント VPN および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。クライアント VPN エンドポイントをモニタリングするには、次の機能を使用して、トラフィックパターンの分析やクライアント VPN エンドポイントのトラブルシューティングを行います。

Amazon CloudWatch

AWS リソースと AWS でリアルタイムに実行されるアプリケーションをモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

AWS CloudTrail

AWS アカウントにより、またはそのアカウントに代わって、行われた API コールや関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrailユーザーガイドを参照してください。

Amazon CloudWatch Logs

AWS Client VPN エンドポイントへの接続の試行をモニタリングできます。接続の試行とクライアント VPN 接続のリセットを表示できます。接続試行では、成功した接続試行と失敗した接続試行の両方を確認できます。接続の詳細をログに記録する CloudWatch Logs ログストリームを指定できます。詳細については、接続ログ および Amazon CloudWatch Logs ユーザーガイドを参照してください。

AWS Client VPN の CloudWatch メトリクス

AWS クライアント VPN は、クライアント VPN エンドポイントについて、以下のメトリクスを Amazon CloudWatch に発行します。メトリクスは、5 分ごとに Amazon CloudWatch に公開されます。

メトリクス	説明
ActiveConnectionsCount	クライアント VPN エンドポイントへのアクティブな接続の数。 単位はカウント
AuthenticationFailures	クライアント VPN エンドポイントの認証失敗の数。 単位はカウント
CrlDaysToExpiry	クライアント VPN エンドポイントで設定されている証明書失効リスト (CRL) の有効期限が切れるまでの日数。 単位: 日数
EgressBytes	クライアント VPN エンドポイントから送信されたバイト数。 単位: バイト
EgressPackets	クライアント VPN エンドポイントから送信されたパケットの数。 単位はカウント
IngressBytes	クライアント VPN エンドポイントが受信したバイト数。 単位: バイト
IngressPackets	クライアント VPN エンドポイントが受信したパケット数。 単位はカウント
SelfServicePortalClientConfigurationDownloads	セルフサービスポータルからの Client VPN エンドポイント設定ファイルのダウンロード数。

メトリクス	説明
	単位: 個

AWS クライアント VPN は、クライアント VPN エンドポイントについて、以下の体制評価メトリクスを公開します。

メトリクス	説明
ClientConnectHandlerTimeouts	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーを呼び出す際のタイムアウトの数。 単位はカウント
ClientConnectHandlerInvalidResponses	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーが返す無効なレスポンスの数。 単位はカウント
ClientConnectHandlerOtherExecutionErrors	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーを実行中の予期しないエラーの数。 単位はカウント
ClientConnectHandlerThrottlingErrors	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーを呼び出す際のスロットリングエラーの数。 単位はカウント
ClientConnectHandlerDeniedConnections	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーによって拒否された接続の数。 単位はカウント

メトリクス	説明
ClientConnectHandlerFailedServiceErrors	クライアント VPN エンドポイントへの接続のクライアント接続ハンドラーを実行中のサービス側エラーの数。 単位はカウント

エンドポイントごとにクライアント VPN エンドポイントのメトリクスをフィルタリングできます。

CloudWatch では、それらのデータポイントについての統計を、順序付けられた時系列データのセット (メトリクスと呼ばれる) として取得できます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。たとえば、メトリクスが許容範囲外になる場合、CloudWatch アラームを作成して、指定されたメトリクスを監視し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

CloudWatch メトリクスの表示

次のようにして、クライアント VPN エンドポイントのメトリクスを表示できます。

CloudWatch コンソールを使用してメトリクスを表示するには

メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. [All metrics] で、[ClientVPN] メトリクス名前空間を選択します。
4. メトリクスを表示するには、エンドポイントごとにメトリクスディメンションを選択します。

AWS CLI を使ってメトリクスを表示するには

コマンドプロンプトで次のコマンドを使用して、クライアント VPN で利用可能なメトリクスを一覧表示します。

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

AWS クライアント VPN の CloudTrail ログ

AWS クライアント VPN は、AWS CloudTrail と統合されます。クライアント VPN のユーザー、ロール、または AWS サービスで実行されたアクションのレコードを提供するサービスです。CloudTrail は、クライアント VPN のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされたコールには、クライアント VPN コンソールからの呼び出しと、クライアント VPN API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、クライアント VPN のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、クライアント VPN に対して行われたリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエストの実行日時、その他の詳細を判別します。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail でのクライアント VPN 情報

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。クライアント VPN でアクティビティが発生すると、そのアクティビティは [Event history (イベント履歴)] の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「Viewing Events with CloudTrail Event History」(CloudTrail イベント履歴でのイベントの表示) を参照してください。

クライアント VPN のイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 追跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail 通知の設定

- CloudTrail ログファイルを複数のリージョンから受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべてのクライアント VPN アクションは CloudTrail が記録します。これらのアクションは Amazon EC2 API リファレンスで説明されています。例えば、CreateClientVpnEndpoint、AssociateClientVpnTargetNetwork、AuthorizeClientVpnIr の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーティッドユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

クライアント VPN ログファイルエントリの概要

[トレイル] は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように構成できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

詳細については、Amazon EC2 API リファレンスのAWS CloudTrail を使用した Amazon EC2、Amazon EBS、および Amazon VPC API 呼び出しのログ記録を参照してください。

AWS クライアント VPN クォータ

AWS アカウントには、クライアント VPN エンドポイントに関連する、以前は制限と呼ばれていた以下のクォータがあります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。

調整可能なクォータについて、クォータの引き上げをリクエストするには、[Adjustable] (調整可能) 列で [Yes] (はい) を選択します。詳細については、「Service Quotas ユーザーガイド」の「クォータの引き上げのリクエスト」を参照してください。

クライアント VPN クォータ

名前	デフォルト	引き上げ可能
クライアント VPN エンドポイントあたりの承認ルール	50	はい
リージョンあたりのクライアント VPN エンドポイント	5	はい
クライアント VPN エンドポイントあたりの同時実行クライアント接続	この値は、エンドポイントごとのサブネット関連付けの数によって異なります。 • 1 ~ 20,000 • 2 ~ 36,500 • 3 ~ 66,500 • 4 ~ 96,500 • 5 ~ 126,000	はい
クライアント VPN エンドポイントあたりの同時実行オペレーション †	10	いいえ
クライアント VPN エンドポイントのクライアント証明書の失効リストのエントリ	20,000	いいえ

名前	デフォルト	引き上げ可能
クライアント VPN エンドポイントあたりのルート	10	はい

† オペレーションは次のとおりです。

- サブネットの関連付けまたは関連付けの解除
- ルートの作成または削除
- インバウンドおよびアウトバウンドルールの作成または削除
- セキュリティグループの作成または削除

ユーザーとグループのクォータ

Active Directory または SAML ベースの IdP のユーザーおよびグループを設定する場合、次のクォータが適用されます。

- ユーザーは最大 200 個のグループに属することができます。200 番目を超えたグループは無視されます。
- グループ ID の最大長は 255 文字です。
- 名前 ID の最大長は 255 文字です。255 番目を超えた文字は切り捨てられます。

一般的な考慮事項

クライアント VPN エンドポイントを使用する場合は、次の点に注意してください。

- Active Directory を使用してユーザーを認証する場合、クライアント VPN エンドポイントは Active Directory 認証に使用される AWS Directory Service リソースと同じアカウントに属している必要があります。
- SAML ベースのフェデレーション認証を使用してユーザーを認証する場合、クライアント VPN エンドポイントは、IdP とAWS 信頼の関係を定義するために作成する IAM SAML ID プロバイダーと同じアカウントに属している必要があります。IAM SAML ID プロバイダーは、同じ AWS アカウントの複数のクライアント VPN エンドポイント間で共有できます。

AWS クライアント VPN のトラブルシューティング

以下のトピックは、クライアント VPN エンドポイントに関する問題のトラブルシューティングに役立ちます。

クライアントがクライアント VPN への接続に使用する OpenVPN ベースのソフトウェアのトラブルシューティングに関する詳細は、AWS Client VPN ユーザーガイドの「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。

よくある問題

クライアント VPN エンドポイント DNS 名を解決できない

問題

クライアント VPN エンドポイントの DNS 名を解決できません。

原因

クライアント VPN エンドポイント設定ファイルには、remote-random-hostname というパラメータが含まれています。このパラメータは、DNS キャッシュを防止するために、クライアントが DNS 名の前にランダム文字列を追加するよう強制します。一部のクライアントではこのパラメータを認識しないため、必要なランダム文字列を DNS 名の前に追加しません。

ソリューション

任意のテキストエディタを使用して、クライアント VPN エンドポイント設定ファイルを開きます。クライアント VPN エンドポイントの DNS 名を指定する行を見つけ、その前にランダム文字列を追加して、*random_string.displayed_DNS_name* という形式にします。次に例を示します。

- 元の DNS 名: cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com
- 変更された DNS 名: asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com

トラフィックがサブネット間で分割されていない

問題

2 つのサブネット間でネットワークトラフィックを分割しようとしています。プライベートトラフィックはプライベートサブネット経由でルーティングし、インターネットトラフィックはパブリックサブネット経由でルーティングする必要があります。ただし、両方のルートをクライアント VPN エンドポイントルートテーブルに追加しても、1 つのルートしか使用されていません。

原因

クライアント VPN エンドポイントに複数のサブネットを関連付けることができますが、アベイラビリティーゾーンごとにサブネットを 1 つのみ関連付けることができます。複数サブネットの関連付けの目的は、クライアントに高可用性とアベイラビリティーゾーンの冗長性を提供することです。ただし、クライアント VPN では、クライアント VPN エンドポイントに関連付けられたサブネット間でトラフィックを選択的に分割することはできません。

クライアントは、DNS ラウンドロビンアルゴリズムに基づいてクライアント VPN エンドポイントに接続します。つまり、接続を確立するときに、関連付けられたサブネットのいずれかを経由してトラフィックがルーティングされます。したがって、必要なルートエントリを持たない関連付けられたサブネットを確定すると、接続の問題が発生する可能性があります。

たとえば、次のサブネットの関連付けとルートを設定するとします。

- サブネットの関連付け
  - 関連付け 1：サブネット A (us-east-1a)
  - 関連付け 2：サブネット B (us-east-1b)
- ルート
  - ルート 1: サブネット A にルーティングされる 10.0.0.0/16
  - ルート 2: サブネット B にルーティングされる 172.31.0.0/16

この例では、接続時にサブネット A を確定するクライアントはルート 2 にアクセスできず、接続時にサブネット B を確定するクライアントはルート 1 にアクセスできません。

ソリューション

クライアント VPN エンドポイントに、関連付けられた各ネットワークのターゲットを持つ同じルートエントリがあることを確認します。これにより、トラフィックがルーティングされるサブネットに関係なく、クライアントはすべてのルートにアクセスできます。

Active Directory グループの承認ルールが想定どおりに機能しない

問題

Active Directory グループの承認ルールを設定しましたが、想定どおりに機能していません。すべてのネットワークのトラフィックを承認するため `0.0.0.0/0` の承認ルールを追加しましたが、特定の送信先 CIDR のトラフィックはいまだに失敗します。

原因

承認ルールは、ネットワーク CIDR にインデックス化されます。承認ルールでは、特定のネットワーク CIDR へのアクセスを Active Directory グループに許可する必要があります。`0.0.0.0/0` の承認ルールは特殊なケースとして扱われるため、承認ルールの作成順序に関係なく、最後に評価されます。

例えば、次の順序で 5 つの承認ルールを作成するとします。

- ルール 1: グループ 1 は `10.1.0.0/16` にアクセスする
- ルール 2: グループ 1 は `0.0.0.0/0` にアクセスする

- ルール 3: グループ 2 は 0.0.0.0/0 にアクセスする
- ルール 4: グループ 3 は 0.0.0.0/0 にアクセスする
- ルール 5: グループ 2 は 172.131.0.0/16 にアクセスする

この例では、ルール 2、ルール 3、およびルール 4 が最後に評価されます。グループ 1 は 10.1.0.0/16 にのみアクセスでき、グループ 2 は 172.131.0.0/16 にのみアクセスできます。グループ 3 は 10.1.0.0/16 または 172.131.0.0/16 にアクセスできませんが、他のすべてのネットワークにアクセスできます。ルール 1 と 5 を削除すると、3 つのグループすべてがすべてのネットワークにアクセスできます。

クライアント VPN は、承認ルールを評価するときに、最長プレフィックスマッチングを使用します。詳細については、Amazon VPC ユーザーガイドの「ルーティングの優先度」を参照してください。

ソリューション

Active Directory グループに特定のネットワーク CIDR へのアクセスを明示的に許可する承認ルールを作成することを確認します。0.0.0.0/0 の承認ルールを追加する場合、そのルールは最後に評価され、以前の承認ルールによってアクセスを許可するネットワークが制限される可能性があることに注意してください。

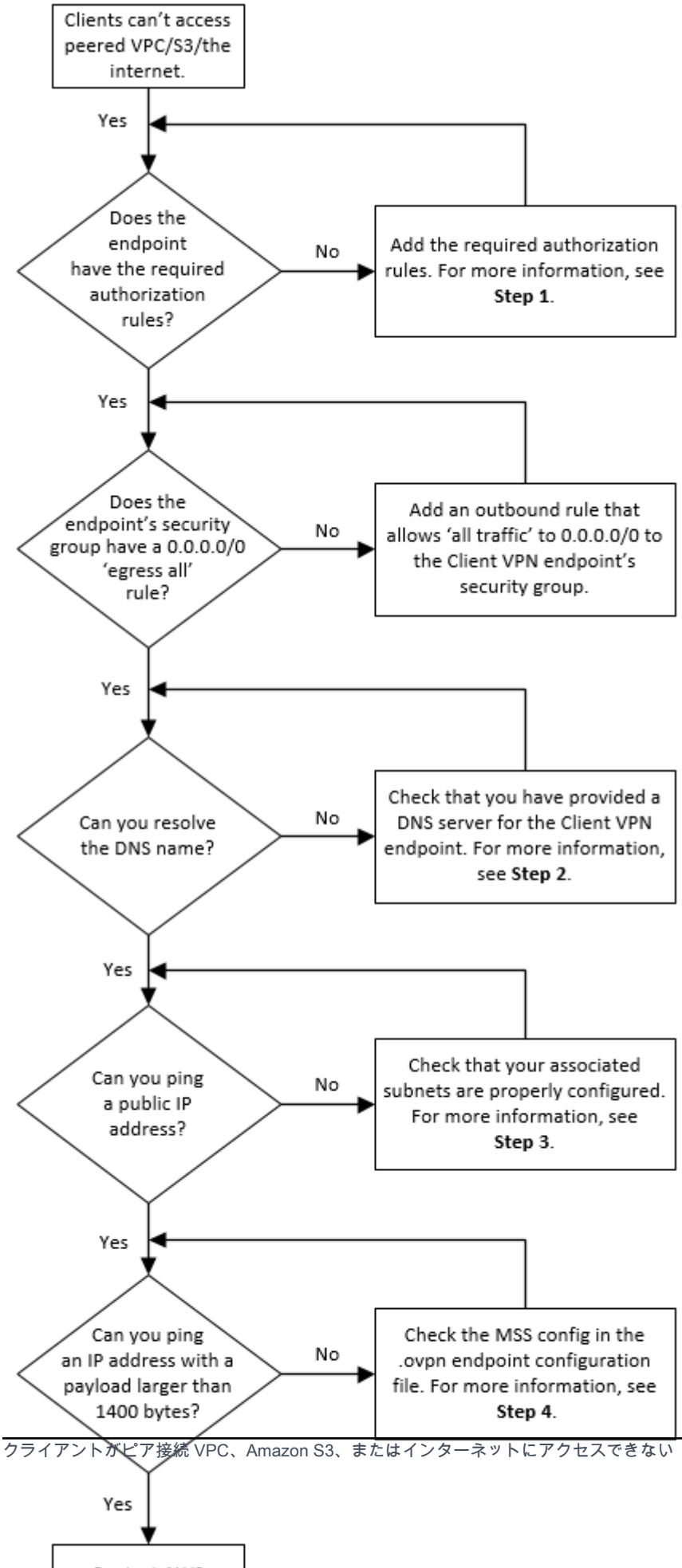
クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできない

問題

クライアント VPN エンドポイントルートを適切に設定しましたが、クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできません。

ソリューション

次のフローチャートには、インターネット、ピア接続 VPC、および Amazon S3 接続の問題を診断するステップが含まれています。


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. インターネットにアクセスする場合は、`0.0.0.0/0` の承認ルールを追加します。

   ピア接続 VPC にアクセスする場合は、VPC の IPv4 CIDR 範囲の承認ルールを追加します。

   S3 にアクセスする場合は、Amazon S3 エンドポイントの IP アドレスを指定します。

2. DNS 名を解決できるかどうかを確認します。

   DNS 名を解決できない場合は、クライアント VPN エンドポイントの DNS サーバーが指定されていることを確認します。独自の DNS サーバーを管理する場合は、その IP アドレスを指定します。DNS サーバーが VPC からアクセスできることを確認します。

   DNS サーバーに指定する IP アドレスが不明な場合は、VPC の .2 IP アドレスに VPC DNS リゾルバーを指定します。

3. インターネットアクセスの場合は、パブリック IP アドレスまたはパブリックウェブサイト (`amazon.com` など) に ping できるかどうかを確認します。応答が得られない場合は、関連付けられたサブネットのルートテーブルに、インターネットゲートウェイまたは NAT ゲートウェイのいずれかをターゲットとするデフォルトルートがあることを確認します。ルートが設定されている場合は、関連付けられたサブネットに、インバウンドおよびアウトバウンドのトラフィックをブロックするネットワークアクセスコントロールリストのルールがないことを確認します。

   ピア接続 VPC に到達できない場合は、関連付けられたサブネットのルートテーブルにピア接続 VPC のルートエントリがあることを確認します。

   Amazon S3 に到達できない場合は、関連付けられたサブネットのルートテーブルにゲートウェイ VPC エンドポイントのルートエントリがあることを確認します。

4. 1400 バイトを超えるペイロードを持つパブリック IP アドレスに ping を実行できるかどうかを確認します。以下のいずれかのコマンドを使用します。

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

1400 バイトを超えるペイロードを持つ IP アドレスに ping を実行できない場合は、任意のテキストエディタを使用してクライアント VPN エンドポイント .ovpn 設定ファイルを開き、以下を追加します。

```
mssfix 1328
```

ピア接続 VPC、Amazon S3、またはインターネットへのアクセスが断続的である

問題

ピア接続 VPC、Amazon S3、またはインターネットへの接続時に断続的な接続の問題がありますが、関連付けられたサブネットへのアクセスには影響しません。接続の問題を解決するには、切断して再接続する必要があります。

原因

クライアントは、DNS ラウンドロビンアルゴリズムに基づいてクライアント VPN エンドポイントに接続します。つまり、接続を確立するときに、関連付けられたサブネットのいずれかを経由してトラフィックがルーティングされます。したがって、必要なルートエントリを持たない関連付けられたサブネットを確定すると、接続の問題が発生する可能性があります。

ソリューション

クライアント VPN エンドポイントに、関連付けられた各ネットワークのターゲットを持つ同じルートエントリがあることを確認します。これにより、トラフィックがルーティングされる関連付けられたサブネットに関係なく、クライアントはすべてのルートにアクセスできます。

たとえば、クライアント VPN エンドポイントに 3 つの関連付けられたサブネット (サブネット A、B、および C) があり、クライアントのインターネットアクセスを有効にするとします。これを行うには、関連付けられた各サブネットをターゲットとする `0.0.0.0/0` ルートを 3 つ追加する必要があります。

- ルート 1: サブネット A に `0.0.0.0/0`
- ルート 2: サブネット B に `0.0.0.0/0`
- ルート 3: サブネット C に `0.0.0.0/0`

クライアントソフトウェアが TLS エラーを返す

問題

以前はクライアントをクライアント VPN に正常に接続することができましたが、OpenVPN ベースのクライアントは、接続しようとするといずれかの次のエラーを返します。

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

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

考えられる原因 1

相互認証を使用し、クライアント証明書失効リストをインポートした場合、クライアント証明書失効リストの有効期限が切れていた可能性があります。認証フェーズでは、クライアント VPN エンドポイントは、インポートしたクライアント証明書失効リストと照合してクライアント証明書をチェックします。クライアント証明書失効リストの有効期限が切れている場合は、クライアント VPN エンドポイントに接続できません。

解決策 1

OpenSSL ツールを使用して、クライアント証明書失効リストの有効期限を確認します。

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

出力には、有効期限の日時が表示されます。クライアント証明書失効リストの有効期限が切れている場合は、新しい証明書失効リストを作成してクライアント VPN エンドポイントにインポートする必要があります。詳細については、「クライアント証明書失効リスト」を参照してください。

考えられる原因 2

クライアント VPN エンドポイントに使用されているサーバー証明書の有効期限が切れています。

解決策 2

AWS Certificate Manager コンソールまたは AWS CLI を使用して、サーバー証明書のステータスを確認します。サーバー証明書の有効期限が切れている場合は、新しい証明書を作成して ACM にアップロードします。OpenVPN easy-RSA ユーティリティを使用してサーバーおよびクライアント証明

書とキーを生成し、ACM にインポートするステップの詳細については、「相互認証」を参照してください。

または、クライアントがクライアント VPN への接続に使用している OpenVPN ベースのソフトウェアに問題がある可能性があります。OpenVPN ベースのソフトウェアのトラブルシューティングに関する詳細は、AWS Client VPN ユーザーガイドの「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。

クライアントソフトウェアがユーザー名とパスワードのエラーを返す (Active Directory 認証)

問題

クライアント VPN エンドポイントに Active Directory 認証を使用しています。以前はクライアントをクライアント VPN に正常に接続することができました。しかし、現在、クライアントは無効なユーザー名とパスワードのエラーを受け取っています。

考えられる原因

Active Directory 認証を使用し、クライアント設定ファイルを配布した後に Multi-Factor Authentication (MFA) を有効にした場合、ファイルにはユーザーに MFA コードの入力を求めるために必要な情報が含まれていません。ユーザー名とパスワードのみを入力するよう求められ、認証は失敗します。

ソリューション

新しいクライアント設定ファイルをダウンロードし、クライアントに配布します。新しいファイルに次の行が含まれていることを確認します。

```
static-challenge "Enter MFA code " 1
```

詳細については、「クライアント設定ファイルをエクスポートして設定する」を参照してください。クライアント VPN エンドポイントを使用せずに Active Directory の MFA 設定をテストし、MFA が想定どおりに機能していることを確認します。

クライアントソフトウェアがユーザー名とパスワードのエラーを返す (フェデレーティッド認証)

問題

フェデレーティッド認証でユーザー名とパスワードを使用してログインしようとして、「受信した認証情報が正しくありませんでした。IT 管理者に連絡してください。」

原因

このエラーは、IdP からの SAML レスポンスに少なくとも 1 つの属性が含まれていないことが原因である可能性があります。

ソリューション

IdP からの SAML レスポンスに少なくとも 1 つの属性が含まれていることを確認します。詳細については、「SAML ベースの IdP 設定リソース」を参照してください。

クライアントが接続できない (相互認証)

問題

クライアント VPN エンドポイントに相互認証を使用しています。クライアントが TLS キーネゴシエーション失敗のエラーとタイムアウトエラーを受け取っています。

考えられる原因

クライアントに提供された設定ファイルにクライアント証明書とクライアントのプライベートキーが含まれていないか、証明書とキーが正しくありません。

ソリューション

設定ファイルに正しいクライアント証明書とキーが含まれていることを確認します。必要に応じて、設定ファイルを修正し、クライアントに再配布します。詳細については、「クライアント設定ファイルをエクスポートして設定する」を参照してください。

クライアントから、認証情報が最大サイズを超えるというエラーが返される (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントが SAML ベースの ID プロバイダーの (IdP) ブラウザウィンドウにユーザー名とパスワードを入力したときに、認証情報について、サポートされている最大サイズを超えているというエラーが表示されます。

原因

IdP によって返される SAML 応答が、サポートされている最大サイズを超えています。詳細については、「SAML ベースのフェデレーション認証の要件と考慮事項」を参照してください。

ソリューション

IdP でユーザーが属するグループの数を減らし、接続を再試行してください。

クライアントでブラウザが開かない (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントがエンドポイントに接続しようとすると、クライアントソフトウェアによってブラウザウィンドウが開かれず、代わりにユーザー名とパスワードがポップアップウィンドウに表示されます。

原因

クライアントに提供された設定ファイルに、`auth-federate` フラグが含まれていません。

ソリューション

最新の設定ファイルをエクスポートし、 AWS が提供するクライアントにインポートして、接続を再試行してください。

クライアントから、使用可能なポートがないというエラーが返される (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントがエンドポイントに接続しようとすると、クライアントソフトウェアが次のエラーを返します:

```
The authentication flow could not be initiated. There are no available ports.
```

原因

AWS が提供するクライアントでは、認証を完了するために TCP ポート 35001 を使用する必要があります。詳細については、「SAML ベースのフェデレーション認証の要件と考慮事項」を参照してください。

ソリューション

クライアントのデバイスが TCP ポート 35001 をブロックしていないこと、または別のプロセスで使用していることを確認します。

IP の不一致により VPN 接続が終了しました

問題

VPN 接続が終了し、クライアントソフトウェアは次のエラーを返します。 "The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."

原因

AWS が提供するクライアントでは、接続先の IP アドレスが、クライアント VPN エンドポイントをバックアップする VPN サーバーの IP と一致する必要があります。詳細については、「のルールとベストプラクティス AWS Client VPN」を参照してください。

ソリューション

AWS が提供するクライアントとクライアント VPN エンドポイントの間に DNS プロキシがないことを確認します。

LAN へのトラフィックのルーティングが想定どおりに機能しない

問題

LAN IP アドレス範囲が 、10.0.0.0/8、、または の標準プライベート IP アドレス範囲にない場合192.168.0.0/16、トラフィックをローカルエリアネットワーク (LAN) 172.16.0.0/12にルーティングしようとしたときに期待どおりに動作しない169.254.0.0/16。

原因

クライアント LAN アドレス範囲が上記の標準範囲外であることが検出された場合、クライアント VPN エンドポイントは OpenVPN ディレクティブ「リダイレクトゲートウェイブロックローカル」をクライアントに自動的にプッシュし、すべての LAN トラフィックを VPN に強制します。詳細については、「のルールとベストプラクティス AWS Client VPN」を参照してください。

ソリューション

VPN 接続中に LAN アクセスが必要な場合は、LAN に上記の従来のアドレス範囲を使用することをお勧めします。

クライアント VPN エンドポイントの帯域幅制限を確認する

問題

クライアント VPN エンドポイントの帯域幅制限を確認する必要があります。

原因

スループットは、現在地からの接続の容量や、コンピュータ上のクライアント VPN デスクトップアプリケーションと VPC エンドポイント間のネットワークレイテンシーなど、複数の要因によって異なります。また、ユーザー接続ごとに 10 Mbps の帯域幅制限があります。

ソリューション

以下のコマンドを実行して、帯域幅を確認します。

```
sudo iperf3 -s -V
```

クライアント側:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

クライアント VPN ユーザーガイドのドキュメント履歴

次の表では、AWS Client VPN 管理者ガイドの更新について説明します。

変更	説明	日付
承認ルールの例	承認ルールのシナリオ例を追加。	2022 年 9 月 15 日
VPN セッションの最大継続時間	セキュリティおよびコンプライアンス要件を満たすために、VPN セッションの最大継続時間を短く設定することができます。	2022 年 1 月 20 日
クライアントログインバナー	規制やコンプライアンスのニーズに対応した VPN セッションを確立した場合、AWS が提供する Client VPN デスクトップアプリケーションでテキストバナーを有効にできます。	2022 年 1 月 20 日
クライアント接続ハンドラー	クライアント VPN エンドポイントのクライアント接続ハンドラーを有効にして、新しい接続を許可するカスタムロジックを実行できます。	2020 年 11 月 4 日
セルフサービスポータル	クライアントの クライアント VPN エンドポイントでセルフサービスポータルを有効にできます。	2020 年 10 月 29 日
クライアント間のアクセス	クライアント VPN エンドポイントに接続するクライアント	2020 年 9 月 29 日

	が相互に接続できるようにすることができます。	
SAML 2.0 ベースのフェデレーション認証	SAML 2.0 ベースのフェデレーション認証を使用して、クライアント VPN ユーザーを認証できます。	2020 年 5 月 19 日
作成中にセキュリティグループを指定する	AWS Client VPN エンドポイントの作成時に VPC とセキュリティグループを指定できます。	2020 年 3 月 5 日
設定可能な VPN ポート	AWS Client VPN エンドポイントでサポートされる VPN ポート番号を指定できます。	2020 年 1 月 16 日
多要素認証 (MFA) のサポート	AWS Client VPN エンドポイントがアクティブディレクトリで有効になっている場合、MFA をサポートします。	2019 年 9 月 30 日
分割トンネルのサポート	AWS Client VPN エンドポイントでスプリットトンネルを有効にできます。	2019 年 7 月 24 日
初回リリース	このリリースでは、AWS クライアント VPN が導入されています。	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。