aws

管理者ガイド

AWS Client VPN

AWS Client VPN: 管理者ガイド

Table of Contents

とは AWS Client VPN

AWS Client VPN は、オンプレミスネットワーク内の AWS 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 ではVPN、オープンVPNベースのVPNクライアントを使用して、任意の場所から リソースにアクセスできます。

トピック

クライアントの機能 VPN

クライアントVPNには、次の機能があります。

- 安全な接続 — OpenVPN クライアントを使用して、任意の場所から安全なTLS接続を提供します。
- マネージドサービス — これは 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なくなります。
- 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ルされます。
- 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 — AWS Directory Service や Amazon などの既存の AWS サービスと統合されますVPC。

クライアントのコンポーネント VPN

クライアント の主な概念は次のとおりですVPN。

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セッションを有効化および管理するために作成および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。のサブネットVPC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じ のものである必要がありますVPC。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、使用可能な送信先ネットワークルートを記述する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 Open VPNクライアントをダウンロードし、作成したクライアント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範囲から一意の 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。たとえば、 です`10.2.0.0/16`。

クライアントVPNポート

AWS Client VPN は、 と の両方でポート 443 TCPと 1194 をサポートしていますUDP。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VPCから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。その後、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、フォレンジックの実行、クライアントVPNエンドポイントの使用方法の分析、接続問題のデバッグを行うことができます。

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AWSVPNデスクトップ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をダウンロードするためのウェブページとしてセルフサービスポータルを提供します。これには、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サポートされるグローバルサービスです。

クライアントの使用 VPN

クライアントは、次のいずれかVPNの方法で操作できます。

AWS Management Console

コンソールには、クライアント 用のウェブベースのユーザーインターフェイスが用意されていますVPN。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VPNでクライアントを選択できます。

AWS Command Line Interface (AWS CLI)

AWS CLI は、クライアントVPNパブリック への直接アクセスを提供します 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 のコマンドの詳細についてはVPN、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 サービス用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。クライアントのコマンドレットの詳細についてはVPN、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VPNHTTPS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、サービスに直接HTTPSリクエストを発行できます。を使用する場合はHTTPSAPI、認証情報を使用してリクエストにデジタル署名するための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。

クライアントの料金 VPN

各エンドポイントの関連付けと各VPN接続に対して時間単位で課金されます。詳細については、AWS Client VPN の料金を参照してください。

Amazon からインターネットEC2へのデータ転送には料金が発生します。詳細については、「Amazon EC2 オンデマンド料金設定期間のデータ転送」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 Logs 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」を参照してください (有料利用枠でログを選択します)。

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 の料金を参照してください。

クライアントVPNエンドポイントは、 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VPC。インターネットゲートウェイVPCがある場合は、Elastic IP アドレスをクライアントの VPN Elastic Network Interface () に関連付けます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。

AWS Client VPNを使用するためのルールとベストプラクティス

以下は、 を使用するためのルールとベストプラクティスです。 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VPCが配置されている CIDRのローカル、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範囲のブロックサイズは /22 以上、/12 以下である必要があります。
- クライアントCIDR範囲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 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たサブネットは、同じ にある必要がありますVPC。
- 同じ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、専用テナンシー のサブネット関連付けをサポートしていませんVPC。
- クライアントはIPv4トラフィックのみVPNをサポートします。の詳細については、IPv6 に関する考慮事項 AWS Client VPN「」を参照してくださいIPv6。
- クライアントVPNは連邦情報処理標準 (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名前が解決される IP アドレスの変更が表示されることがあります。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。指定されたDNS名前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、 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 AWS Managed Microsoft AD。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ある必要があります。
- 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は次の形式を使用できません。

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- オペレーティングシステムにログインしているユーザーが複数いる場合、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DNSの名前が解決される IP と一致する必要があります。つまり、クライアントVPNエンドポイントのカスタムDNSレコードを設定し、エンドポイントDNSの名前が解決される実際の IP アドレスにトラフィックを転送する場合、この設定は最近 AWS 提供された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) の 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169.254.0.0/16す。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 に強制しますVPN。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 に使用することをお勧めしますLAN。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 クライアントで使用される証明書は、メモのセクション RFC 4.2 で指定されている証明書拡張を含む、5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile に準拠VPNする必要があります。

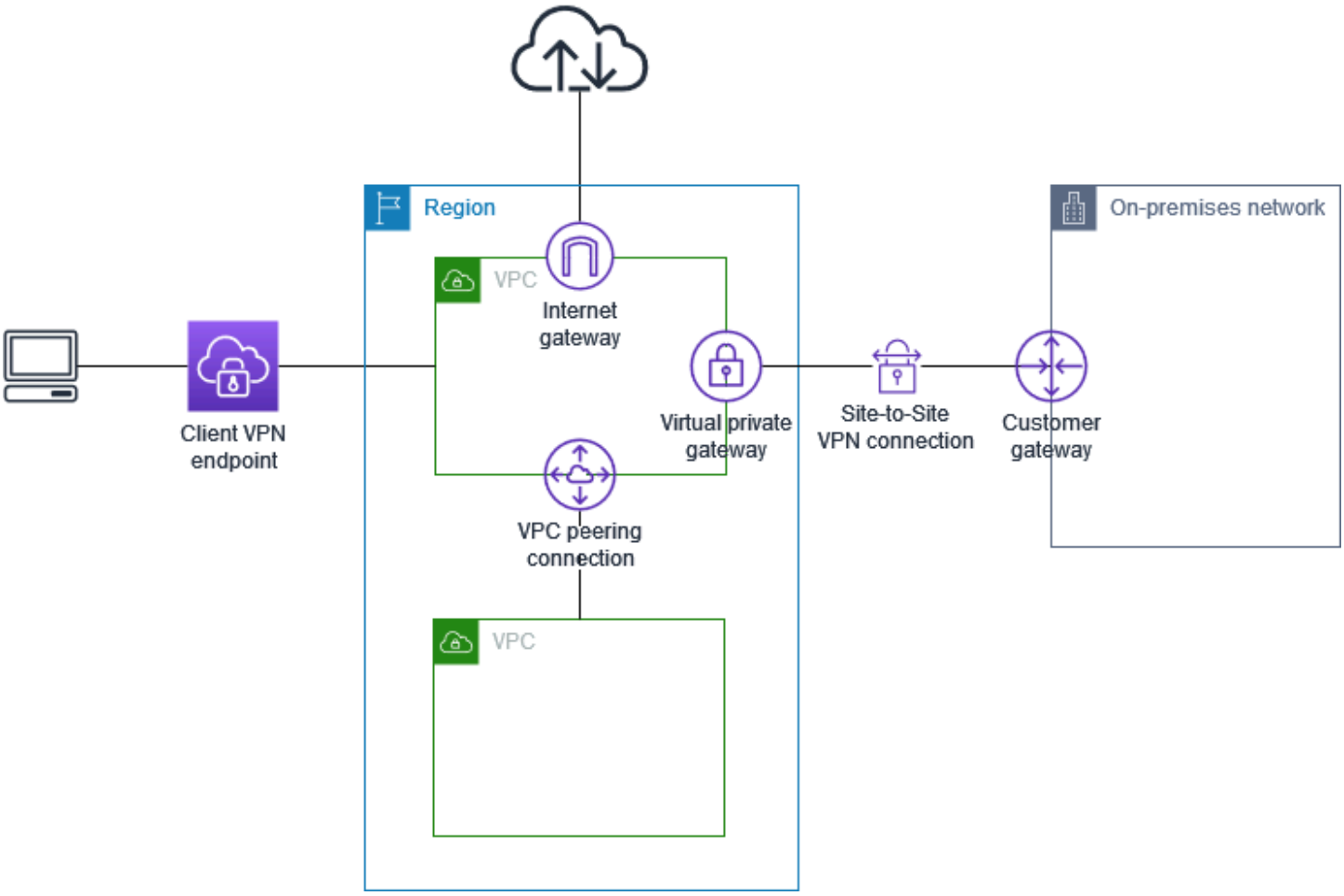
AWS Client VPN の仕組み

では AWS Client VPN、クライアントVPNエンドポイントとやり取りするユーザーペルソナには、管理者とクライアントの 2 種類があります。

管理者は、サービスの設定と設定を担当します。これには、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、認可ルールの設定、および追加のルートの設定 (必要な場合) が含まれます。クライアントVPNエンドポイントをセットアップして設定すると、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、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DNSの名前と、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、「の使用を開始する AWS Client VPN」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、クライアントVPNエンドポイントに接続してVPNセッションを確立するユーザーです。クライアントは、オープンVPN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ると、関連付けられたサブネットがある VPC 内のリソースに安全にアクセスできます。必要なルートと認可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。クライアントVPNエンドポイントに接続してVPNセッションを確立する方法の詳細については、「 AWS Client VPN ユーザーガイド」の「開始方法https://docs.aws.amazon.com/vpn/latest/clientvpn-user/user-getting-started.html」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。



クライアントのシナリオと例 VPN

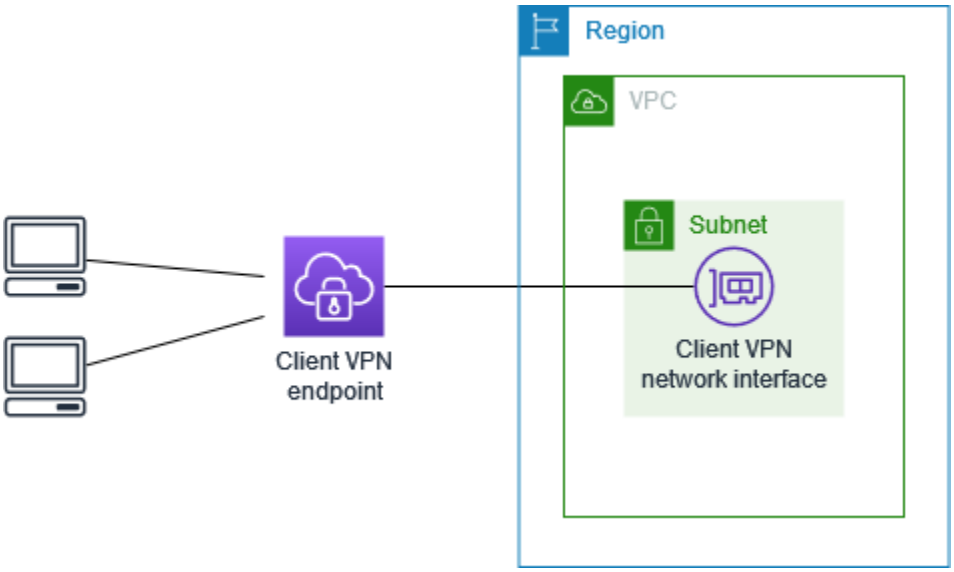
AWS Client VPN は、クライアントが AWS とオンプレミスネットワークの両方内のリソースに安全にアクセスできるようにするフルマネージド型のリモートアクセスVPNソリューションです。アクセスの設定方法には複数のオプションがあります。このセクションでは、クライアントのクライアントVPNアクセスを作成および設定する例を示します。

シナリオ

- the section called “へのアクセス VPC”
- the section called “ピアリング接続された にアクセスする VPC”
- the section called “オンプレミスのネットワークへのアクセス”
- the section called “インターネットへのアクセス”
- the section called “Client-to-client アクセス”
- the section called “ネットワークへのアクセスを制限する”

クライアントVPCを使用して にアクセスする VPN

このシナリオ AWS Client VPN の設定には、単一のターゲット が含まれますVPC。クライアントに 1 つの 内のリソースのみ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VPC。



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VPCを持つ 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VPCに関連付ける のサブネットを特定し、そのIPv4CIDR範囲を書き留めます。
- と重複しないクライアント IP アドレスに適したCIDR範囲を特定しますVPCCIDR。
- 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AWS Client VPNを使用するためのルールとベストプラクティス。

この設定を実装するには

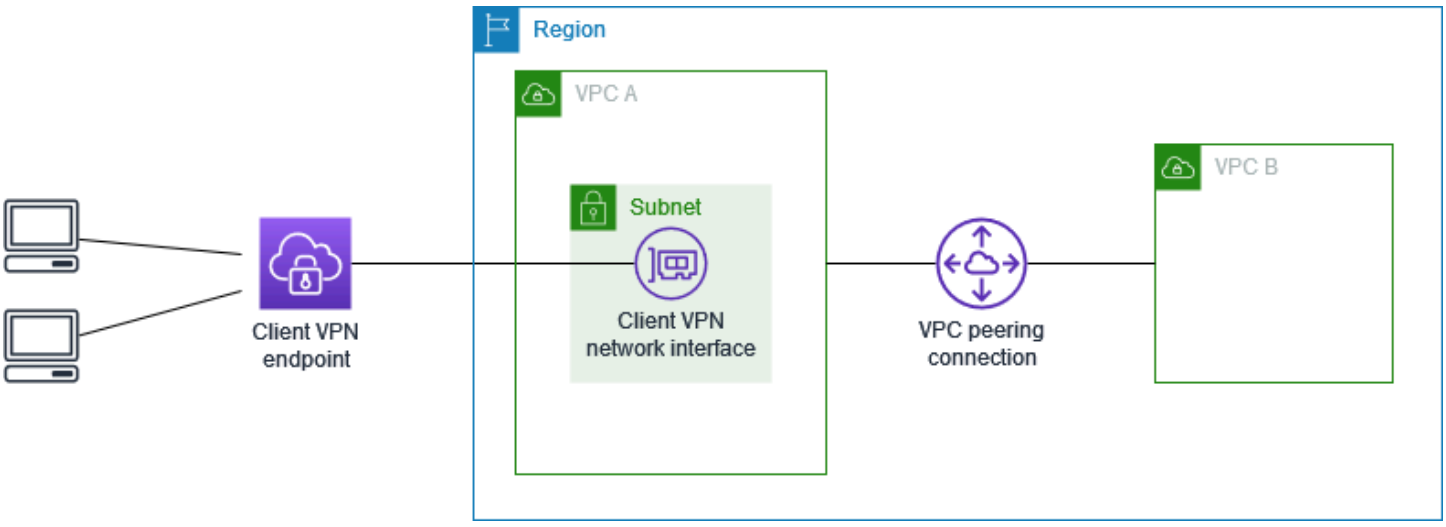
1. と同じリージョンにクライアントVPNエンドポイントを作成しますVPC。これを行うには、「AWS Client VPN エンドポイントを作成する」で説明されているステップを実行します。
2. サブネットをクライアントVPNエンドポイントに関連付けます。これを行うには、「」で説明されているステップを実行し、先ほど特定VPCしたサブネットと ターゲットネットワークをAWS Client VPN エンドポイントに関連付けるを選択します。
3. 認可ルールを追加して、クライアントに へのアクセスを許可しますVPC。これを行うには、「」で説明されているステップを実行し承認ルールを追加する、送信先ネットワークにIPv4CIDRの範囲を入力しますVPC。

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。

クライアントVPCを使用してピアリング接続された にアクセスする VPN

このシナリオ AWS Client VPN の設定には、追加の VPC (VPC B) とピアリング接続されたターゲット VPC (VPC A) が含まれます。ターゲット内のリソースVPCと、ターゲットとピア接続されている他のリソース (VPCB など) へのアクセスをクライアントに許可する必要がある場合VPCsは、この設定をお勧めします。

> **Note**
>
> クライアントVPNエンドポイントが分割トンネルモードに設定されている場合にのみ、ピアリングされた VPC (ネットワーク図に従って概説された) へのアクセスを許可する手順が必要です。フルトンネルモードでは、ピアリングされた へのアクセスVPC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VPCを持つ 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VPCに関連付ける のサブネットを特定し、そのIPv4CIDR範囲を書き留めます。
- と重複しないクライアント IP アドレスに適したCIDR範囲を特定しますVPCCIDR。

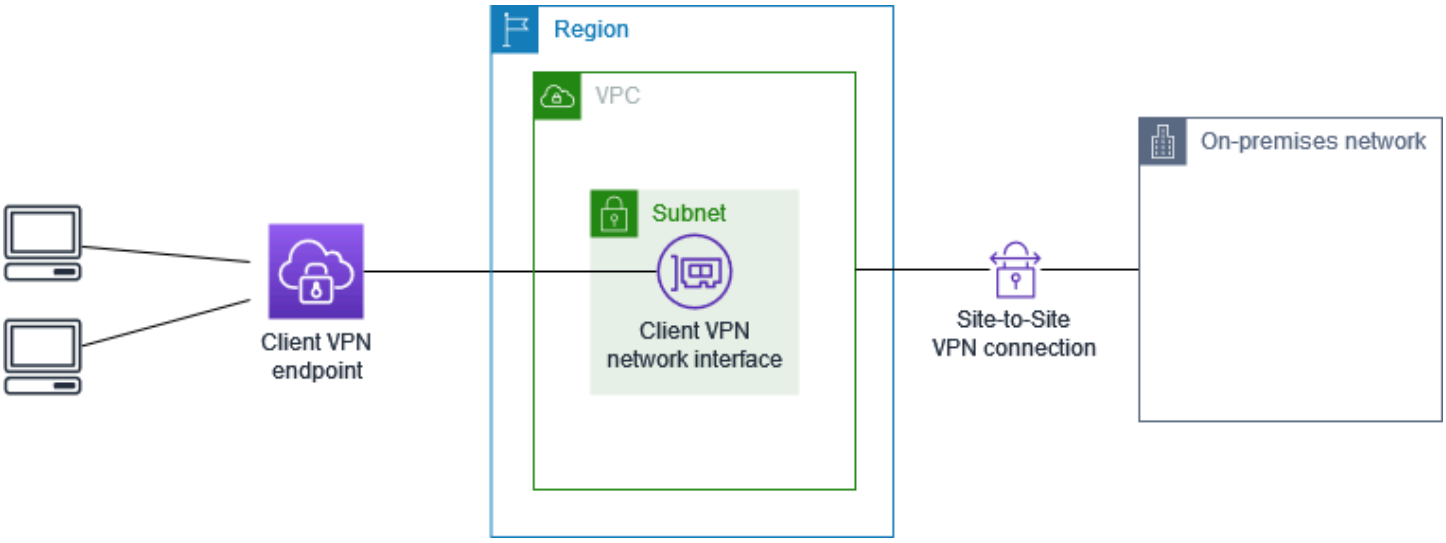
- のクライアントVPNエンドポイントのルールと制限を確認しますAWS Client VPNを使用するためのルールとベストプラクティス。

この設定を実装するには

1. 間のVPCピアリング接続を確立しますVPCs。「Amazon VPCピアリングガイド」の「ピアリング接続の作成と受け入れ」の手順に従います。 VPC VPC A のインスタンスがピアリング接続を使用して 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 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VPC。この図では、これは VPC A です。「」で説明されているステップを実行しますAWS Client VPN エンドポイントを作成する。
3. 識別したサブネットを、作成したクライアントVPNエンドポイントに関連付けます。これを行うには、「」で説明されているステップを実行しターゲットネットワークを AWS Client VPN エンドポイントに関連付ける、 VPCとサブネットを選択します。デフォルトでは、 のデフォルトの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VPC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. クライアントにターゲット へのアクセスを許可する承認ルールを追加しますVPC。これを行うには、「承認ルールを追加する」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で を有効にするには、 IPv4CIDRの範囲を入力しますVPC。
5. ピアリングされた にトラフィックを誘導するルートを追加しますVPC。この図では、これは VPC B です。これを行うには、「」で説明されているステップを実行しますAWS Client VPN エンドポイントルートの作成。ルート送信先には、ピアリングされた IPv4CIDRの範囲を入力しますVPC。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. 認可ルールを追加して、クライアントにピア接続された へのアクセスを許可しますVPC。これを行うには、「承認ルールを追加する」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は、ピアリングされた IPv4CIDRの範囲を入力しますVPC。
7. A と VPC B VPC の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て、ステップ 3 でクライアントVPNエンドポイント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。

クライアントを使用してオンプレミスネットワークにアクセスする VPN

このシナリオ AWS Client VPN 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VPCを持つ 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VPCに関連付ける のサブネットを特定し、そのIPv4CIDR範囲を書き留めます。
- と重複しないクライアント IP アドレスに適したCIDR範囲を特定しますVPCCIDR。
- 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AWS Client VPNを使用するためのルールとベストプラクティス。

この設定を実装するには

1. 接続を介して AWS Site-to-Site VPN 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。

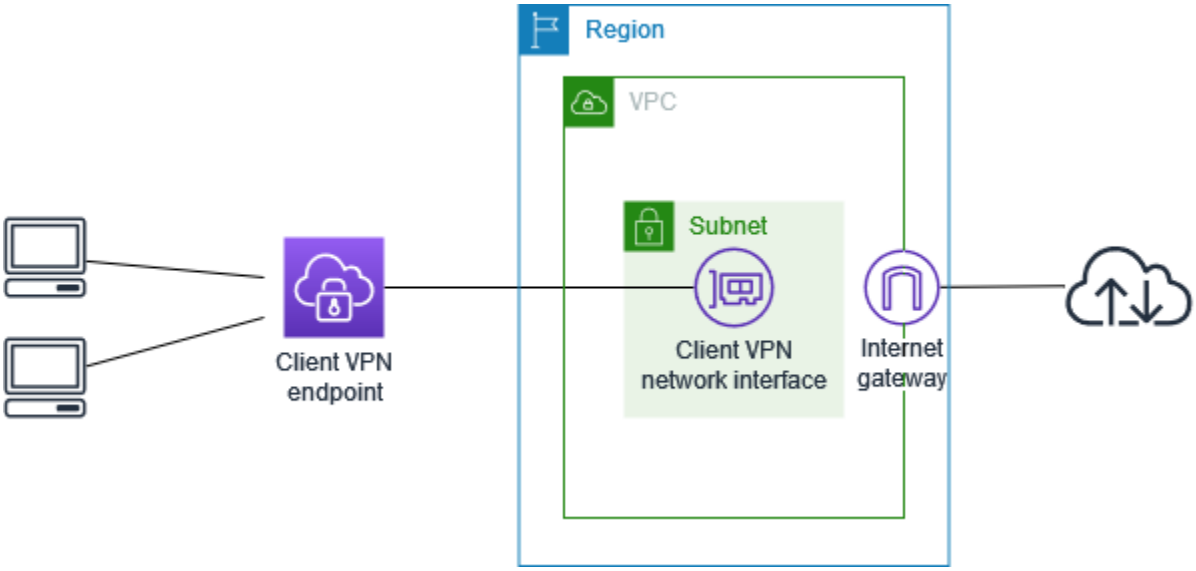
> **Note**
>
> または、 VPCとオンプレミスネットワーク間の AWS Direct Connect 接続を使用して、このシナリオを実装することもできます。詳細については、AWS Direct Connect ユーザーガイドをご参照ください。

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VPN「接続の Site-to-Siteテスト」で説明されているステップを実行します。VPN 接続が正常に機能している場合は、次のステップに進みます。
3. 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VPC。これを行うには、「AWS Client 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. 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、「」で説明されているステップを実行しターゲットネットワークを AWS Client VPN エンドポイントに関連付ける、 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、「」で説明されているステップを実行しますAWS Client VPN エンドポイントルートの作成。ルートの送信先には接続IPv4CIDRの範囲 AWS Site-to-Site VPNを入力し、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られ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、「」で説明されているステップを実行しますAWS Client VPN エンドポイントに承認ルールを追加する。送信先ネットワークの場合は、接続IPv4CIDR範囲を入力します AWS Site-to-Site VPN。

クライアントを使用してインターネットにアクセスする VPN

このシナリオ AWS Client VPN 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ます。クライアントに単一のターゲット内のリソースへのアクセスを許可VPC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。

の使用を開始する AWS Client VPN 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VPCを持つ 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VPCに関連付ける のサブネットを特定し、そのIPv4CIDR範囲を書き留めます。
- と重複しないクライアント IP アドレスに適したCIDR範囲を特定しますVPCCIDR。
- 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AWS Client VPNを使用するためのルールとベストプラクティス。

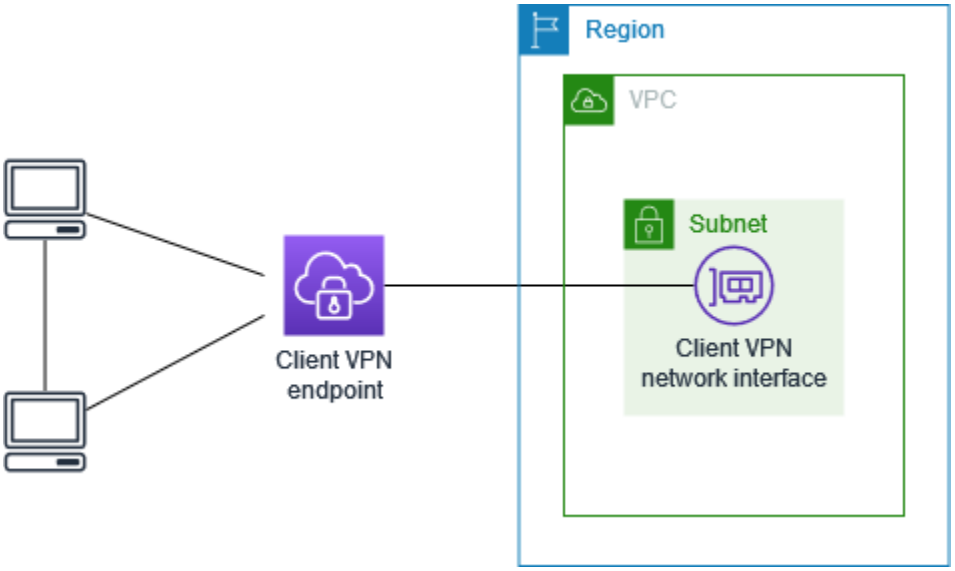
この設定を実装するには

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。これを行うには、 HTTPおよび トラフィックのトラフィックを 0.0.0.0/0 に許可するアウトバウンドルールを追加しますHTTPS。
2. インターネットゲートウェイを作成し、 にアタッチしますVPC。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サブネットを選択し、ルートテーブルを選択してから、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. 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VPC。これを行うには、「AWS Client 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. 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、「」で説明されているステップを実行しターゲットネットワークを AWS Client VPN エンドポイントに関連付ける、 VPC とサブネットを選択します。
6. 認可ルールを追加して、クライアントに へのアクセスを許可しますVPC。これを行うには、承認ルールを追加する「」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で を有効にするには、 IPv4CIDRの範囲を入力しますVPC。
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、「」で説明されているステップを実行しますAWS Client VPN エンドポイントルートの作成。ルートの送信先には「」と入力し`0.0.0.0/0`、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られたサブネットを選択します。
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、「承認ルールを追加する」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. 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VPCがあることを確認します。これにより、クライアントは のリソースにアクセスできますVPC。

Client-to-client クライアントを使用した アクセス VPN

このシナリオ AWS Client VPN の設定により、クライアントは単一の にアクセスしVPC、クライアントはトラフィックを相互に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VPCを持つ 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VPCに関連付ける のサブネットを特定し、そのIPv4CIDR範囲を書き留めます。
- と重複しないクライアント IP アドレスに適したCIDR範囲を特定しますVPCCIDR。
- 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AWS Client VPNを使用するためのルールとベストプラクティス。

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

この設定を実装するには

1. 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VPC。これを行うには、「AWS Client 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. 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、「」で説明されているステップを実行しターゲットネットワークを AWS Client VPN エンドポイントに関連付ける、 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、「AWS Client VPN 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。ルート

送信先にはクライアントCIDR範囲を入力し、ターゲットVPCサブネット ID には を指定しますlocal。

4. 認可ルールを追加して、クライアントに へのアクセスを許可しますVPC。これを行うには、「承認ルールを追加する」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で を有効にするには、 IPv4CIDRの範囲を入力しますVPC。
5. クライアントにクライアントCIDR範囲へのアクセスを許可する承認ルールを追加します。これを行うには、「承認ルールを追加する」で説明されているステップを実行します。有効にする送信先ネットワークには、クライアントCIDR範囲を入力します。

クライアントを使用してネットワークへのアクセスを制限する VPN

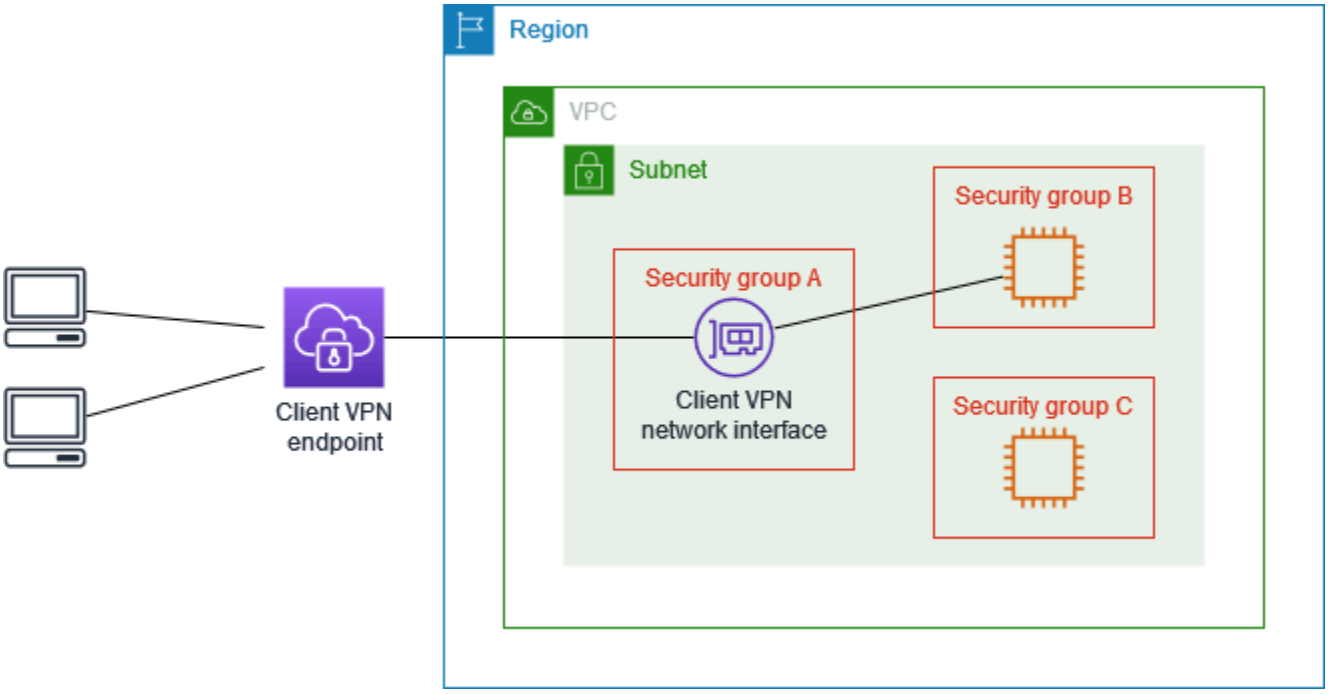
AWS Client VPN エンドポイントを設定して、 内の特定のリソースへのアクセスを制限できますVPC。ユーザーベースの認証では、クライアントVPNエンドポイントにアクセスするユーザーグループに基づいて、ネットワークの一部へのアクセスを制限することもできます。

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 (クライアントセキュリティグループ) に適用された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VPCすることで、 内の特定のリソースへのアクセスを許可または拒否できますVPN。この設定は「クライアントVPCを使用して にアクセスする VPN」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承認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。

次の図では、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、セキュリティグループ B はEC2インスタンス、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 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VPC。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場合、他の関連リソースへのアクセスを許可または削除することもできます。これを防ぐには、クライアントVPNエンドポイントで使用するために特別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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
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、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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Security Groups] 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。Source 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、ルールの編集を選択し、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、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、以下の各トピックを参照してください。
   - クライアントでの Active Directory 認証 VPN
   - SAMLベースのフェデレーション認証の要件と考慮事項
2. ネットワークの全部または一部への指定されたグループアクセスを許可するクライアントVPNエンドポイントの認可ルールを作成します。詳細については、「AWS Client VPN 認可ルール」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、ユーザーグループを設定することはできません。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。特定のユーザーの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できます。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、「での相互認証 AWS Client VPN」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、「AWS Client 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承認ルールを作成できます。詳細については、「承認ルールを追加する」を参照してください。

でのクライアント認証 AWS Client VPN

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。これは、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、VPNセッションを確立します。認証に失敗すると、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。

クライアントは、次のタイプのクライアント認証VPNを提供します。

- 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ティッド認証) (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、「での相互認証 AWS Client VPN」の手順を参照してください。

クライアントでの Active Directory 認証 VPN

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。

クライアントは、 Managed Microsoft AD または AD Connector で AWS 有効になっている場合、多要素認証 (MFA) VPN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。の有効化の詳細についてはMFA、「 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」および「AD Connector の多要素認証を有効にする」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。

での相互認証 AWS Client VPN

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。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VPNエンドポイントに接続しようとしたときに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 にアップロードするときは ACM、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 については、「AWS Certificate Manager User Guide」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、ARNクラ

イアント証明書のサーバー証明書を指定できます。ただし、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ることが条件です。

AWS クライアントで使用される証明書は、メモのセクション RFC 4.2 で指定された証明書拡張を含む、5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile に準拠VPNする必要があります。

> **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キーサイズのみをサポートします。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サービスで使用されている証明書が更新されると、ACM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 へのメタデータ更新によって、クライアントVPNサービスは新しい証明書でクライアントVPNエンドポイントを自動的に更新します。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。

タスク

- AWS Client VPN の相互認証を有効にする
- AWS Client VPN サーバー証明書の更新

AWS Client VPN の相互認証を有効にする

Linux/MacOS または Windows でクライアント VPN で相互認証を有効にすることができます。

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。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。

AWS Client VPN サーバー証明書の更新

有効期限が切れたクライアント VPN 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に関するドキュメント」を参照してください。

サーバー証明書を更新するには

1. 次のいずれかを行います。
   - 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. 期限切れにするコマンドを実行します。

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

        ```
        $ ./easyrsa --san=DNS:server 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 \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

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 — クライアント VPN

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。2.0 をサポートする ID プロバイダー (IdPs) SAML 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を使用す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。

トピック

- AWS Client VPN の SAML を有効にする
- 認証ワークフロー
- 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 IdP 設定リソース

AWS Client VPN の SAML を有効にする

次の手順を実行して、クライアント VPN のシングルサインオンの SAML を有効にすることができます。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アクセスして設定ファイルと AWS が提供する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、「AWS Client VPN セルフサービスポータルへのアクセス」を参照してください。

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. AWS Client VPN と連携するには、選択した IdP で SAML ベースのアプリを作成するか、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 の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。

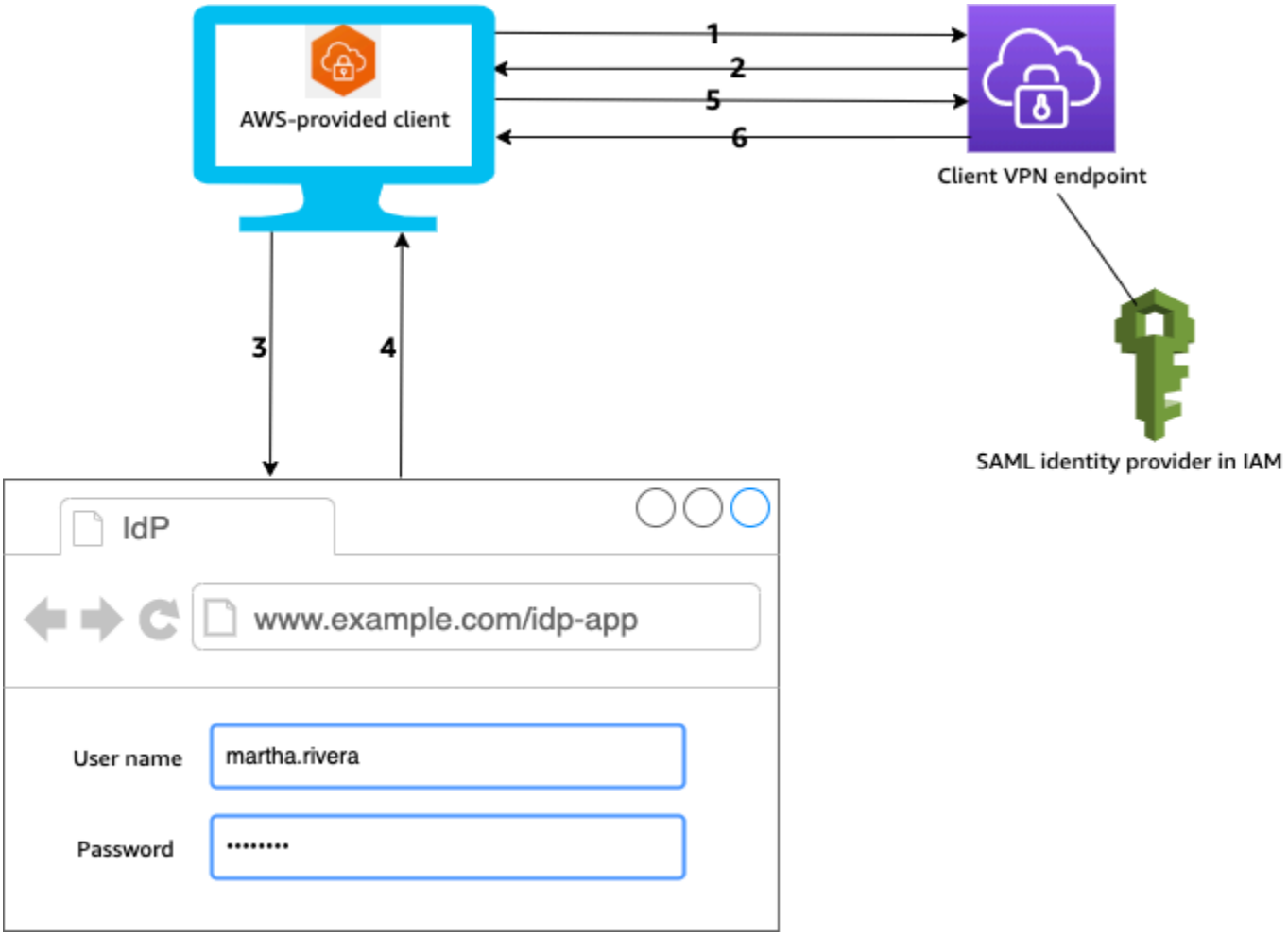
   IAM SAML ID プロバイダーは、IdP によって生成されたメタデータドキュメントを使用して、組織の IdP と AWS の信頼関係を定義します。詳細については、IAM ユーザーガイドの「SAML ID プロバイダーの作成」を参照してください。後で IdP のアプリ設定を更新する場合は、新しいメタデータドキュメントを生成し、IAM SAML ID プロバイダーを更新します。

   > **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、「AWS Client 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。

認証ワークフロー

次の図は、 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ています。クライアントVPNエンドポイントを作成して設定するときは、IAMSAMLID 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、IAMSAMLID 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. ユーザーはログインページで認証情報を入力し、IdP は署名付きSAMLアサーションをクライアントに送り返します。

5. AWS 提供されたクライアントは、クライアントVPNエンドポイントにSAMLアサーションを送信します。
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、「」を参照してくださいユーザーとグループのクォータ。
- SAML アサーションとSAMLドキュメントは署名する必要があります。
- AWS Client VPN は、SAMLアサーションでAudienceRestriction「」およびNotBefore 「and NotOnOrAfter」条件のみをサポートします。
- SAML レスポンス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。
- クライアントVPNエンドポイントは 1 つの IdP のみをサポートします。
- 多要素認証 (MFA) は、IdP で有効になっている場合にサポートされます。
- 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 提供されたクライアントは、ユーザーのデバイスでSAMLレスポンス用にTCPポート 35001 を予約します。
- IAM SAML ID プロバイダーのメタデータドキュメントが不正または悪意のある で更新されるとURL、ユーザーの認証の問題が発生したり、フィッシング攻撃が発生したりする可能性があります。したがって、 AWS CloudTrail を使用して、IAMSAMLID プロバイダーに加えられた更新を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「 を使用したログ記録IAMと AWS STS 呼び出し AWS CloudTrail」を参照してください。

- AWS Client VPN は、リダイレクトバインディングを介して IdP に AuthN HTTP リクエストを送信します。したがって、IdP はHTTPリダイレクトバインディングをサポートし、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 アサーションには、 `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、 での使用がテスト IdPs された SAMLベースの 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	で AWS Client VPN ユーザーを認証する SAML
Microsoft Entra ID (以前の Azure Active Directory)	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: Microsoft Entra シングルサインオン (SSO) と AWS クライアントの統合VPN」を参照してください。
JumpCloud	との統合 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。

- アサーションコンシューマーサービス (ACS) URL: `http://127.0.0.1:35001`
- 対象者URI: `urn:amazon:webservices:clientvpn`

IdP からのSAMLレスポンスには、少なくとも 1 つの属性を含める必要があります。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 IdP SAML グループベースの承認ルールを使用するために必要です。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「AWS Client VPN 認可ルール」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エンドポイントのセルフサービスポータルを有効にすると、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 が複数のアサーションコンシューマーサービス (ACS) をサポートしている場合はURLs、アプリACSURLに以下を追加します。

```
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、ACSURL代わりに以下を使用します。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、 の両方を追加できますURLs。

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

IdP が複数の ACS をサポートしていない場合はURLs、次の操作を行います。

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

   ```
   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IAMSAML「 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 ID 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、作成した両方の IAM SAML ID プロバイダーを指定します。

でのクライアント認可 AWS Client VPN

クライアントは、セキュリティグループとネットワークベースの認可 (認可ルールを使用) の 2 種類のクライアント認可VPNをサポートしています。

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 のセキュリティグループを指定VPC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のデフォルトのセキュリティグループが自動的に適用されます。セキュリティグループは、クライアントVPNエンドポイントの作成後に変更できます。詳細については、「AWS Client VPN の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」を参照してください。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ています。

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ルールをアプリケーションのセキュリティグループに追加VPCすることで、クライアントVPNユーザーが 内のアプリケーションにアクセスできるようにします。

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、「クライアントのシナリオと例 VPN」を参照してください。

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「 のセキュリティグループVPC」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。指定されたネットワークでは、アクセスが許可されている Active Directory グループまたは SAMLベースの IdP グループを設定します。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ティッド認証を使用していない場合、またはすべてのユーザーへのアクセスを開く場合は、すべてのクライアントへの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、「AWS Client VPN 認可ルール」を参照してください。

タスク

- AWS Client VPN エンドポイントセキュリティグループルールを作成する

AWS Client VPN エンドポイントセキュリティグループルールを作成する

サブネットをクライアントに関連付けるときにVPC適用される のデフォルトのセキュリティグループは、許可するデフォルトのセキュリティグループトラフィックからのトラフィックを制限し、同時に許可しないトラフィックを許可するVPN場合があります。リソースまたはアプリケーションに関連付けられたVPNエンドポイントセキュリティグループのトラフィックを許可または制限するクライアントエンドポイントセキュリティグループルールを作成するには、次のステップを使用します。セキュリティグループルールの詳細については、「Amazon VPCユーザーガイド」の「 のセキュリティグループVPC」を参照してください。

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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
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、 などの特定のタイプのトラフィックへのアクセスを制限することもできますSSH。

Source には、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。

での接続認可 AWS Client VPN

クライアント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。 VPN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 関数を作成します AWS Lambda 。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のみがクライアントVPNエンドポイントに接続できます。

> **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、クライアントVPNエンドポイントと同じ AWS リージョンおよび同じ AWS アカウントに存在する必要があります。
- 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。
- Lambda 関数が新しい接続に対して呼び出され、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サービスは接続リクエストを拒否します。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、「AWS Client VPN クライアント接続を終了する」を参照してください。
- クライアントが AWS が提供するクライアントを使用してクライアントVPNエンドポイントに接続する場合は、Windows の場合はバージョン 1.2.6 以降、macOS の場合はバージョン 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、デバイス属性、ユーザー属性、および接続属性をクライアントVPNサービスからの入力として受け取ります。次に、接続を許可するか拒否するかの決定をクライアントVPNサービスに返す必要があります。

リクエストスキーマ

Lambda 関数は、以下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 ですNameID。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に Open VPNクライアント設定に --push-peer-info ディレクティブが存在する場合、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 — AWS クライアントバージョン。
- 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ティッド認証の場合、これは ID プロバイダー (IdP) グループのリストになります。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 関数をデバイス認可ハンドラーとして機能させるには、クライアントVPNエンドポイントの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 (クライアントVPNサービスから渡される) の一意の共通名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。例えば、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**
>
> 接続ハンドラーを使用して最小 AWS Client VPN アプリケーションバージョンを適用できますが、接続ハンドラー`aws-client-version`の フィールドは AWS Client VPN アプリケーションにのみ適用され、ユーザーデバイス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を有効化する

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、AWS Client VPN エンドポイントを作成するおよびAWS Client 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 は、 というサービスにリンクされたロールをアカウントに自動的に作成します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、「のサービスにリンクされたロールの使用 AWS Client VPN」を参照してください。

接続承認失敗をモニタリングする

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

クライアント接続ハンドラーを体制評価に使用すると、接続ログでクライアント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表示することもできます。詳細については、「AWS Client VPN エンドポイントの接続ログ記録」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。

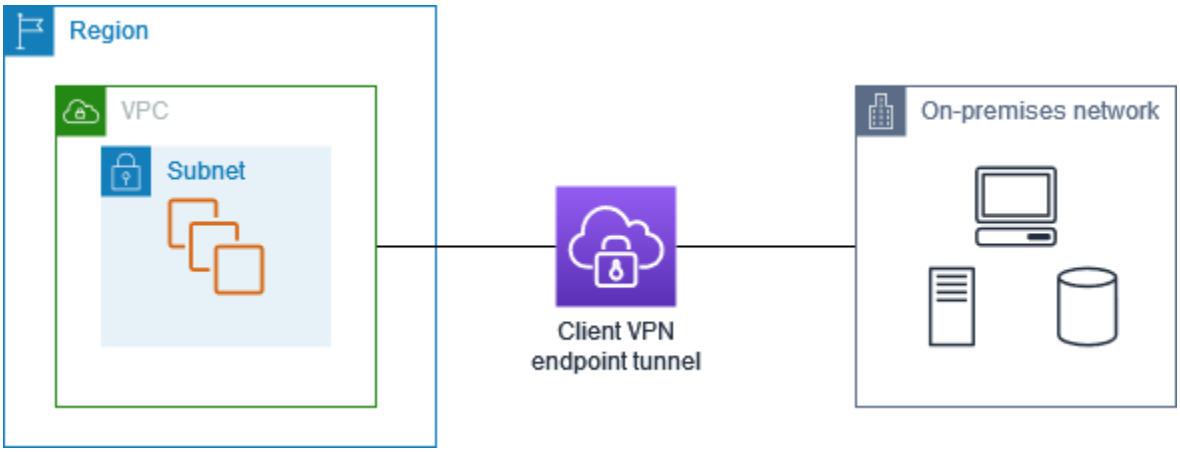
- `client-connect-failed` — Lambda 関数によって接続が確立されませんでした。
- `client-connect-handler-timed-out` — Lambda 関数がタイムアウトしました。
- `client-connect-handler-other-execution-error` — Lambda 関数で予期しないエラーが発生しました。
- `client-connect-handler-throttled` — Lambda 関数がスロットルされました。
- `client-connect-handler-invalid-response` — 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。

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に一致するネットワークへの送信先を持つ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。

すべてのユーザートラフィックがクライアントVPNエンドポイントを経由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。

- 送信 AWS 先トラフィックのみがVPNトンネルを通過す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。
- からの送信トラフィックの量を減らすことができるため AWS、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

- 分割トンネルモードを有効にすると、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、クライアントのルートテーブルを エントリで上書き`0.0.0.0/0`して、 経由ですべてのトラフィックをルーティングするデフォルトの動作とは異なりますVPN。

> **Note**
>
> 分割トンネルモードを使用するときにクライアントVPNエンドポイントのルートテーブルに 0.0.0.0/0 ルートを追加すると、接続が中断される可能性があるため、推奨されません。

- 分割トンネルモードが有効になっている場合、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、以下の各トピックを参照してください。

- AWS Client VPN エンドポイントを作成する
- AWS Client VPN エンドポイントを変更する

AWS Client VPN エンドポイントの接続ログ記録

接続ログ記録は、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 AWS Client VPN できる の機能です。

接続ログには、クライアント (エンドユーザー) がクライアントエンドポイントに接続する、接続を試みる、クライアントVPNエンドポイントから切断するなど、接続イベントに関する情報をキャプチャする接続ログエントリが含まれます。この情報を使用して、フォレンジックの実行、クライアントVPNエンドポイントの使用方法の分析、接続問題のデバッグを行うことができます。

接続ログは、 AWS Client VPN が利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IPv4CIDR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) が使用されたときに記録されます。
- connection-duration-seconds - 接続の継続時間 (秒)。connection-start-time「」と「」の差と同じですconnection-end-time。

接続ログの有効化の詳細については、「AWS Client VPN 接続ログ」を参照してください。

クライアントの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の需要に合わせてスケーリングできるかどうかを考慮する必要があります。

次の要因は、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。クライアント範囲は、/12 ネットマスクと /22 ネットマスクの間の IPv4CIDRブロックです。クライアントVPNエンドポイントへの各VPN接続には、クライアントCIDR範囲から一意の IP アドレスが割り当てられます。クライアントCIDR範囲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。

一般的に、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 アドレスの数の 2 倍 (つまり同時接続) 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、ユーザーがクライアント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クライアントVPNエンドポイントに関連付けることで、高可用性を実現したり、追加の接続容量を有効にしたりできます。

クライアントVPNエンドポイントのサブネット関連付けの数に基づいて、サポートされている同時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	20,000
2	36,500

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

同じ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 リージョンで使用できる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 VPNの接続をサポートすることが予想される場合は、最小クライアントCIDR範囲サイズ /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接続数が不明な場合は、サイズ/16CIDRブロック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を操作するためのルールと制限の詳細については、「」を参照してくださいAWS Client VPNを使用するためのルールとベストプラクティス。

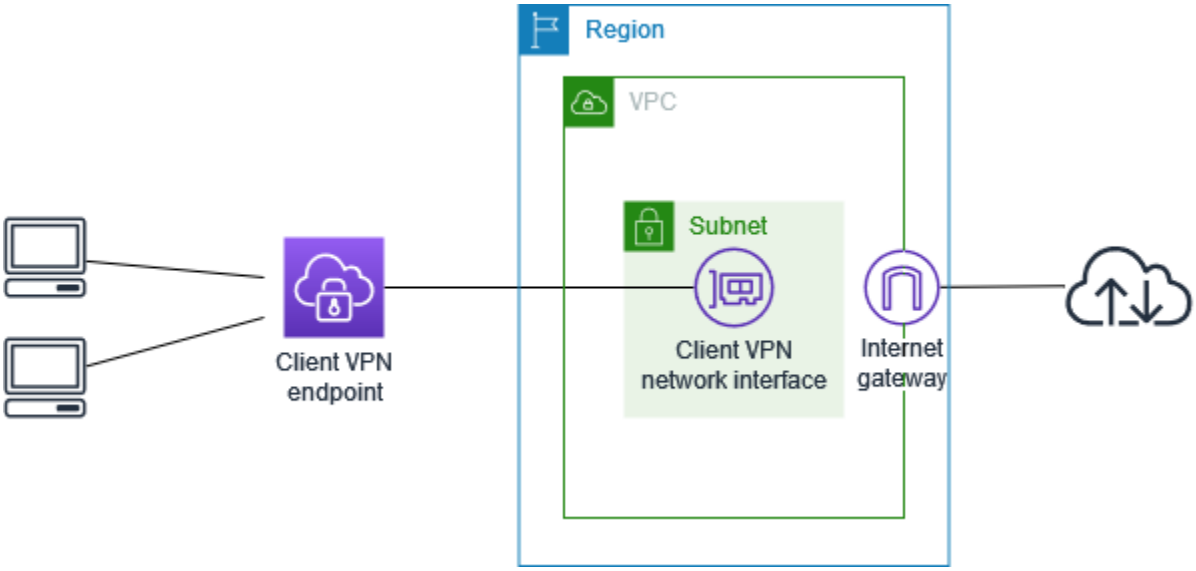
クライアントVPNエンドポイントのクォータの詳細については、「」を参照してくださいAWS Client VPN クォータ。

の使用を開始する AWS Client VPN

このチュートリアルでは、以下を実行する AWS Client VPN エンドポイントを作成します。

- すべてのクライアントに 1 つの へのアクセスを提供しますVPC。
- 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: の承認ルールを追加する VPC
- 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アクセス許可。
- 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VPCを持つ 。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) にインポートし、クライアントVPNエンドポイントの作成時に指定する必要があります。クライアント証明書の へのインポートACMはオプションです。

この目的で使用する証明書がまだない場合は、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とクライアントの証明書とキーを生成し、 にインポートする詳細な手順については、ACM「」を参照してくださいでの相互認証 AWS Client VPN。

> **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セッションを有効化および管理するために作成および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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで、クライアントVPNエンドポイントを選択し、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. クライアント にはIPv4CIDR、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**
>
> アドレス範囲は、ターゲットネットワークアドレス範囲、VPC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することはできません。クライアントアドレス範囲は /22 以上で、/12 CIDRブロックサイズ以下である必要があります。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アドレス範囲を変更することはできません。

5. サーバー証明書 でARN、ステップ 1 で生成したサーバー証明書ARNの を選択します。 ???
6. 「認証オプション」で「相互認証を使用する」を選択し、「クライアント証明書ARN」で、クライアント証明書として使用する証明書ARNの 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局 (CA) によって署名されている場合、クライアント証明書とサーバー証明書の両方ARNにサーバー証明書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. (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サーバー 1 の IP アドレスとDNSサーバー 2 の 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サーバー 1 の IP アドレスまたはDNSサーバー 2 の IP アドレスのいずれかで、IP アドレスを指定し、VPCDNS サーバー IP アドレスを追加します。

> **Note**
>
> クライアントがDNSサーバーにアクセスできることを確認します。

8. 残りのデフォルト設定を保持し、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 になりますpending-associate。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にのみ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、「」を参照してくださいAWS Client 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

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、 のサブネットですVPC。

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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、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、ターゲットネットワークの関連付け、ターゲットネットワークの関連付けを選択します。
4. にはVPC、サブネットVPCがある を選択します。
5. 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. 承認ルールで許可されている場合は、クライアントが VPCのネットワーク全体にアクセスするために 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、次のようになります。

- クライアントVPNエンドポイントの状態が に変わりますavailable。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、承認ルールを追加するVPCまで のリソースにアクセスすることはできません。
- のローカルルートVPCは、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は、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: の承認ルールを追加する VPC

クライアントが にアクセスするにはVPC、クライアントVPNエンドポイントのルートテーブルVPC に へのルートと認可ルールが必要です。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 へのアクセスを許可しますVPC。

の認可ルールを追加するには VPC

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、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. 送信先ネットワークでアクセスを有効にするには、アクセスを許可するネットワークの CIDR を入力します。たとえば、 全体へのアクセスを許可するにはVPC、 の IPv4CIDRブロックを指定しますVPC。
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、ピアリング接続された VPC、VPCsオンプレミスネットワーク、インターネットなど、 に接続された追加のネットワーク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でネットワークにルートを追加し、クライアントにアクセスを許可する承認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 へのアクセスを許可しますVPC。へのアクセスは既に設定されているためVPC、このステップはインターネットへのアクセス用です。

インターネットへのアクセスを提供するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、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 のクライアントVPNエンドポイントの作成中にセキュリティグループが指定されていませんでした。つまり、ターゲットネットワークが関連付けられると、 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VPCに自動的に適用されます。その結果、 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るVPCようになりました。

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) が、インターネットへのアウトバウンドトラフィックを許可していること。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。
- 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 (この場合はデフォルトのVPCセキュリティグループ) に適用される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VPCがあること。これにより、クライアントは のリソースにアクセスできますVPC。

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、VPN接続を確立するために必要なクライアントVPNエンドポイントの詳細と証明書情報が含まれています。このファイルは、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 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. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、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、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 リポジトリ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布します。

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、「」を参照してくださいAWS Client VPN エンドポイント設定ファイルのエクスポート。

ステップ 8: 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VPNエンドポイントに接続するには、 AWS が提供するクライアントまたは別のオープンVPNベースのクライアントアプリケーションと、先ほど作成した設定ファイルを使用します。詳細については、AWS Client VPN ユーザーガイドをご参照ください。

の操作 AWS Client VPN

以下のトピックでは、クライアント の操作に必要な主要な管理タスクについて説明しますVPN。

- セルフサービスポータルへのアクセス — クライアントがクライアントVPNエンドポイント設定ファイルを自分でダウンロードできるように、クライアントVPNセルフサービスポータルへのアクセスを設定します。セルフサービスポータルへのアクセスについては、「the section called “セルフサービスポータルへのアクセス”」を参照してください。
- 承認ルール — 指定されたネットワークへのクライアントアクセスを制御するための承認ルールを追加します。承認ルールの追加については、「the section called “承認ルール”」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、クライアントVPNエンドポイントへのアクセスを取り消します。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、「the section called “クライアント証明書失効リスト”」を参照してください。
- クライアント接続 — クライアントVPNエンドポイントへのクライアント接続を表示または終了します。クライアント接続の表示または終了については、「the section called “クライアント接続”」を参照してください。
- クライアントログインバナー — VPNセッションが確立されると、クライアントVPNデスクトップアプリケーションにテキストバナーを追加します。規制およびコンプライアンスのニーズを満たすために、テキストバナーを使用できます。ログインバナーの詳細については、「the section called “クライアントログインバナー”」を参照してください。
- クライアントVPNエンドポイント — すべてのVPNセッションを管理および制御するようにクライアントVPNエンドポイントを設定します。エンドポイントの設定については、「the section called “エンドポイント”」を参照してください。
- 接続ログ — 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します。接続ログの詳細については、「the section called “接続ログ”」を参照してください。
- クライアント設定ファイルのエクスポート — クライアントクライアントがVPN接続を確立するために必要なVPNクライアント設定ファイルを設定します。ファイルを設定したら、クライアントに配布するためにダウンロード (エクスポート) します。クライアント設定ファイルのエクスポートについては、「the section called “エンドポイント設定ファイルのエクスポート”」を参照してください。
- ルート — 各クライアントVPNルートの認可ルールを設定して、送信先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。承認の設定については、「the section called “承認ルール”」を参照してください。

- ターゲットネットワーク — 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て、クライアントがそれに接続してVPN接続を確立できるようにします。ターゲットネットワークの詳細については、「the section called “ターゲットネットワーク”」を参照してください。
- 最大VPNセッション期間 — 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、最大VPNセッション期間のオプションを設定します。最大VPNセッション期間の詳細については、「」を参照してくださいthe section called “最大VPNセッション期間”。

AWS Client VPN セルフサービスポータルへのアクセス

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 をクライアントに提供できますURL。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でき、 AWS 提供されたクライアントの最新バージョンをダウンロードできます。

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使用できる設定ファイルは、Amazon VPCコンソールまたは を使用してエクスポートする設定ファイルと同じです AWS CLI。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ら、次のいずれかの をクライアントに提供しますURLs。

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

  クライアントがこの を使用してポータルにアクセスする場合はURL、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>`

  前述の *<endpoint-id>* の を、 などのクライアントVPNエンドポイントの ID URLに置き換えますcvpn-endpoint-0123456abcd123456。

コマンドURLの出力でセルフサービスポータルの を表示することもできますdescribe-client-vpn-endpoints AWS CLI 。または、Amazon URL VPCコンソールのクライアントVPNエンドポイントページの 詳細 タブで を使用できます。

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。

AWS Client VPN 認可ルール

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 を使用して、クライアントVPNエンドポイントに認可ルールを追加できます AWS CLI。

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

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処理されます。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。
- 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送信先」と考える`0.0.0.0/0`CIDR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。

トピック

- クライアントVPN承認ルールのシナリオ例
- AWS Client VPN エンドポイントに承認ルールを追加する
- AWS Client VPN エンドポイントから承認ルールを削除する
- AWS Client VPN 承認ルールの表示

クライアントVPN承認ルールのシナリオ例

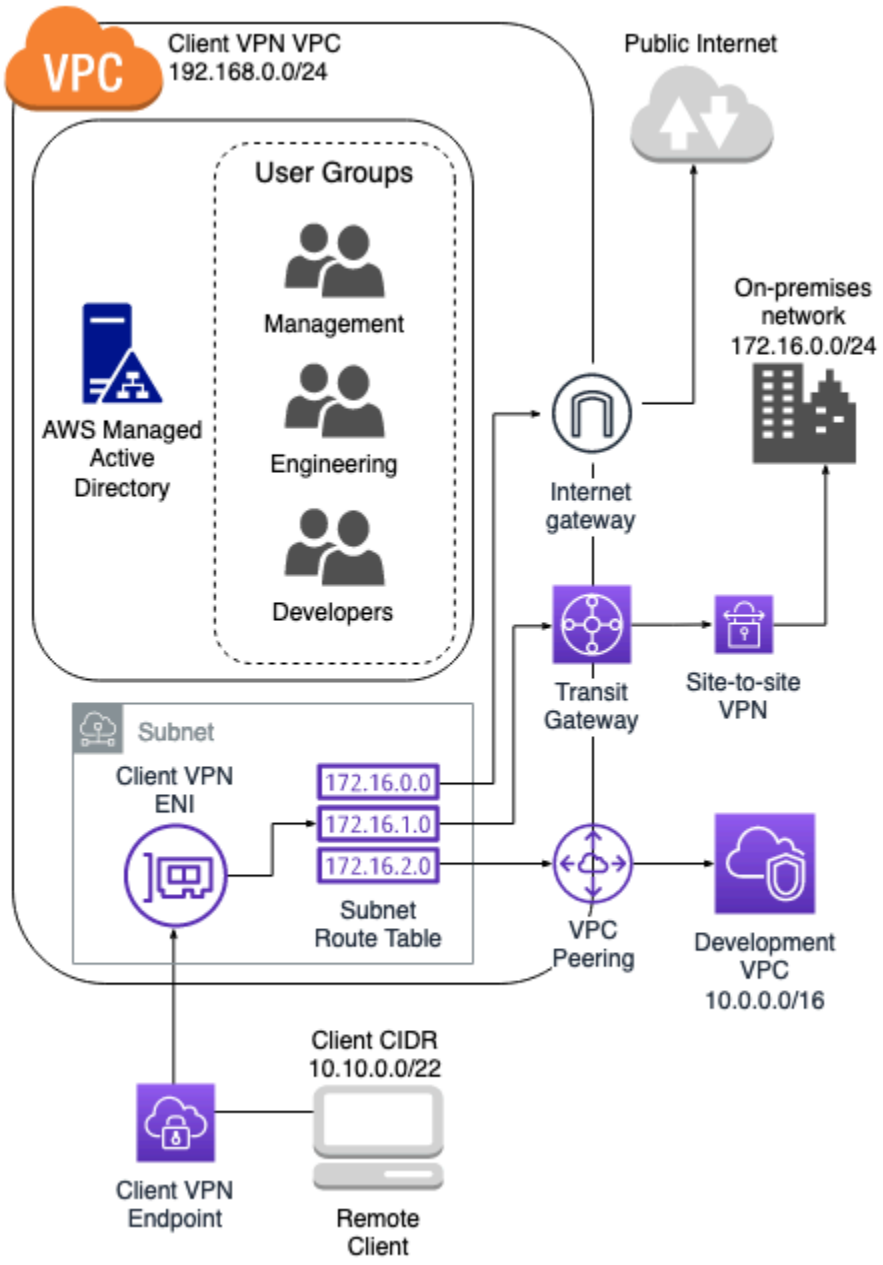
このセクションでは、認可ルールの仕組みについて説明します AWS Client VPN。承認ルールを理解するための重要なポイント、アーキテクチャの例、およびアーキテクチャの例に対応するシナリオ例の説明が含まれています。

シナリオ

- the section called “アーキテクチャの例”
- the section called “単一の送信先へのアクセス”
- the section called “任意の送信先 (0.0.0.0/0) を使用する CIDR”
- the section called “IP プレフィックスのより長い一致”
- the section called “重複 CIDR (同じグループ) ”
- the section called “追加の 0.0.0.0/0 ルール”
- the section called “192.168.0.0/24 のルールを追加する”
- the section called “すべてのユーザーグループのアクセス”

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。



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へのアクセスを提供する VPC	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へのアクセスを提供する VPN VPC	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ドロップされます。

> **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。

任意の送信先 (0.0.0.0/0) を使用する CIDR

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へのアクセスを提供する VPC	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。

IP プレフィックスのより長い一致

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へのアクセスを提供する VPC	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
開発中の 1 つのホストにマネージャーグループアクセスを提供する VPC	s-xxxxx16	False	10.0.2.119/32

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、開発 内のパブリックインターネット192.168.0.0/24、、および 1 つのホスト (10.0.2.119/32) にアクセスできますがVPC、開発 内の残りのホスト172.16.0.0/24にはアクセスできませんVPC。

> **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。

重複 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へのアクセスを提供する VPC	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
開発中の単一ホストへのマネージャーグループアクセスを提供する VPC	s-xxxxx16	False	10.0.2.119/32
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	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
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。

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へのアクセスを提供する VPC	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			
開発中の単一ホストへのマネージャーグループアクセスを提供する VPC	s-xxxxx16	False	10.0.2.119/32
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。

192.168.0.0/24 のルールを追加する

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へのアクセスを提供する VPC	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
開発中の単一ホストへのマネージャーグループアクセスを提供する VPC	s-xxxxx16	False	10.0.2.119/32
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へのアクセスを提供する VPN VPC	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。

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へのアクセスを提供する VPC	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
開発中の単一ホストへのマネージャーグループアクセスを提供する VPC	s-xxxxx16	False	10.0.2.119/32
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へのアクセスを提供する VPN VPC	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	真	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。

AWS Client VPN エンドポイントに承認ルールを追加する

を使用して、クライアントVPNエンドポイントへのアクセスを許可または制限する承認ルールを追加できます AWS Management Console。認可ルールは、Amazon VPCコンソールを使用するか、コマンドラインまたは を使用してクライアントVPNエンドポイントに追加できますAPI。

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 AWS Management Console

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、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、認可ルールを選択し、認可ルールを追加を選択します。
4. 送信先ネットワークでアクセスを有効にするには、ユーザーがアクセスするネットワークの IP アドレス (の CIDRブロックなどVPC) をCIDR表記で入力します。
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。例えば、Active Directory グループのセキュリティ識別子 (SID) 、または 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/名前などです。
     - (アクティブディレクトリ) を取得するにはSID、Microsoft Powershell Get-ADGroup コマンドレットを使用できます。次に例を示します。

       ```
       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 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。

AWS Client VPN エンドポイントから承認ルールを削除する

特定のクライアント VPN エンドポイントの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。

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. 承認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、[承認ルール] を選択します。
4. 削除する承認ルールを選択してから、[承認ルールの削除] を選択し、[承認ルールの削除] を再度選択して削除を確認します。

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。

AWS Client VPN 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。

AWS Client VPN クライアント証明書失効リスト

クライアントVPNクライアント証明書失効リストは、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ために使用されます。失効リストを生成したり、既存のリストをインポートしたり、現在のリストを失効リストファイルをエクスポートしたりできます。リストの生成は、Linux/macOS または Windows で OpenVPN ソフトウェアを使用して実行されま

す。インポートとエクスポートは、Amazon VPCコンソールまたは を使用して実行できます AWS CLI。

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、「での相互認証 AWS Client VPN」を参照してください。

> **Note**
>
> 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。新しいものを作成し、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。

クライアント証明書失効リストに追加できるエントリの数は限られています。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。

タスク

- AWS Client VPN クライアント証明書失効リストの生成
- AWS Client VPN クライアント証明書失効リストのインポート
- AWS Client VPN クライアント証明書失効リストのエクスポート

AWS Client VPN クライアント証明書失効リストの生成

Linux/macOS または Windows オペレーティングシステムでクライアント VPN 証明書失効リストを生成できます。失効リストを使用して、特定の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。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」を参照してください。

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 を入力します。

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 シェルを起動します。

```
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 を入力します。
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
```

AWS Client VPN 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、「AWS Client VPN 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
```

AWS Client VPN クライアント証明書失効リストのエクスポート

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

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。

AWS Client VPN クライアント接続

AWS Client VPN 接続は、クライアントによって特定のクライアントVPNエンドポイントに確立されたアクティブなVPNセッションと、そのエンドポイントで過去 60 分以内に終了した接続です。接続は、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すると確立されます。セッションを終了すると、クライアントVPNエンドポイントへのクライアント接続が終了します。

クライアントVPN接続を表示および終了できます。接続情報を表示すると、クライアントCIDRブロック範囲から割り当てられた IP アドレス、エンドポイント ID、タイムスタンプなどの情報が返されます。セッションを終了すると、エンドポイントへの指定されたVPN接続が終了します。セッションの表示と終了は、Amazon VPCコンソールまたは を使用して行うことができます AWS CLI。エンドポイントに接続できない場合、問題を解決するための手順については、エラーに応じて「トラブルシューティング」を参照してください。

タスク

- AWS Client VPN クライアント接続の表示
- AWS Client VPN クライアント接続を終了する

AWS Client VPN クライアント接続の表示

アクティブなクライアント VPN 接続は、Amazon VPC コンソールまたは AWS CLI を使用して表示できます。

クライアント VPN 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 VPN 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。

AWS Client VPN クライアント接続を終了する

Amazon VPC コンソールまたは AWS CLI を使用して、クライアント VPN クライアント接続を終了できます。

クライアント VPN 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、[接続] を選択します。
4. 終了する接続を選択し、[接続の終了] を選択し、[接続の終了] を再度選択して終了を確認します。

クライアント VPN 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。

AWS Client VPN クライアントログインバナー

AWS Client VPN には、VPNセッションの確立時に、 AWS 提供されたクライアント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があります。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 1400UTF ~ 8 個のエンコード文字を使用できます。

> **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セッションにのみ表示されます。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たときにバナーが表示されます。

バナーの作成

ログインバナーは、クライアントVPNエンドポイントの作成時に最初に作成され、有効になります。クライアント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手順については、「」を参照してくださいAWS Client VPN エンドポイントを作成する。

タスク

- 既存の AWS 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 AWS Client 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 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
- 現在設定されている AWS Client VPN ログインバナーを表示する

既存の AWS 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 AWS Client 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。

AWS 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 VPN 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 AWS Client VPN ログインバナーを表示する

現在設定されているクライアント VPN クライアント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。

AWS Client VPN エンドポイント

すべての AWS Client VPN セッションは、クライアントVPNエンドポイントとの通信を確立します。クライアントVPNエンドポイントを管理して、そのエンドポイントでクライアントVPNセッションを作成、変更、表示、削除できます。エンドポイントは、Amazon VPCコンソールまたは を使用して AWS 作成および変更できますCLI。

クライアントVPNエンドポイントを作成するための要件

> **Important**
>
> クライアントVPNエンドポイントは、目的の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 アカウントで作成する必要があります。また、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生成する必要があります。詳細については、「でのクライアント認証 AWS Client VPN」を参照してください。

作業を開始する前に、次のことを必ず実行してください。

- AWS Client VPNを使用するためのルールとベストプラクティス 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、「でのクライアント認証 AWS Client VPN」を参照してください。

エンドポイントの変更

クライアントVPNを作成したら、次のいずれか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 および 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
- 最大VPNセッション期間
- 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**
>
> 証明書失効リスト (CRL) の変更を含むクライアントVPNエンドポイントの変更は、クライアントVPNサービスがリクエストを承諾してから最大 4 時間後に有効になります。
> 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IPv4CIDR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

タスク

- AWS Client VPN エンドポイントを作成する
- AWS Client VPN エンドポイントを表示する
- AWS Client VPN エンドポイントを変更する
- AWS Client VPN エンドポイントを削除します

AWS Client VPN エンドポイントを作成する

クライアントVPNエンドポイントを作成して、クライアントが Amazon VPCコンソールまたは を使用してVPNセッションを確立できるようにします AWS CLI。

エンドポイントを作成する前に、要件を理解してください。詳細については、「the section called "クライアントVPNエンドポイントを作成するための要件"」を参照してください。

コンソールを使用してクライアントVPNエンドポイントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、クライアントVPNエンドポイントを選択し、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. クライアント にはIPv4CIDR、クライアント IP アドレスの割り当て元となる IP アドレス範囲をCIDR表記で指定します。例えば、`10.0.0.0/22` と指定します。

   > **Note**
   >
   > アドレス範囲は、ターゲットネットワークアドレス範囲、VPC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することはできません。クライアントアドレス範囲は /22 以上で、/12 CIDRブロックサイズ以下である必要があります。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アドレス範囲を変更することはできません。

5. サーバー証明書 ARNARNには、サーバーが使用するTLS証明書の を指定します。クライアントはサーバー証明書を使用して、接続先のクライアントVPNエンドポイントを認証します。

> **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するリージョンの AWS Certificate Manager（ACM) に存在する必要があります。証明書は、 でプロビジョニングACMすることも、 にインポートすることもできますACM。

6. VPN 接続を確立するときに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。
     - フェデレーティッド認証: SAMLベースのフェデレーティッド認証の場合は、このオプションを選択します。

       SAML プロバイダー にはARN、IAMSAMLID プロバイダーARNの を指定します。

       (オプション) セルフサービスSAMLプロバイダー ARNで、該当する場合は、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 ARN IAM SAML ID プロバイダーの を指定します。 ???
   - 相互証明書認証を使用するには、相互認証を使用する を選択し、クライアント証明書ARNに、 AWS Certificate Manager () でプロビジョニングされているクライアント証明書ARNの を指定しますACM。

   > **Note**
   >
   > サーバー証明書とクライアント証明書が同じ認証局 (CA) によって発行された場合は、サーバー証明書をサーバーとクライアントの両方ARNに使用できます。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を指定ARN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) Client Connect Handler で、クライアント接続ハンドラを有効にして、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します。Client Connect Handler 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サーバー 1 の IP アドレスとDNSサーバー 2 の 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サーバー 1 の IP アドレスまたはDNSサーバー 2 の IP アドレスのいずれかで、IP アドレスを指定し、VPCDNS サーバー IP アドレスを追加します。

> **Note**
>
> クライアントがDNSサーバーにアクセス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トランスポート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 で を選択しますTCP。

> **Note**
>
> UDP 通常、 は よりも優れたパフォーマンスを提供しますTCP。クライアントVPNエンドポイントの作成後に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) エンドポイントを分割トンネルクライアントVPNエンドポイントにするには、分割トンネルを有効にするをオンにします。デフォルトでは、クライアント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VPCに関連付ける を選択します。セキュリティグループ でIDs、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 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) クライアント用のセルフサービスポータルURLを生成するには、セルフサービスポータルを有効にするをオンにします。
15. （オプション) セッションタイムアウト時間 では、使用可能なオプションから希望する最大VPNセッション期間を時間単位で選択するか、 をデフォルト 24 時間に設定します。

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。クライアントログインバナーテキストには、VPNセッションの確立時にAWS提供された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 エンコード文字のみ。最大 1400 文字。
17. 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、次の操作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 ですpending-associate。クライアントは、最初のターゲットネットワークを関連付けた後にのみクライアントVPNエンドポイントに接続できます。
- 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。
- クライアントに配信するクライアント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 提供されたクライアントまたは別のオープンVPN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にクライアントに指示します。詳細については、AWS Client VPN ユーザーガイドをご参照ください。

を使用してクライアントVPNエンドポイントを作成するには AWS CLI

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

AWS Client VPN エンドポイントを表示する

Amazon VPC 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 コマンドを使用します。

AWS Client VPN エンドポイントを変更する

Amazon VPC 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。変更できるクライアント VPN フィールドの詳細については、「the section called “エンドポイントの変更”」を参照してください。

> **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 log group name] (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 log stream name] (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します。または、このオプションを空白のままにしておくと、ログストリームが自動的に作成されます。
   - 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 コマンドを使用します。

AWS Client VPN エンドポイントを削除します

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 コマンドを使用します。

AWS Client VPN 接続ログ

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。接続ログには、クライアントVPNエンドポイントのログイベントのシーケンスが表示されます。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サービスはログストリームを作成します。次に、接続ログは、クライアント接続リクエスト、クライアント接続結果 (成功または失敗)、接続結果に失敗した理由、エンドポイントからのクライアント終了時間を記録します。

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 Logs ユーザーガイド」の「ロググループとログストリームの使用 CloudWatch 」を参照してください。 CloudWatch ログ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」を参照してください。

クライアントVPN接続ログは、Amazon VPCコンソールまたは AWS を使用して作成できますCLI。

タスク

- 新しい AWS Client VPN エンドポイントの接続ログを有効にする
- 既存の AWS Client VPN エンドポイントの接続ログを有効にする
- AWS Client VPN 接続ログの表示
- AWS Client VPN の接続ログを停止する

新しい AWS Client 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、「AWS Client 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 AWS Client 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"
}
```

AWS Client VPN 接続ログの表示

CloudWatch Logs コンソールを使用して、クライアント VPN 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。

AWS Client VPN の接続ログを停止する

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。

AWS Client VPN エンドポイント設定ファイルのエクスポート

AWS Client 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VPNの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、 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VPN。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、設定ファイルを自分でダウンロードできます。詳細については、「AWS Client VPN セルフサービスポータルへのアクセス」を参照してください。

クライアントVPNエンドポイントで相互認証を使用する場合は、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ダウンロードした .ovpn 設定ファイルに追加する必要があります。情報を追加すると、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、オープンVPN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 を有効にしますDNS。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せず、エンドポイントDNSの名前に ping を送信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 認証を使用していて、クライアント設定ファイルを配布した後にディレクトリで多要素認証 (MFA) を有効にする場合は、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。

タスク

- AWS Client VPN クライアント設定ファイルをエクスポートする
- AWS Client VPN クライアント証明書と相互認証のキー情報を追加する

AWS Client VPN 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 VPN 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、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
```

AWS Client VPN クライアント証明書と相互認証のキー情報を追加する

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
```

AWS Client VPN ルート

各 AWS Client VPN エンドポイントには、使用可能な送信先ネットワークルートを記述する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アクセスできるクライアントを指定するには、クライアントVPNエンドポイントルートごとに承認ルールを設定する必要があります。

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VPCと、 のルートVPCがクライアントVPNエンドポイントのルートテーブルに自動的に追加されます。ピア接続された 、オンプレミスネットワークVPCs、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) 、インターネットなどの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、ここで説明しているように、サブネットごとにルートを作成する必要がありますトラブルシューティング AWS Client VPN: ピア接続された 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。

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際の考慮事項

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と、 が確立されると、クライアントルートテーブルにあるすべてのVPNルートVPNがクライアントルートテーブルに追加されます。の確立後にルートを追加する場合は、新しいルートVPN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の数を考慮することをお勧めします。

タスク

- AWS Client VPN エンドポイントルートの作成

- AWS Client VPN エンドポイントルートの表示
- AWS Client VPN エンドポイントルートの削除

AWS Client VPN エンドポイントルートの作成

クライアント VPN エンドポイント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。

AWS Client VPN 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。

AWS Client VPN エンドポイントルートの削除

削除できるクライアント VPN ルートは、手動で追加したものに限られます。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。

AWS Client VPN ターゲットネットワーク

ターゲットネットワークは、 のサブネットですVPC。クライアントがエンドポイントに接続して接続を確立できるようにするには、 AWS Client 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VPN。

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、「クライアントのシナリオと例 VPN」を参照してください。

クライアントVPNターゲットのネットワーク要件

ターゲットネットワークを作成する場合、次のルールが適用されます。

- サブネットには、10.0.0.0/27 など、/27 ビットマスク以上の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範囲と重複することはできません。
- 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ある必要があります。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VPC時に を指定した場合、サブネットは同じ に存在する必要がありますVPC。をクライアントVPNエンドポイントVPCにまだ関連付けていない場合は、任意の の任意のサブネットを選択できますVPC。

  それ以降のすべてのサブネット関連付けは、同じ からのものである必要がありますVPC。別の からサブネットを関連付けるにはVPC、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、「AWS Client 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、関連付けられたサブネットVPCがプロビジョニングされている のローカルルートがクライアントVPNエンドポイントのルートテーブルに自動的に追加されます。

> **Note**
>
> ターゲットネットワークが関連付けられたら、アタッチされた CIDRsに追加 を追加または削除するときにVPC、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エンドポイントをターゲットネットワークから関連付け解除し、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または削除します。

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availableと、クライアントVPNエンドポイントのステータスが から pending-associate に変わり、クライアントはVPN接続を確立できます。

タスク

- ターゲットネットワークを AWS Client VPN エンドポイントに関連付ける
- AWS Client VPN の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
- AWS Client VPN 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と AWS Client 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を AWS Client VPN エンドポイントに関連付ける

Amazon VPC コンソールまたは AWS CLI を使用して、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。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前に、要件に精通してください。「ターゲットネットワークを作成するための要件」を参照してください。

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。

AWS Client VPN の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

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、「クライアントのシナリオと例 VPN」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。

AWS Client VPN 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。

ターゲットネットワークと AWS Client 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。

AWS Client VPN 最大VPNセッション期間

AWS Client VPN には、クライアントVPNエンドポイントへのクライアント接続に許可される最大時間である最大VPNセッション期間に関するいくつかのオプションが用意されています。セキュリティとコンプライアンスの要件を満たすために、最大VPNセッション期間を短く設定できます。デフォルトでは、最大VPNセッション時間は 24 時間です。セッションタイムアウトの有効期限が切れると、キャッシュされたユーザー認証情報 (Active Directory) または証明書ベースの認証 (相互認証) の場合、新しいセッションが自動的に確立されます。完全に切断して自動的に再接続しない場合は、これらのユーザーが手動で切断する必要があります。フェデレーティッド認証 (SAML) の場合、新しいセッションは自動的に確立されないため、これらのユーザーはセッションタイムアウトの有効期限が切れた後に再度認証してVPN接続を確立する必要があります。

> **Note**
>
> 最大VPNセッション期間値を現在の値から減らすと、新しく設定した期間よりも長い時間枠でエンドポイントに接続されているアクティブなVPNセッションは切断されます。

AWS 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

VPN セッションの期間は、クライアントVPNエンドポイントの作成中に設定されます。クライアントVPNエンドポイントを作成し、最大セッション期間を設定する手順AWS Client VPN エンドポイントを作成するについては、「」を参照してください。

タスク

- AWS Client VPN における現在の VPN セッションの最大継続時間を表示

- AWS Client VPN の最大セッション継続時間を変更する

AWS Client VPN における現在の VPN セッションの最大継続時間を表示

クライアント VPN における、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。

AWS Client VPN の最大セッション継続時間を変更する

既存のクライアント VPN で 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。

のセキュリティ AWS Client VPN

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、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からメリットを得られます。

セキュリティは、 AWS とお客様の間での責任共有です。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 クラウドで AWS 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 AWS を担います。 AWS また、 では、安全に使用できるサービスも提供しています。AWS コンプライアンスプログラム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者は定期的にセキュリティの有効性をテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS Client VPN、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

AWS Client VPN は Amazon VPCサービスの一部です。Amazon のセキュリティの詳細については VPC、「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 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VPN。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VPNように クライアントを設定する方法について説明します。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他の AWS のサービスの使用方法についても説明します。

トピック

- でのデータ保護 AWS Client VPN
- の Identity and Access Management AWS Client VPN
- の耐障害性 AWS Client VPN
- のインフラストラクチャセキュリティ AWS Client VPN
- のセキュリティのベストプラクティス AWS Client VPN
- IPv6 に関する考慮事項 AWS Client VPN

でのデータ保護 AWS Client VPN

責任 AWS 共有モデル、 AWS クライアント でのデータ保護に適用されますVPN。このモデルで説明されているように、 AWS はすべての 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があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。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FAQ」を参照してください。欧州におけるデータ保護の詳細については、 AWS セキュリティブログの AWS 責任共有モデルとGDPRブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。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権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 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。1TLS.2 が必要で、1.3 TLS をお勧めします。
- API とユーザーアクティビティのログ記録を でセットアップします AWS CloudTrail。 CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」の CloudTrail 「証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- 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 AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、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) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、、VPNまたは を使用してクライアントまたは他の AWS のサービス を操作する場合も同様ですAPI AWS CLI AWS SDKs。タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を 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 は、Transport Layer Security (TLS) 1.2 以降を使用して、任意の場所からの安全な接続を提供します。

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

クライアントは、クライアントVPNエンドポイントを介して VPCおよびその他のネットワークに接続できます。詳細な説明と例については、「クライアントのシナリオと例 VPN」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、 内の特定のリソースへのアクセスを制限できますVPC。ユーザーベースの認証では、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、「クライアントを使用してネットワークへのアクセスを制限する VPN」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。これは、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、VPNセッションを確立します。認証に失敗すると、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。

クライアントは、次のタイプのクライアント認証VPNを提供します。

- 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ティッド認証) (ユーザーベース)

の Identity and Access Management AWS Client VPN

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リソースの使用を承認する (アクセス許可を付与 AWS のサービス する) かを制御します。IAMは、追加料金なしで使用できる 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 で行う作業によって異なりますVPN。

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、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの クライアントVPN機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。クライアント の機能にアクセスできない場合はVPN、「」を参照してくださいAWS Client VPN ID とアクセスのトラブルシューティング。

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 へのフルアクセスがありますVPN。サービスユーザーがどのクライアントVPN機能と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。その後で、サービスユーザーのアクセス許可を変更するために、IAM 管理者にリクエストを送信する必要があります。IAM の基本概念については、このページの情報を確認します。会社がクライアント IAMで を使用する方法の詳細についてはVPN、「」を参照してくださいと AWS Client VPN の連携方法 IAM。

IAM 管理者 – IAM管理者は、クライアント 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VPN。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IAM、「」を参照してくださいAWS Client VPNのアイデンティティベースのポリシーの例。

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ロールを引き受けることで、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 認証情報は、フェデレーティッド ID の例です。フェデレーテッドアイデンティティ としてサインインする場合、管理者は以前に IAM ロールを使用して ID フェデレーションを設定しています。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、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」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、 はソフトウェア開発キット (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に署名する方法の詳細については、「 IAMユーザーガイド」のAWS API「リクエストの署名バージョン 4」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。たとえば、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS 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「 ユーザーガイド」のAWS 「 での多要素認証IAMIAM」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、アカウントのすべての AWS のサービス およびリソースへの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「ルートユーザー資格情報が必要なタスク」を参照してください。

フェデレーテ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、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

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 ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できるように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。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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 ユーザーのコレクション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、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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「 ユーザーのユースケース」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、特定のユーザーに関連付けられていません。で IAMロールを一時的に引き受けるには AWS Management Console、ユーザーから IAMロールに切り替えることができます (コンソール) 。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。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「ロールを引き受ける方法」を参照してください。

IAM ロールと一時認証情報は、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ロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) のロールを作成する」を参照してください。 IAM IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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を許可する主な方法は、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) リソースに直接ポリシーをアタッチできます。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「 でのクロスアカウントリソースアクセスIAM」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。たとえば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。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と、別のサービスで別のアクションを開始するアクションを実行できます。 FASは、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストを使用します。 FAS リクエストは、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サービスが受信し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 – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける 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「 にアクセス許可を委任するロールを作成する AWS のサービス」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、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon で実行されているアプリケーション EC2 – 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認証情報を取得することができます。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与する」を参照してください。 IAM

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、ID AWS またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、そのアクセス許可を定義します。 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) 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「ポリシーの概要」を参照してください。

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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アクセス許可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。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションのアクセス許可を定義します。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 からロール情報を取得できます API。

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のポリシーは、 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アクセス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。ID 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「カスタマー管理ポリシーを使用してカスタムIAMアクセス許可を定義する」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。管理ポリシーまたはインラインポリシーを選択する方法については、「 IAMユーザーガイド」の「管理ポリシーとインラインポリシーの選択」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、リソースにアタッチするJSONポリシードキュメントです。リソースベースポリシーの例としては、IAMロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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コントロールできます。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IAMでは、 から AWS 管理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 (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。 ACLsは、ポリシードキュメント形式を使用しませんが、リソースベースのJSONポリシーに似ています。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、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がIAMエンティティ (IAM ユーザーまたはロール) に付与できるアクセス許可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) の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、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。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 (SCPs) をアカウントの一部またはすべてに適用できます。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SCPを制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCPs) – 所有する各リソースにアタッチされたJSONポリシーを更新することなく、アカウント内のリソースに使用可能なアクセス許可の上限を設定するために使用できるIAMポリシーRCPsです。は、メンバーアカウントのリソースのアクセス許可RCPを制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。をサポートする のリストRCPsを含む Organizations と の詳細についてはRCPs、AWS Organizations 「 ユーザーガイド AWS のサービス 」の「リソースコントロールポリシー (RCPs) 」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係する場合に が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「ポリシーの評価ロジック」を参照してください。

と AWS Client VPN の連携方法 IAM

IAM を使用してクライアント へのアクセスを管理する前にVPN、クライアント で使用できるIAM機能を確認してくださいVPN。

IAM AWS クライアントで使用できる の機能 VPN

IAM 機能	クライアントVPNサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
ACLs	いいえ
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	はい
プリンシパル権限	はい

IAM 機能	クライアントVPNサポート
サービスロール	はい
サービスリンクロール	あり

クライアントのアイデンティティベースのポリシー VPN

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースのポリシーは、 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アクセス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「カスタマー管理ポリシーを使用してカスタムIAMアクセス許可を定義する」を参照してください。

IAM の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、またアクションが許可または拒否され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「 IAMJSONポリシー要素リファレンス」を参照してください。

クライアントのアイデンティティベースのポリシーの例 VPN

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、「」を参照してくださいAWS Client VPNのアイデンティティベースのポリシーの例。

クライアント内のリソースベースのポリシー VPN

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースポリシーの例としては、IAMロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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コントロールできます。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、全体のアカウント、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場合 AWS アカウント、信頼されたアカウントのIAM管理者は、リソースへのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。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「 でのクロスアカウントリソースアクセスIAM」を参照してください。

クライアントのポリシーアクション VPN

ポリシーアクションのサポート:あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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`要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス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、「サービス認可リファレンス」のAWS 「 クライアントで定義されるアクションVPN」を参照してください。

クライアントのポリシーアクションは、アクションの前に次のプレフィックスVPN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、「」を参照してくださいAWS Client VPNのアイデンティティベースのポリシーの例。

クライアントのポリシーリソース VPN

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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 のリストを確認するにはARNs、「サービス認可リファレンス」のAWS 「 クライアントで定義されるリソースVPN」を参照してください。各リソースARNのを指定できるアクションについては、AWS 「クライアント で定義されるアクションVPN」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、「」を参照してくださいAWS Client VPNのアイデンティティベースのポリシーの例。

クライアントのポリシー条件キー VPN

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、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、どのリソースに対してどのような条件下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して、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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では 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。たとえば、IAM ユーザー名でタグ付けされている場合のみ、リソースにアクセスする IAM ユーザーアクセス許可を付与できます。詳細については、IAMユーザーガイドの「 IAMポリシーエレメント: 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ています。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、「サービス認可リファレンス」の AWS 「 クライアントの条件キーVPN」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 で定義されるアクションVPN」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、「」を参照してくださいAWS Client VPNのアイデンティティベースのポリシーの例。

ACLs クライアントで VPN

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。 ACLsは、ポリシードキュメント形式を使用しませんが、リソースベースのJSONポリシーに似ています。

ABAC クライアントを使用する VPN

サポート ABAC (ポリシー内のタグ): いいえ

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可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、 の最

初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、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ありです。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。

の詳細についてはABAC、「 IAMユーザーガイド」のABAC「認可によるアクセス許可の定義」を参照してください。をセットアップする手順を含むチュートリアルを表示するにはABAC、「 IAMユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

クライアントでの一時的な認証情報の使用 VPN

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報と AWS のサービス 連携する 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 「 と連携する IAM 」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は、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (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。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ユーザーからIAM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 を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。 AWS では、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、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

クライアントのクロスサービスプリンシパル許可 VPN

転送アクセスセッションをサポート (FAS): 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と、別のサービスで別のアクションを開始するアクションを実行できます。 FASは、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストを使用します。 FAS リクエストは、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サービスが受信し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。

クライアントのサービスロール VPN

サービスロールのサポート: 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「 にアクセス許可を委任するロールを作成する AWS のサービス」を参照してください。

クライアントのサービスにリンクされたロール VPN

サービスリンクロールのサポート: あり

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アクセス許可を表示できますが、編集することはできません。

AWS Client 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、ユーザーと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 を使用してタスクを実行することはできません AWS API。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アクセス許可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。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSON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 (コンソール) 」を参照してください。

各リソースタイプの の形式などVPN、クライアント で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のARNsAWS 「 クライアントのアクション、リソース、および条件キーVPN」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- 自分の権限の表示をユーザーに許可する

ポリシーに関する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 ポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス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 を使用してアクセス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 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 を使用して送信するように指定できますSSL。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に 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IAMJSON「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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。 IAMAccess Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されてい

ます。詳細については、「 IAMユーザーガイド」のIAM「Access Analyzer を使用したポリシーの検証」を参照してください。

- 多要素認証を要求する (MFA) – 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MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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「 を使用した安全なAPIアクセスMFA」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 でのセキュリティのベストプラクティス」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザー ID にアタッチされたインラインおよび管理ポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または 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 AWS API。

```
{
    "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 Client VPN ID とアクセスのトラブルシューティング

次の情報は、クライアントと の使用時に発生する可能性がある一般的な問題の診断VPNと修正に役立ちますIAM。

トピック

- クライアントでアクションを実行する権限がない VPN
- iam を実行する権限がありません。PassRole
- 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

クライアントでアクションを実行する権限がない VPN

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、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。

次の例のエラーは、mateojacksonIAMユーザーがコンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のec2:*GetWidget*アクセス許可がない場合に発生します。

```
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 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VPN。

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、既存のロールをそのサービスに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。

次の例のエラーは、 という名前のIAMユーザーがコンソールを使用してクライアント marymajor でアクションを実行しようする場合に発生しますVPN。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 (ACLs) をサポートするサービスでは、それらのポリシーを使用して、リソースへのアクセスをユーザーに許可できます。

詳細については、以下を参照してください。

- クライアントがこれらの機能VPNをサポートしているかどうかを確認するには、「」を参照してくださいと AWS Client VPN の連携方法 IAM。
- 所有 AWS アカウント する 全体で 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 する別の 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「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」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「 でのクロスアカウントリソースアクセスIAM」を参照してください。

のサービスにリンクされたロールの使用 AWS Client VPN

AWS Client VPN は AWS Identity and Access Management 、 (IAM) 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 に直接リンクされた一意のタイプのIAMロールですVPN。サービスにリンクされたロールは、 クライアントによって事前定義VPNされており、ユーザーに代わってサービスから他の 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

- での ロールの使用 AWS Client VPN
- クライアント での接続認可に ロールを使用する VPN

での ロールの使用 AWS Client VPN

AWS Client VPN は AWS Identity and Access Management 、 (IAM) 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 に直接リンクされた一意のタイプのIAMロールですVPN。サービスにリンクされたロールは、 クライアントによって事前定義VPNされており、ユーザーに代わってサービスから他の 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と、必要なアクセス許可を手動で追加する必要がなくなるため、クライアントの設定VPNが簡単になります。クライアントは、サービスにリンクされたロールのアクセス許可VPNを定義します。特に定義されている場合を除き、クライアントのみがそのロールを引き受けVPNることができます。定義されるアクセス権限には、信頼ポリシーやアクセス権限ポリシーなどがあり、そのアクセス権限ポリシーをその他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、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、VPNリソースへのアクセス許可が誤って削除されないため、クライアントリソースが保護されます。

クライアントのサービスにリンクされたロールのアクセス許可 VPN

クライアントは、 という名前のサービスにリンクされたロールVPNを使用します。AWSServiceRoleForClientVPNこれにより、クライアントVPNは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 サービスにリンクされたロールはその引き受け時に、以下のサービスを信頼します。

- `clientvpn.amazonaws.com`

このサービスにリンクされたロールは、 マネージドポリシー C を使用しますlientVPNServiceRolePolicy。 このポリシーのアクセス許可を確認するには、「 AWS 管理ポリシーリファレンス」の「ClientVPNServiceRolePolicy」を参照してください。

クライアントのサービスにリンクされたロールを作成する VPN

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 を使用して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 AWS API、クライアントによってサービスにリンクされたロールVPNが作成されます。

このサービスリンク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、クライアントはサービスにリンクされたロールを再度VPN作成します。

クライアントのサービスにリンクされたロールを編集する VPN

クライアントVPNでは、 AWSServiceRoleForClientVPN 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。サービスリンクロールを作成した後は、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説明を編集する」を参照してください。

クライアントのサービスにリンクされたロールを削除する VPN

クライアント を使用する必要がなくなった場合はVPN、AWSServiceRoleForClientVPNサービスにリンクされた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。

IAM コンソール、CLI、または IAM IAMAPIを使用して、サービスにリンクされたロールを削除します。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 での接続認可に ロールを使用する VPN

AWS Client VPN は AWS Identity and Access Management 、 (IAM) 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 に直接リンクされた一意のタイプのIAMロールですVPN。サービスにリンクされたロールは、 クライアントによって事前定義VPNされており、ユーザーに代わってサービスから他の 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と、必要なアクセス許可を手動で追加する必要がなくなるため、クライアントの設定VPNが簡単になります。クライアントは、サービスにリンクされたロールのアクセス許可VPNを定義します。特に定義されている場合を除き、クライアントのみがそのロールを引き受けVPNることができます。定義されるアクセス権限には、信頼ポリシーやアクセス権限ポリシーなどがあり、そのアクセス権限ポリシーをその他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、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、VPNリソースへのアクセス許可が誤って削除されないため、クライアントリソースが保護されます。

クライアントのサービスにリンクされたロールのアクセス許可 VPN

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

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

- `clientvpn-connections.amazonaws.com`

C という名前のロールアクセス許可ポリシーlientVPNServiceConnectionsRolePolicy はVPN、クライアントが指定されたリソースに対して次のアクションを実行することを許可します。

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

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。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アクセス許可」を参照してください。

クライアントのサービスにリンクされたロールを作成する VPN

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 を使用して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 AWS API、クライアントによってサービスにリンクされたロールVPNが作成されます。

このサービスリンク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、クライアントはサービスにリンクされたロールを再度VPN作成します。

クライアントのサービスにリンクされたロールを編集する VPN

クライアントVPNでは、 AWSServiceRoleForClientVPNConnections 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。サービスリンクロールを作成した後は、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説明を編集する」を参照してください。

クライアントのサービスにリンクされたロールを削除する VPN

クライアント を使用する必要がなくなった場合は VPN、AWSServiceRoleForClientVPNConnectionsサービスにリンクされた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。

IAM コンソール、CLI、または IAM IAMAPIを使用して、サービスにリンクされたロールを削除します。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。

の耐障害性 AWS Client VPN

AWS 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に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。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が高く、フォールトトレラントで、スケーラブルです。

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。

グローバル AWS インフラストラクチャに加えて、 はデータの耐障害性とバックアップのニーズをサポートする機能 AWS Client VPN を提供します。

高可用性対応の複数のターゲットネットワーク

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て、クライアントがVPNセッションを確立できるようにします。ターゲットネットワークは、 のサブネットですVPC。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。

のインフラストラクチャセキュリティ AWS Client VPN

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 がインフラストラクチャ AWS 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」の「インフラストラクチャの保護」を参照してください。 AWS

が AWS 公開したAPI呼び出しを使用して、ネットワークVPN経由でクライアントにアクセスします。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) 。1TLS.2 が必要で、1.3 TLS をお勧めします。
- （ エフェメラル Diffie-HellmanPFS) や DHE (エリプティック カーブ エフェメラル Diffie-Hellman) など、完全な前方秘匿性 ECDHE () を持つ暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新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の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。

のセキュリティのベストプラクティス AWS Client VPN

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べき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を説明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お客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

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、「AWS Client VPN 認可ルール」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、ユーザーが でアクセスできるリソースを制御しますVPC。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します。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、「AWS Client VPN 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、「モニタリング AWS Client VPN」を参照してください。

Identity and Access Management

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

IPv6 に関する考慮事項 AWS Client VPN

現在、クライアントVPNサービスはVPNトンネル経由の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IPv6は、 IPv4 と の両方が有効で に接続されているときに発生する可能性がありますがVPN、 VPNはIPv6トラフィックをトンネルにルーティングしません。この場合、IPv6有効な送信先に接続するときに、実際には によって提供されたIPv6アドレスに接続していることになりますISP。これにより、実際のIPv6アドレスが漏洩します。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`はローカルトンネルデバイスIPv6アドレスを に設定`fd15:53b6:dead::2`し、リモートVPNエンドポイントIPv6アドレスを に設定します`fd15:53b6:dead::1`。

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

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

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、設定は現在割り当てられているすべてのIPv6トラフィックを VPN接続にルーティングします。

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。基本的な検証では、完全なトンネル VPN接続を設定し、IPv6アドレスを使用して IPv6サーバーに ping6 を実行します。サーバーのIPv6 アドレスは、 route-ipv6 コマンドで指定された範囲内である必要があります。この ping テストは失敗します。ただし、サポートIPv6が今後クライアントVPNサービスに追加されると、これは変更され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。公開されているツールもあります。

モニタリング AWS Client VPN

モニタリングは、 およびその他の 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 AWS Client VPN です。次の機能を使用して、クライアントVPNエンドポイントのモニタリング、トラフィックパターンの分析、クライアントVPNエンドポイントの問題のトラブルシューティングを行うことができます。

Amazon CloudWatch

AWS リソースと で実行しているアプリケーションを AWS リアルタイムで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、 で Amazon EC2インスタンスのCPU使用状況やその他のメトリクス CloudWatch 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 アカウントによって、またはアカウントに代わって行われたAPI呼び出しおよび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。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。すべてのクライアントVPNアクションは によってログに記録 CloudTrail され、Amazon EC2 API リファレンスに文書化されます。

Amazon CloudWatch ログ

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。クライアント接続の接続試行とVPN接続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。 CloudWatch Logs ログストリームを指定して、接続の詳細をログに記録できます。詳細については、AWS Client VPN エンドポイントの接続ログ記録「」および「Amazon CloudWatch Logs ユーザーガイド」を参照してください。

トピック

- の Amazon CloudWatch メトリクス AWS Client VPN

の Amazon CloudWatch メトリクス AWS Client VPN

AWS Client VPN は、クライアントVPNエンドポイント CloudWatch の次のメトリクスを Amazon に発行します。メトリクスは 5 分 CloudWatch ごとに Amazon に発行されます。

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: 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: カウント
CrlDaysToExpiry	クライアントVPNエンドポイントで設定された証明書失効リスト (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: 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エンドポイントによって受信されたパケットの数。

メトリクス	説明
	単位: カウント
SelfServicePortalClientConfigurationDownloads	セルフサービスポータルからのクライアントVPNエンドポイント設定ファイルのダウンロード数。 単位: 数

AWS Client VPN は、クライアントVPNエンドポイントの以下の体制評価メトリクスを発行します。

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ためにクライアント接続ハンドラーを呼び出すときのタイムアウトの数。 単位: カウント
ClientConnectHandlerInvalidResponses	クライアントVPNエンドポイントへの接続のためにクライアント接続ハンドラーから返された無効なレスポンスの数。 単位: 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の実行中の予期しないエラーの数。 単位: カウント
ClientConnectHandlerThrottlingErrors	クライアントVPNエンドポイントへの接続のために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: カウント

メトリクス	説明
ClientConnectHandlerDeniedConnections	クライアントVPNエンドポイントへの接続について、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: カウント
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の実行中のサービス側のエラーの数。 単位: カウント

クライアントVPNエンドポイントのメトリクスをエンドポイントでフィルタリングできます。

CloudWatch では、これらのデータポイントに関する統計を、メトリクスと呼ばれる時系列データの順序付けられたセット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。例えば、指定したメトリクスをモニタリングする CloudWatch アラームを作成し、メトリクスが許容範囲外になった場合にアクション (E メールアドレスへの通知の送信など) を開始できます。

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。

タスク

- Amazon でクライアントVPNエンドポイントメトリクスを表示する CloudWatch

Amazon でクライアントVPNエンドポイントメトリクスを表示する CloudWatch

クライアントVPNエンドポイントのメトリクスは、次のように表示できます。

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. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
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. すべてのメトリクスで、クライアントVPN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。

を使用してメトリクスを表示するには AWS CLI

コマンドプロンプトで、次のコマンドを使用して、クライアントで使用できるメトリクスを一覧表示します。 VPN

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

AWS Client 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	可能
リージョンあたりのクライアントVPNエンドポイント	5	可能
クライアントVPNエンドポイントあたりの同時クライアント接続数	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	可能
クライアントVPNエンドポイントあたりの同時オペレーション数 †	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失効リストへのエントリ	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	可能

† 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 のユーザーと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、次の点を考慮してください。

- 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ティッド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、 AWS 信頼関係に IdP 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。

トラブルシューティング AWS Client VPN

以下のセクションは、クライアントVPNエンドポイントで発生する可能性のあ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 への接続に使用するオープンVPNベースのソフトウェアのトラブルシューティングの詳細についてはVPN、「 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

- トラブルシューティング AWS Client VPN: クライアント VPN エンドポイント DNS 名を解決できない
- トラブルシューティング AWS Client VPN: トラフィックがサブネット間で分割されていない
- トラブルシューティング AWS Client VPN: Active Directory グループの承認ルールが想定どおりに機能しない
- トラブルシューティング AWS Client VPN: クライアントがピア接続された VPC、Amazon S3、またはインターネットにアクセスできない
- トラブルシューティング AWS Client VPN: ピア接続された 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
- トラブルシューティング AWS Client VPN: クライアントソフトウェアは、クライアント VPN に接続しようとすると TLS エラーを返します。
- トラブルシューティング AWS Client VPN: 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
- トラブルシューティング AWS Client VPN: 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 — フェデレーション認証
- トラブルシューティング AWS Client VPN: クライアントが接続できない — 相互認証
- AWS Client VPN のトラブルシューティング: クライアントから、クライアント VPN で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
- トラブルシューティング AWS Client VPN: クライアントがエンドポイントのブラウザを開かない — フェデレーション認証
- トラブルシューティング AWS Client VPN: 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
- トラブルシューティングAWS Client VPN: IP の不一致により接続が終了する

- トラブルシューティング AWS Client VPN: LAN へのトラフィックのルーティングが期待どおりに機能しない
- トラブルシューティング AWS Client VPN: 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

トラブルシューティング AWS Client VPN: 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`

トラブルシューティング AWS Client VPN: 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。

トラブルシューティング AWS Client VPN: 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。

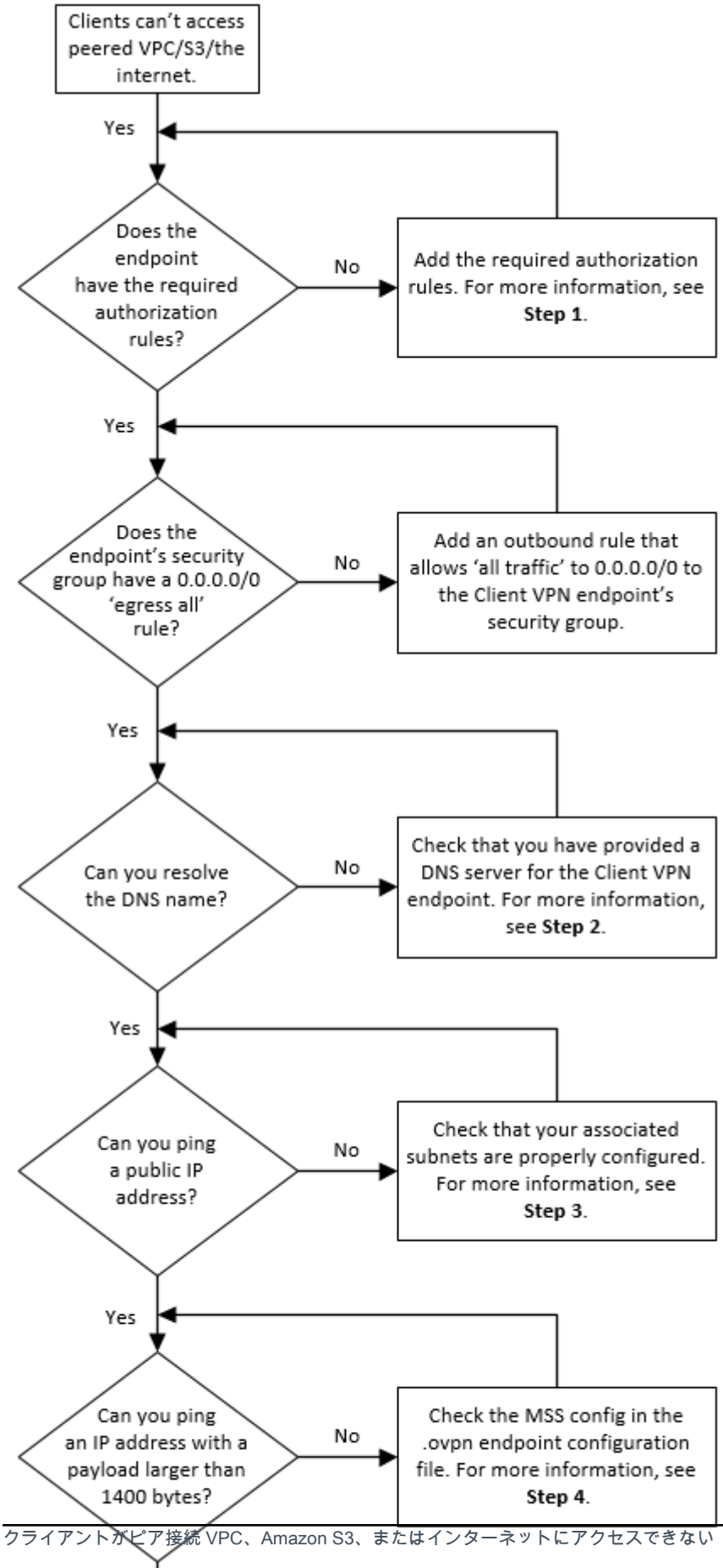
トラブルシューティング AWS Client VPN: クライアントがピア接続された VPC、Amazon S3、またはインターネットにアクセスできない

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
```

トラブルシューティング AWS Client VPN: ピア接続された 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`

トラブルシューティング AWS Client VPN: クライアントソフトウェアは、クライアント VPN に接続しようとすると TLS エラーを返します。

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、「AWS Client VPN 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 コンソールで、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、「での相互認証 AWS Client VPN」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。

トラブルシューティング AWS Client VPN: 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、「AWS Client VPN エンドポイント設定ファイルのエクスポート」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。

トラブルシューティング AWS Client VPN: 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 — フェデレーション認証

問題

フェデレーション認証を使用してユーザー名とパスワードで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。管理者に問い合わせてください」というエラーが発生する

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。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。

トラブルシューティング AWS Client VPN: 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、「AWS Client VPN エンドポイント設定ファイルのエクスポート」を参照してください。

AWS Client VPN のトラブルシューティング: クライアントから、クライアント VPN で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。

トラブルシューティング AWS Client VPN: クライアントがエンドポイントのブラウザを開かない — 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 提供のクライアントにインポートして、接続を再試行します。

トラブルシューティング AWS Client VPN: 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 提供のクライアントでは、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。

トラブルシューティングAWS Client VPN: IP の不一致により接続が終了する

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、「AWS Client VPN を使用するためのルールとベストプラクティス」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。

トラブルシューティング AWS Client VPN: LAN へのトラフィックのルーティングが期待どおりに機能しない

問題

LAN IP アドレス範囲が、標準プライベート IP アドレスである `10.0.0.0/8`、`172.16.0.0/12`、`192.168.0.0/16`、`169.254.0.0/16` の範囲内にない場合、トラフィックをローカルエリアネットワーク (LAN) にルーティングしようとすると、期待どおりに動作しません。

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、「AWS Client VPNを使用するためのルールとベストプラクティス」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、上記の標準のアドレス範囲を LAN に使用することをお勧めします。

トラブルシューティング AWS Client VPN: 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

次の表は、 AWS Client VPN 管理者ガイドの更新を示しています。

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、最大VPNセッション期間を短く設定できます。	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を満たすためにVPNセッションが確立されると、AWS が提供するクライアント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
Client-to-client access (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を有効にして、相互に接続できます。	2020 年 9 月 29 日

SAML 2.0 ベースのフェデレーション認証	2.0 SAML 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	エンドポイントを作成する AWS Client VPN ときに、VPCおよび 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ているVPNポート番号を指定できます。	2020 年 1 月 16 日
多要素認証のサポート (MFA)	Active Directory で有効MFAになっている場合、 AWS Client VPN エンドポイントは 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 エンドポイントで分割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 Client VPNを導入しています。	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。