

AWS Client VPN で作るリモート接続環境④

2020年10月15日

こんにちは。米須です。

今回は AWS Client VPN の設定について説明したいと思います。

※オンプレヘリモート接続する際は、別途オンプレと VPC をサイト間 VPN で接続が必要です。

目次

1. Client VPN エンドポイントの作成
2. サブネットの関連づけ
3. ルートの作成
4. 認証ルールの追加
5. さいごに

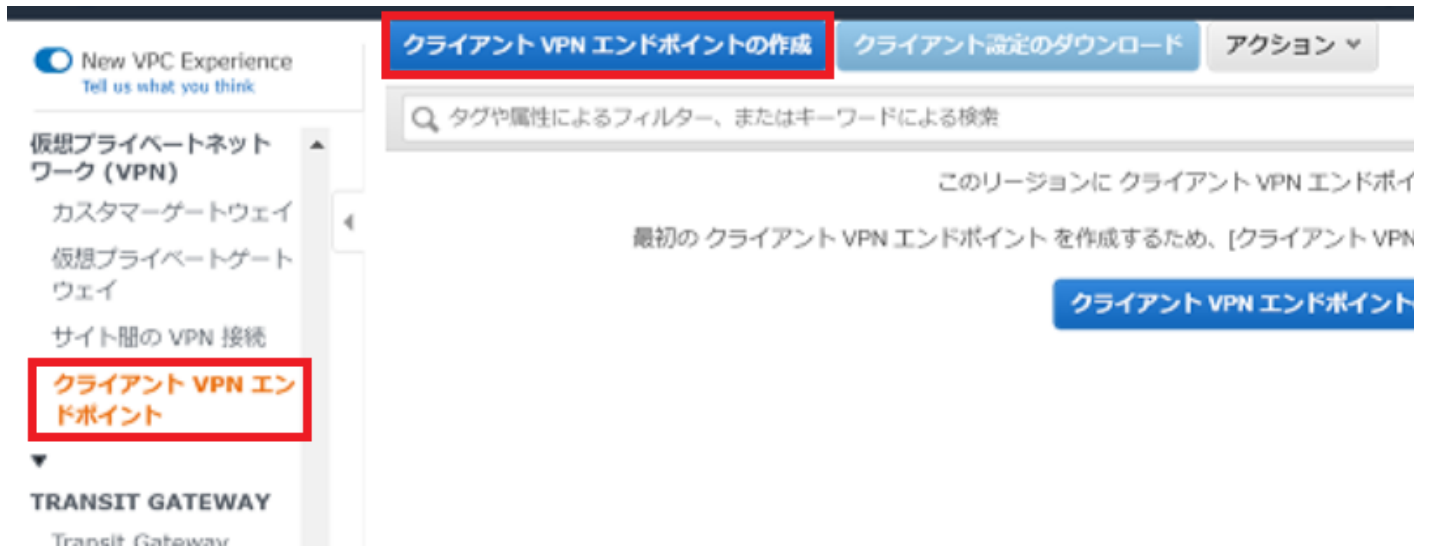
Client VPN エンドポイントの作成

[AWS ドキュメント]

クライアント VPN の操作

https://docs.aws.amazon.com/ja_jp/vpn/latest/clientvpn-admin/cvpn-working.html

VPC のメニューから「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」ボタンを押します。



次に、クライアント VPN エンドポイントの各項目について設定していきます。必要に応じて設定してください。

クライアント VPN エンドポイント > クライアント VPN エンドポイントの作成

クライアント VPN エンドポイントの作成

新しいクライアント VPN エンドポイントを作成してクライアントを有効にし、TLS VPN セッション経由でネットワークにアクセスします

名前タグ	<input type="text" value="RCM-ClientVPN-001"/>	?
説明	<input type="text" value="RCM-ClientVPN-001"/>	?
クライアント IPv4 CIDR*	<input type="text" value=""/>	?

認証情報

サーバー証明書 ARN*

認証オプション 1つ以上の認証方法を以下から選択します ?

- ☒ 相互認証の使用
- ☒ ユーザーベースの認証を使用
- ☐ Active Directory 認証

※がついている項目は、作成後の変更不可です

名前タグ	任意の値を入力します。
説明	任意の値を入力します。
クライアント IPv4 CIDR※	接続時の NAT で払い出される IP アドレスの範囲を設定します。（/16~/22が設定可）
サーバ証明書 ARN	AWS Client VPN で作るリモート接続環境② においてAWS Certificate Manager（以下、ACMとします）に登録したサーバ証明書の ARN を選択します。
認証オプション※	AWS Client VPN で作るリモート接続環境② に記載したように、認証方法を選択できます。今回は「相互認証の使用」と「ユーザベースの認証を使用」の両方にチェックを入れ、「Active Directory 認証」を選択しています。

クライアント証明書 ARN*

🔄 ⓘ

ディレクトリ ID*

d-

🔄 ⓘ

接続ログ記録

クライアント接続の詳細を記録しますか*

☒ はい ⓘ
 ☐ いいえ

CloudWatch Logs ロググループ名*

🔄 ⓘ

CloudWatch Logs ログストリーム名

🔄 ⓘ

その他のオプションパラメータ

DNS サーバー 1 IP アドレス

ⓘ

DNS サーバー 2 IP アドレス

ⓘ

トランスポートプロトコル

☐ TCP ⓘ
 ☒ UDP

※がついている項目は、作成後の変更不可です

クライアント証明書 ARN	ACM に登録したクライアント証明書の ARN を選択します。
ディレクトリ ID※	Active Directory 認証をしている場合は、ActiveDirectory（以下、AD とします）のディレクトリ ID を入力します。
接続ログ記録	ここを設定すると、CloudWatch Logs に接続ログが記録されます。
DNS サーバ 1 IP アドレス、DNS サーバ 2 IP アドレス	ClientVPN 接続後、ホスト名でRDP接続したい場合などは、ここに DNS サーバを設定します。AWS 環境とオンプレがサイト間 VPN で接続されている場合は、オンプレの DNS も設定できます。
トランスポートプロトコル※	TCP と UDP が選べますが、速度面を考慮し今回は UDP を選択しました。

スプリットトンネルを有効にする ☐ ⓘ

VPC ID ⓘ

VPN ポート ⓘ

* 必須

キャンセル

クライアント VPN エンドポイントの作成

スプリットトンネルを有効にする	<p>[チェックを外した場合]</p> <p>すべてのパケットが ClientVPN を通して AWS に流れます。VPN 接続しつつインターネットに繋がりたい場合は、インターネットGWを作成するなど AWS 側からインターネットに接続するルートを作る必要があります。</p>
	<p>[チェックをつけた場合]</p> <p>AWS 向け以外のパケットは接続元 PC から接続している別のネットワークに流れます。接続元PCがインターネットに接続できるのであれば、ここにチェックをつけるだけで VPN 接続しつつインターネットができます。</p> <p>チェックをつけておくと余計なパケットが AWS 側に流れないのでいいかなと思います。</p>

ここまで設定したら、「クライアント VPN エンドポイントの作成」を押してエンドポイントを作成しましょう。

サブネットの関連づけ

作成されたエンドポイントを選択し、サブネットを関連付けましょう。
「関連付け」タブの「関連付け」ボタンを押します。

クライアント VPN エンドポイントの作成

クライアント設定のダウンロード

アクション

タグや属性によるフィルター、またはキーワードによる検索

<input type="checkbox"/>	Name	エンドポイント	状態	クライアント
<input checked="" type="checkbox"/>		cvpn-endp...	保留中 - 関連付け	

クライアント VPN エンドポイント: cvpn-endpoint-

概要

関連付け

セキュリティグループ

認証

ルートテーブル

接続

タグ

関連付け

関連付けの解除

属性によるフィルター、またはキーワードによる検索

<input type="checkbox"/>	関連 ID	ネットワーク ID	説明	エンドポイント ID	状態	セキュリティグループ
--------------------------	-------	-----------	----	------------	----	------------

このリージョンに クライアント VPN ターゲットネットワーク はありません。

ClientVPN と関連付ける VPC とサブネットを選択し、「関連付け」ボタンを押します。

クライアント VPN エンドポイント > ターゲットネットワークへのクライアント VPN の関連付けの作成

ターゲットネットワークへのクライアント VPN の関連付けの作成

ターゲットネットワークは VPC 内のサブネットです。アベイラビリティゾーン内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。アベイラビリティゾーンごとに 1 つのサブネットを関連付けできます。アベイラビリティゾーンごとにサブネットを関連付けできます。1 つの VPC 内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できます。

クライアント VPN エンドポイント cvpn-endpoint-

VPC*

関連付けるサブネットの選択*

* 必須

キャンセル

関連付け

ボタンを押した直後は、黄色のアイコンと「関連付け中」と表示されますが、しばらくすると緑のアイコンで「関連付け済み」に変わります。なお、サブネットを関連付けたところからが費用発生となり、関連付けているサブネットの数が増えると費用も増えます。

クライアント VPN エンドポイントの作成 クライアント設定のダウンロード アクション ▾

🔍 タグや属性によるフィルター、またはキーワードによる検索

<input type="checkbox"/>	Name	エンドポイント	状態	クライアント
<input checked="" type="checkbox"/>		cvpn-endp...	● 使用可能	

クライアント VPN エンドポイント: cvpn-endpoint-

概要 **関連付け** セキュリティグループ 認証 ルートテーブル 接続 タグ

関連付け 関連付けの解除

🔍 属性によるフィルター、またはキーワードによる検索

<input type="checkbox"/>	関連 ID	ネットワーク ID	説明	エンドポイント ID	状態	セキュ
<input checked="" type="checkbox"/>	cvpn-assoc-	subnet-	-	cvpn-endpoint-	● 関連付け済み	

ルートの作成

次はルートの作成です。ここで作成したルートのみが接続可能です。
「ルートテーブル」タブから「ルートの作成」ボタンを押します。

クライアント VPN エンドポイント: cvpn-endpoint-

概要 関連付け セキュリティグループ 認証 **ルートテーブル** 接続 タグ

ルートの作成 ルートの削除

🔍 属性によるフィルター、またはキーワードによる検索 < 4 中の 1 ~ 4 >

<input type="checkbox"/>	エンドポイント ID	宛先の CIDR	ターゲットサブネット	タイプ	オリジ
--------------------------	------------	----------	------------	-----	-----

ClientVPN を作成した VPC から接続したい先を設定します。

クライアント VPN エンドポイント > ルートの作成

ルートの作成

ルートを追加してトラフィックが送信先ネットワークに振り分けられる方法を指定します

クライアント VPN エンドポイント cvpn-endpoint-

ルート送信先* ⓘ

ターゲット VPC サブネット ID* ⓘ

説明 ⓘ

* 必須

キャンセル **ルートの作成**

ルート送信先	接続先の CIDR を設定します。ピアリング先の VPC にあるサブネットの CIDR や サイト間 VPN 接続されているオンプレの CIDR も設定できます。
ターゲット VPC サブネット ID	クライアント VPN エンドポイントに紐づけたサブネットを設定します。

認証ルールを追加

「認証」タブの「受信の承認」ボタンを押します。

クライアント VPN エンドポイント: cvpn-endpoint

概要 関連付け セキュリティグループ **認証** ルートテーブル 接続 タグ

受信の承認 受信の取り消し

属性によるフィルター、またはキーワードによる検索

☐ エンドポイント ID
 ☐ 説明
 ☐ グループ ID
 ☐ すべてにアクセス
 ☐ 宛先の CIDR
 ☐ 状態

各項目を設定します。私はあまり AD に詳しくないので、アクセスグループ ID に設定するためのオブジェクト SID を取得するのに少し苦労しました。。。(^^;

クライアント VPN エンドポイント > 認証ルールを追加

認証ルールを追加

ネットワークへのアクセスをクライアントに付与する認証ルールを追加します。

クライアント VPN エンドポイント cvpn-endpoint

アクセスを有効にする送信先ネットワーク

アクセスを付与する対象:

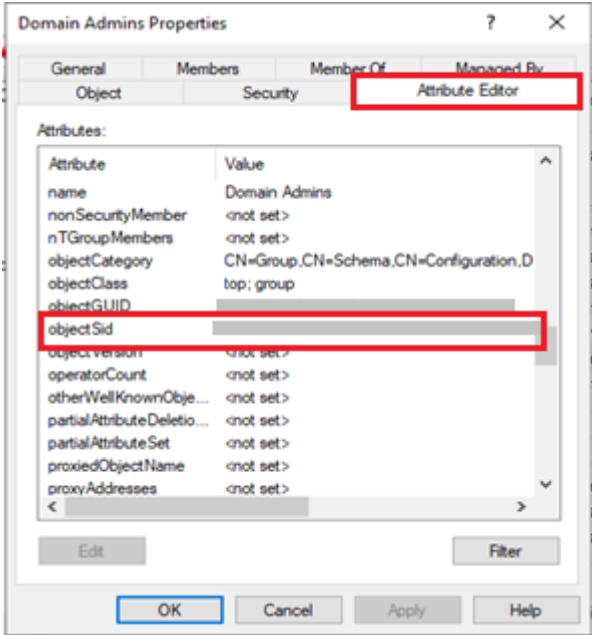
- ☐ すべてのユーザーにアクセスを許可する
- ☒ 特定のアクセスグループのユーザーへのアクセスを許可する

アクセスグループ ID

説明

* 必須

キャンセル **認証ルールを追加**

アクセスを有効にする送信先ネット	アクセスを許可する CIDR を設定します。
アクセスを付与する対象	<p>[すべてのユーザにアクセスを許可する を選択した場合] 認証OKとなったすべてのユーザが指定された指定された送信先ネットに接続することができます。</p> <p>[特定のアクセスグループのユーザへのアクセスを許可するを選択した場合] を選択した場合は、「アクセスグループ ID」にて設定したグループのみ接続が許可されます。</p>
アクセスグループ ID	<p>ADに登録されているユーザのプロパティにある「Object Sid」を設定します。</p>  <p>The screenshot shows the 'Domain Admins Properties' dialog box with the 'Attribute Editor' tab selected. The 'objectSid' attribute is highlighted with a red box. The 'Attributes' list includes: name (Domain Admins), nonSecurityMember (<not set>), nTGroupMembers (<not set>), objectCategory (CN=Group,CN=Schema,CN=Configuration,D), objectClass (top: group), objectGUID, objectSid (highlighted), objectVersion (<not set>), operatorCount (<not set>), otherWellKnownObje... (<not set>), partialAttributeDeletio... (<not set>), partialAttributeSet (<not set>), proxiedObjectName (<not set>), and proxyAddresses (<not set>).</p>