aws

Guide de l'administrateur

AWS Client VPN

AWS Client VPN: Guide de l'administrateur

Table of Contents

Qu'est-ce que AWS Client VPN ?

AWS Client VPN est un service VPN géré basé sur le client qui vous permet d'accéder en toute sécurité à vos AWS ressources et aux ressources de votre réseau local. Avec le VPN Client, vous pouvez accéder à vos ressources à partir de n'importe quel emplacement à l'aide d'un client VPN basé sur OpenVPN.

Table des matières

Caractéristiques du VPN Client

Le VPN Client offre les caractéristiques et fonctionnalités suivantes:

- Connexions sécurisées : il fournit une connexion TLS sécurisée à partir de n'importe quel emplacement à l'aide du client OpenVPN.
- Service géré : il s'agit d'un service AWS géré, qui élimine le fardeau opérationnel lié au déploiement et à la gestion d'une solution VPN d'accès à distance tierce.
- Haute disponibilité et élasticité : elle s'adapte automatiquement au nombre d'utilisateurs qui se connectent à vos AWS ressources et aux ressources sur site.
- Authentification : il prend en charge l’authentification du client avec Active Directory, l’authentification fédérée et l’authentification basée sur les certificats.
- Contrôle précis : il vous permet de mettre en œuvre des contrôles de sécurité personnalisés en définissant des règles d'accès basées sur le réseau. Ces règles peuvent être configurées avec une précision basée sur les groupes Active Directory. Vous pouvez également mettre en œuvre le contrôle d'accès à l'aide de groupes de sécurité.
- Facilité d'utilisation : il vous permet d'accéder à vos AWS ressources et aux ressources sur site à l'aide d'un seul tunnel VPN.

- Facilité de gestion : il vous permet d'afficher les journaux de connexion, qui fournissent des détails sur les tentatives de connexion client. Vous pouvez également gérer les connexions client actives, avec la possibilité d’y mettre fin.
- Intégration approfondie : il s'intègre aux AWS services existants, notamment AWS Directory Service Amazon VPC.

Composants de Client VPN

Les concepts clés liés au VPN Client sont les suivants :

Point de terminaison VPN Client

Le point de terminaison VPN Client est la ressource que vous créez et configurez pour activer et gérer des sessions VPN Client. C'est le point de terminaison pour toutes les sessions VPN client.

Réseau cible

Un réseau cible est le réseau que vous associez à un point de terminaison VPN Client. Un sous-réseau d’un VPC est un réseau cible. L’association d'un sous-réseau à un point de terminaison VPN Client vous permet d'établir des sessions VPN. Vous pouvez associer plusieurs sous-réseaux à un point de terminaison VPN Client pour bénéficier d'une haute disponibilité. Tous les sous-réseaux doivent se trouver dans le même VPC. Chaque sous-réseau doit appartenir à une zone de disponibilité différente.

Acheminement

Chaque point de terminaison du VPN client a une table de routage qui décrit la les acheminements réseau de destination disponibles. Chaque acheminement de la table de routage spécifie le chemin d'accès du trafic vers des ressources ou des réseaux spécifiques.

Règles d'autorisation

Une règle d’autorisation limite les utilisateurs qui peuvent accéder à un réseau. Pour un réseau spécifié, vous configurez le groupe Active Directory ou fournisseur d'identité (IdP) auquel l'accès est autorisé. Seuls les utilisateurs appartenant à ce groupe peuvent accéder au réseau spécifié. Par défaut, il n'y a aucune règle d'autorisation et vous devez configurer des règles d'autorisation pour permettre aux utilisateurs d'accéder aux ressources et aux réseaux.

Client

L'utilisateur final se connectant au point de terminaison VPN Client pour établir une séance VPN. Les utilisateurs finaux doivent télécharger un client OpenVPN et utiliser le fichier de configuration VPN client que vous avez créé pour établir une session VPN.

Plage CIDR du client

Plage d'adresses IP à partir de laquelle attribuer des adresses IP de clients. Chaque connexion au point de terminaison VPN Client se voit attribuer une adresse IP unique à partir de la plage CIDR du client. Vous choisissez la plage CIDR du client, par exemple, `10.2.0.0/16`.

Ports VPN client

AWS Client VPN prend en charge les ports 443 et 1194 pour TCP et UDP. La valeur par défaut est le port 443.

Interfaces réseau VPN Client

Lorsque vous associez un sous-réseau à votre point de terminaison VPN Client, nous créons des interfaces réseau VPN Client dans ce sous-réseau. Le trafic qui est envoyé au VPC à partir du point de terminaison VPN Client est envoyé via une interface réseau VPN Client. La fonction de transmission d'adresse réseau source (SNAT) est ensuite appliquée et l'adresse IP source provenant de la plage CIDR du client est convertie en adresse IP de l'interface réseau du VPN Client.

Journalisation des connexions

Vous pouvez activer la journalisation des connexions pour votre point de terminaison VPN Client afin de consigner les événements de connexion. Vous pouvez utiliser ces informations pour exécuter des analyses approfondies, analyser l'utilisation de votre point de terminaison VPN Client ou déboguer des problèmes de connexion.

Portail libre-service

Le VPN Client fournit un portail libre-service sous forme de page Web permettant aux utilisateurs finaux de télécharger la dernière version du bureau AWS VPN Client et la dernière version du fichier de configuration du point de terminaison VPN Client, qui contient les paramètres requis pour se connecter à leur point de terminaison. Votre administrateur de point de terminaison VPN Client peut activer ou désactiver un portail en libre-service pour le point de terminaison VPN Client. Le portail en libre-service est un service mondial soutenu par des ensembles de services dans les régions suivantes : USA Est (Virginie du Nord), Asie-Pacifique (Tokyo), Europe (Irlande) et AWS GovCloud (USA Ouest).

Utilisation du VPN Client

Vous pouvez utiliser le VPN Client selon l'une des méthodes suivantes :

AWS Management Console

La console fournit une interface utilisateur Web pour Client VPN. Si vous vous êtes inscrit à un Compte AWS, vous pouvez vous connecter à la console Amazon VPC et sélectionner Client VPN dans le volet de navigation.

AWS Command Line Interface (AWS CLI)

AWS CLI Fournit un accès direct aux API publiques du Client VPN. Elle est prise en charge sur Windows, macOS et Linux. Pour plus d'informations sur la prise en main du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur. Pour plus d'informations sur les commandes pour le VPN Client, consultez la Référence de l'AWS CLI.

AWS Tools for Windows PowerShell

AWS fournit des commandes pour un large éventail d' AWS offres destinées à ceux qui écrivent des scripts dans l'PowerShell environnement. Pour plus d'informations sur le démarrage avec les AWS Tools for Windows PowerShell, consultez le Guide de l’utilisateur AWS Tools for Windows PowerShell. Pour plus d'informations sur les cmdlets pour le VPN Client, consultez la AWS Tools for Windows PowerShell Référence des cmdlet .

API de requête

L'API de requête HTTPS du Client VPN vous donne un accès programmatique au VPN client et AWS. L'API de requête HTTPS vous permet d'envoyer des demandes HTTPS directement au service. Lorsque vous utilisez l'API HTTPS, vous devez inclure un code pour signer numériquement les demandes à l'aide de vos informations d'identification. Pour plus d'informations, consultez les actions AWS Client VPN.

Tarification du VPN Client

Chaque association de points de terminaison et chaque connexion VPN vous sont facturés toutes les heures. Pour en savoir plus, consultez AWS Client VPN Tarification.

Le transfert de données depuis Amazon EC2 vers l'Internet vous est facturé. Pour plus d'informations, consultez Transfert de données sur la page Tarification à la demande d'Amazon EC2.

Si vous activez la journalisation des connexions pour le point de terminaison de votre Client VPN, vous devez créer un groupe de CloudWatch journaux journaux dans votre compte. Des frais s'appliquent pour l'utilisation de groupes de journaux. Pour plus d'informations, consultez CloudWatch les tarifs Amazon (sous Niveau payant, choisissez Logs).

Si vous activez e gestionnaire de connexion client pour votre point de terminaison VPN Client, vous devez créer et appeler une fonction de type Lambda. Des frais s'appliquent pour l'appel des fonctions de type Lambda. Pour en savoir plus, consultez AWS Lambda Tarification.

Les points de terminaison VPN du Client sont associés à un réseau cible, qui est un sous-réseau d'un VPC. Si ce VPC possède une passerelle Internet, nous associons les adresses IP élastiques aux interfaces réseau élastiques (ENI) du VPN client. Ces adresses IP Elastic sont facturées en tant qu'adresses IPv4 publiques en cours d'utilisation. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique sur la page de tarification des VPC.

Règles et bonnes pratiques de AWS Client VPN

Voici les règles et les meilleures pratiques pour AWS Client VPN

- Une bande passante minimale de 10 Mbits/s est prise en charge par connexion utilisateur. La bande passante maximale par connexion utilisateur dépend du nombre de connexions établies avec le point de terminaison VPN du Client.
- Les plages CIDR client ne peuvent pas chevaucher la CIDR locale du VPC dans lequel se trouve le sous-réseau associé ou n'importe quelle route ajoutée manuellement à la table de routage du point de terminaison VPN Client.
- Les plages CIDR client doivent avoir une taille de bloc d'au moins /22 et ne doivent pas être supérieures à /12.
- Un certain nombre d'adresses de la plage CIDR client sont utilisées pour prendre en charge le modèle de disponibilité du point de terminaison VPN Client et ne peuvent pas être affectées aux clients. Par conséquent, nous vous recommandons d'affecter un bloc d'adresse CIDR contenant deux fois le nombre d'adresses IP requises pour activer le nombre maximal de connexions simultanées que vous prévoyez de prendre en charge sur le point de terminaison VPN Client.
- La plage CIDR client ne peut pas être modifiée après la création du point de terminaison VPN Client.
- Les sous-réseaux associés à un point de terminaison VPN Client doivent se trouver dans le même VPC.

- Vous ne pouvez pas associer plusieurs sous-réseaux de la même zone de disponibilité à un point de terminaison VPN Client.
- Un point de terminaison VPN Client ne prend pas en charge les associations de sous-réseaux dans un VPC de location dédiée.
- Le VPN Client prend uniquement en charge le trafic IPv4. Voir Considérations relatives à IPv6 pour AWS Client VPN pour en savoir plus sur IPv6.
- Le VPN Client n' est pas conforme aux normes fédérales de traitement de l'information (FIPS).
- Le portail libre-service n'est pas disponible pour les clients qui s'authentifient à l'aide d'une authentification mutuelle.
- Nous ne recommandons pas de se connecter à un point de terminaison Client VPN à l'aide d'adresses IP. Puisque Client VPN est un service géré, vous constaterez que les adresses IP que le nom DNS résout peuvent parfois changer. En outre, les interfaces réseau du Client VPN seront supprimées et recréées dans vos CloudTrail journaux. Nous recommandons de se connecter au point de terminaison Client VPN en utilisant le nom DNS fourni.
- Le transfert IP n'est actuellement pas pris en charge lors de l'utilisation de l'application AWS Client VPN de bureau. Le transfert IP est pris en charge par d'autres clients.
- Client VPN ne prend pas en charge la réplication multi-régions dans AWS Managed Microsoft AD. Le point de terminaison VPN du Client doit se trouver dans la même région que la AWS Managed Microsoft AD ressource.
- Si l'authentification multi-facteur (MFA) est désactivée pour votre Active Directory, les mots de passe utilisateur ne peuvent pas utiliser le format suivant.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Vous ne pouvez pas établir de connexion VPN à partir d'un ordinateur si plusieurs utilisateurs sont connectés au système d'exploitation.
- Le service VPN du Client exige que l'adresse IP à laquelle le client est connecté corresponde à l'adresse IP à laquelle le nom DNS du point de terminaison VPN du Client correspond. En d'autres termes, si vous définissez un enregistrement DNS personnalisé pour le point de terminaison VPN du Client, puis que vous transférez le trafic vers l'adresse IP réelle vers laquelle le nom DNS du point de terminaison est résolu, cette configuration ne fonctionnera pas avec les clients récemment AWS fournis. Cette règle a été ajoutée pour atténuer une attaque IP du serveur, comme décrit ici : TunnelCrack.
- Le service Client VPN nécessite que les plages d'adresses IP du réseau local (LAN) des appareils clients se situent dans les plages d'adresses IP privées standard suivantes :

`10.0.0.0/8`,`172.16.0.0/12`,`192.168.0.0/16`, ou`169.254.0.0/16`. S'il est détecté que la plage d'adresses LAN du client se situe en dehors des plages ci-dessus, le point de terminaison VPN client transmet automatiquement la directive OpenVPN « redirect-gateway block-local » au client, forçant ainsi tout le trafic LAN à entrer dans le VPN. Par conséquent, si vous avez besoin d'un accès au réseau local pendant les connexions VPN, il est conseillé d'utiliser les plages d'adresses classiques répertoriées ci-dessus pour votre réseau local. Cette règle est appliquée pour atténuer les risques d'une attaque réseau locale, comme décrit ici : TunnelCrack.

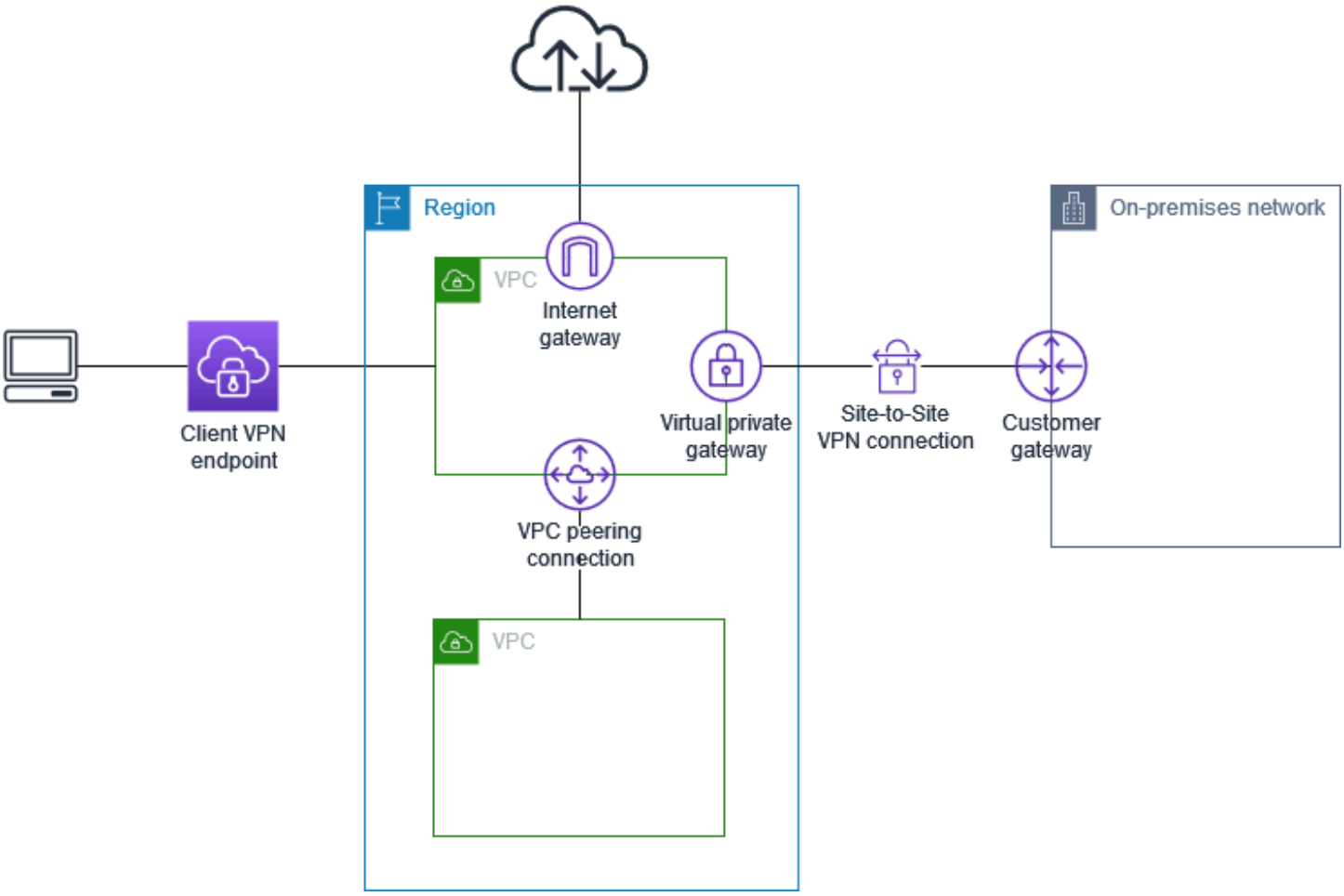
Fonctionnement du AWS VPN Client

Avec AWS le VPN Client, il existe deux types de personas utilisateurs qui interagissent avec le point de terminaison VPN Client: les administrateurs et les clients.

L'administrateur est responsable de l'installation et de la configuration du service. Cette étape implique, notamment, la création du point de terminaison du VPN Client, l'association du réseau cible, la configuration des règles d'autorisation et l'installation de routes supplémentaires (si nécessaire). Une fois que le point de terminaison VPN Client est installé et configuré, l'administrateur télécharge le fichier de configuration de point de terminaison VPN Client et le distribue aux clients qui doivent y accéder. Le fichier de configuration de point de terminaison VPN Client inclut le nom DNS du point de terminaison VPN Client et les informations d'authentification requises pour établir une session VPN. Pour plus d'informations sur la configuration du service, consultez Mise en route avec AWS Client VPN.

Le client est l'utilisateur final. Il s'agit de la personne qui se connecte au point de terminaison VPN Client pour établir une session VPN. Le client met en place la session VPN à partir de son ordinateur local ou de son appareil mobile à l'aide d'une application VPN Client basée sur OpenVPN. Après avoir établi la session VPN, il peut accéder de manière sécurisée aux ressources du VPC dans lequel le sous-réseau associé est situé. Il peut également accéder à d'autres ressources de AWS, à un réseau sur site ou à d'autres clients si l'acheminement requis et les règles d'autorisation ont été configurés. Pour plus d'informations sur la connexion à un point de terminaison VPN Client pour établir une session VPN, veuillez consulter Mise en route dans le Guide de l'utilisateur AWS VPN Client.

Le graphique suivant illustre l'architecture de base du VPN Client.



Authentification client

L'authentification du client est mise en œuvre dès le premier point d'entrée dans le AWS Cloud. Elle est utilisée pour déterminer si les clients sont autorisés à se connecter au point de terminaison VPN Client. Si l'authentification aboutit, les clients se connectent au point de terminaison VPN Client et établissent une session VPN. Si l'authentification échoue, la connexion est refusée et le client n'est pas autorisé à établir une session VPN.

Le VPN Client offre les types d'authentification client suivants:

- Authentification Active Directory (basée sur l'utilisateur)
- Authentification mutuelle (basée sur un certificat)
- Authentification unique (authentification fédérée basée sur SAML) (basée sur l'utilisateur)

Vous pouvez utiliser l'une des méthodes énumérées ci-dessus ou une combinaison d'authentification mutuelle avec une méthode basée sur l'utilisateur, telle que la suivante :

- Authentification mutuelle et authentification fédérée
- Authentification mutuelle et authentification Active Directory

> **Important**
>
> Pour créer un point de terminaison Client VPN, vous devez fournir un certificat de serveur AWS Certificate Manager, quel que soit le type d'authentification que vous utilisez. Pour plus d'informations sur la création et le provisionnement d'un certificat de serveur, consultez les étapes de la section dans Authentification mutuelle.

Authentification Active Directory

Client VPN fournit un support Active Directory en s'intégrant à AWS Directory Service. Avec l'authentification Active Directory, les clients sont authentifiés par rapport aux groupes Active Directory existants. Grâce à AWS Directory Service cela, le Client VPN peut se connecter à des Active Directory existants approvisionnés dans AWS ou dans votre réseau local. Cette option vous permet d'utiliser votre infrastructure d'authentification client existante. Si vous utilisez un Active Directory local et que vous ne possédez pas de Microsoft AD AWS géré existant, vous devez configurer un connecteur Active Directory (AD Connector). Vous pouvez utiliser un serveur Active Directory pour authentifier les utilisateurs. Pour plus d'informations sur l'intégration d'Active Directory, consultez le AWS Directory Service Guide de l'administrateur.

Le VPN Client prend en charge l'authentification multi-facteur (MFA) lorsqu'elle est activée pour AWS Microsoft AD administré ou le connecteur AD Connector. Si la fonction MFA est activée, les clients doivent entrer un nom d'utilisateur, un mot de passe et un code MFA lorsqu'ils se connectent à un point de terminaison VPN Client. Pour plus d'informations sur l'activation de l'authentification MFA, veuillez consulter Activer l'authentification multi-facteurs pour AWS Microsoft AD administré et Activer l'authentification multi-facteurs pour AD Connector dans le Guide de l'administrateur AWS Directory Service .

Pour connaître les quotas et les règles de configuration des utilisateurs et des groupes dans Active Directory, consultez Quotas d'utilisateurs et de groupes.

Authentification mutuelle

Avec l'authentification mutuelle, le VPN Client utilise des certificats pour procéder à l'authentification entre le client et le serveur. Les certificats constituent une forme numérique d'identification émise par une autorité de certification (AC). Le serveur utilise des certificats de client pour authentifier les clients lorsque ces derniers essaient de se connecter au point de terminaison VPN Client. Vous devez créer un certificat et une clé de serveur, et au moins un certificat client et une clé.

Vous devez télécharger le certificat de serveur sur AWS Certificate Manager (ACM) et le spécifier lorsque vous créez un point de terminaison Client VPN. Lorsque vous chargez le certificat du serveur sur ACM, vous spécifiez également l'autorité de certification (AC). Vous n'avez besoin de charger le certificat du client vers ACM que lorsque l'autorité de certification du certificat client est différente de celle du certificat serveur. Pour plus d'informations sur ACM, consultez le Guide de l'utilisateur AWS Certificate Manager.

Vous pouvez créer un certificat client distinct et une clé pour chaque client qui se connectera au point de terminaison VPN Client. Cette étape vous permet de révoquer un certificat client spécifique si un utilisateur quitte votre organisation. Dans ce cas, lorsque vous créez le point de terminaison VPN Client, vous pouvez spécifier l'ARN du certificat de serveur pour le certificat client, à condition que le certificat client ait été émis par la même autorité de certification que le certificat de serveur.

> **Note**
>
> Un point de terminaison VPN Client prend en charge uniquement les tailles de clés RSA 1024-bits et 2048-bits. De plus, le certificat client doit comporter l'attribut CN dans le champ Objet.
> Lorsque les certificats utilisés par le service VPN Client sont mis à jour, soit par une rotation automatique ACM, soit par une importation manuelle d'un nouveau certificat, soit par des mises à jour des métadonnées dans IAM Identity Center, le service VPN Client met automatiquement à jour le point de terminaison VPN Client avec le certificat le plus récent. Ce processus automatique peut prendre jusqu'à 24 heures.

Linux/macOS

La procédure suivante utilise easy-rsa OpenVPN pour générer les certificats et les clés du serveur et du client, puis charge le certificat et la clé de serveur dans ACM. Pour plus d'informations, consultez le document Easy-RSA 3 Quickstart README.

Pour générer les certificats et les clés de serveur et de client et les charger dans ACM

1. Clonez le référentiel OpenVPN easy-rsa sur votre ordinateur individuel et accédez au dossier `easy-rsa/easyrsa3`.

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

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

2. Initialisez un nouvel environnement PKI (infrastructure à clés publiques).

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

3. Pour créer une nouvelle autorité de certification, exécutez cette commande et suivez les invites.

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

4. Générez le certificat et la clé du serveur.

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

5. Générez le certificat et la clé du client.

   Assurez-vous de conserver le certificat du client et la clé privée du client, car vous en aurez besoin pour configurer le client.

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

   Vous pouvez facultativement répéter cette étape pour chaque client (utilisateur final) qui nécessite un certificat et une clé client.

6. Copiez le certificat et la clé du serveur ainsi que le certificat et la clé du client dans un dossier personnalisé, puis accédez au dossier personnalisé.

   Avant de copier les certificats et les clés, créez le dossier personnalisé à l'aide de `mkdir` la commande . L'exemple suivant crée un dossier personnalisé dans votre répertoire personnel.

   ```
   $ 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. Chargez le certificat et la clé du serveur ainsi que le certificat et la clé client vers ACM. Veillez à les charger dans la même région que celle dans laquelle vous prévoyez de créer le point de terminaison VPN Client. Les commandes suivantes utilisent AWS CLI pour charger les certificats. Pour charger les certificats à l'aide de la console ACM, consultez Importer un certificat dans le AWS Certificate Manager Guide de l'utilisateur .

```
$ 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
```

Vous n'avez pas nécessairement besoin de charger le certificat client sur ACM. Si les certificats du serveur et du client ont été émis par la même autorité de certification (AC), vous pouvez utiliser l'ARN du certificat du serveur pour le serveur et le client lorsque vous créez le point de terminaison VPN Client. Dans les étapes ci-dessus, la même autorité de certification a été utilisée pour créer les deux certificats. Toutefois, les étapes de téléchargement du certificat client sont incluses pour des fins d'exhaustivité.

Windows

La procédure suivante installe le logiciel Easy-RSA 3.x, puis l'utilise pour générer les certificats et clés du serveur et du client.

Pour générer les certificats et les clés de serveur et de client et les charger dans ACM

1. Ouvrez la page des versions EasyRSA, téléchargez le fichier ZIP correspondant à votre version de Windows et procédez à son extraction.
2. Ouvrez une invite de commande et accédez à l'emplacement dans lequel le dossier `EasyRSA-3.x` a été extrait.
3. Exécutez la commande suivante pour ouvrir le shell EasyRSA 3.

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

4. Initialisez un nouvel environnement PKI (infrastructure à clés publiques).

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

5. Pour créer une nouvelle autorité de certification, exécutez cette commande et suivez les invites.

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

6. Générez le certificat et la clé du serveur.

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

7. Générez le certificat et la clé du client.

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

   Vous pouvez facultativement répéter cette étape pour chaque client (utilisateur final) qui nécessite un certificat client et une clé.

8. Quittez le shell EasyRSA 3.

```
# exit
```

9. Copiez le certificat et la clé du serveur ainsi que le certificat et la clé du client dans un dossier personnalisé, puis accédez au dossier personnalisé.

   Avant de copier les certificats et les clés, créez le dossier personnalisé à l'aide de la commande `mkdir`. L'exemple suivant crée un dossier personnalisé sur votre unité C:\.

```
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. Chargez le certificat et la clé du serveur ainsi que le certificat et la clé du client vers ACM. Veillez à les charger dans la même région que celle dans laquelle vous prévoyez de créer le point de terminaison VPN Client. Les commandes suivantes utilisent le AWS CLI pour télécharger les certificats. Pour charger les certificats à l'aide de la console ACM, consultez Importer un certificat dans le AWS Certificate Manager Guide de l'utilisateur .

```
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
```

Vous n'avez pas nécessairement besoin de charger le certificat client sur ACM. Si les certificats du serveur et du client ont été émis par la même autorité de certification (AC), vous pouvez utiliser l'ARN du certificat du serveur pour le serveur et le client lorsque vous créez le point de terminaison VPN Client. Dans les étapes ci-dessus, la même autorité de certification a été utilisée pour créer les deux certificats. Toutefois, les étapes de téléchargement du certificat client sont incluses pour des fins d'exhaustivité.

Renouvellement de votre certificat de serveur

Vous pouvez renouveler et réimporter un certificat de serveur arrivé à expiration. Selon la version d'OpenVPN easy-rsa que vous utilisez, la procédure peut varier. Consultez la documentation relative au renouvellement et à la révocation des certificats Easy-RSA 3 pour plus de détails.

Renouvelez votre certificat de serveur

1. Procédez de l'une des manières suivantes :
   - Version 3.1.x d'Easy-RSA
     - Exécutez la commande de renouvellement de certificat.

       ```
       $ ./easyrsa renew server nopass
       ```
   - Version 3.2.x d'Easy-RSA

     a. Exécutez la commande expire.

```
$ ./easyrsa expire server
```

b. Signez un nouveau certificat.

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

2. Créez un dossier personnalisé, copiez-y les nouveaux fichiers, puis accédez au dossier.

```
$ 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. Importez les nouveaux fichiers dans ACM. Veillez à les importer dans la même région que le point de terminaison VPN client.

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

Authentification unique (authentification fédérée basée sur SAML 2.0)

AWS Client VPN prend en charge la fédération d'identité avec le langage SAML 2.0 (Security Assertion Markup Language 2.0) pour les points de terminaison VPN du Client. Vous pouvez utiliser des fournisseurs d'identité (IdPs) qui prennent en charge le protocole SAML 2.0 pour créer des identités utilisateur centralisées. Vous pouvez ensuite configurer un point de terminaison VPN Client pour utiliser l'authentification fédérée basée sur SAML et l'associer à l'IdP. Les utilisateurs se connectent ensuite au point de terminaison VPN Client avec leurs informations d'identification centralisées.

Pour permettre à votre IdP basé sur SAML de fonctionner avec un point de terminaison VPN Client, procédez comme suit.

1. Créez une application basée sur SAML dans l'IdP de votre choix pour l'utiliser avec ou utiliser une AWS Client VPN application existante.
2. Configurez votre fournisseur d'identité pour établir une relation de confiance avec AWS. Pour les ressources, consultez Ressources de configuration d'un IdP basé sur SAML.

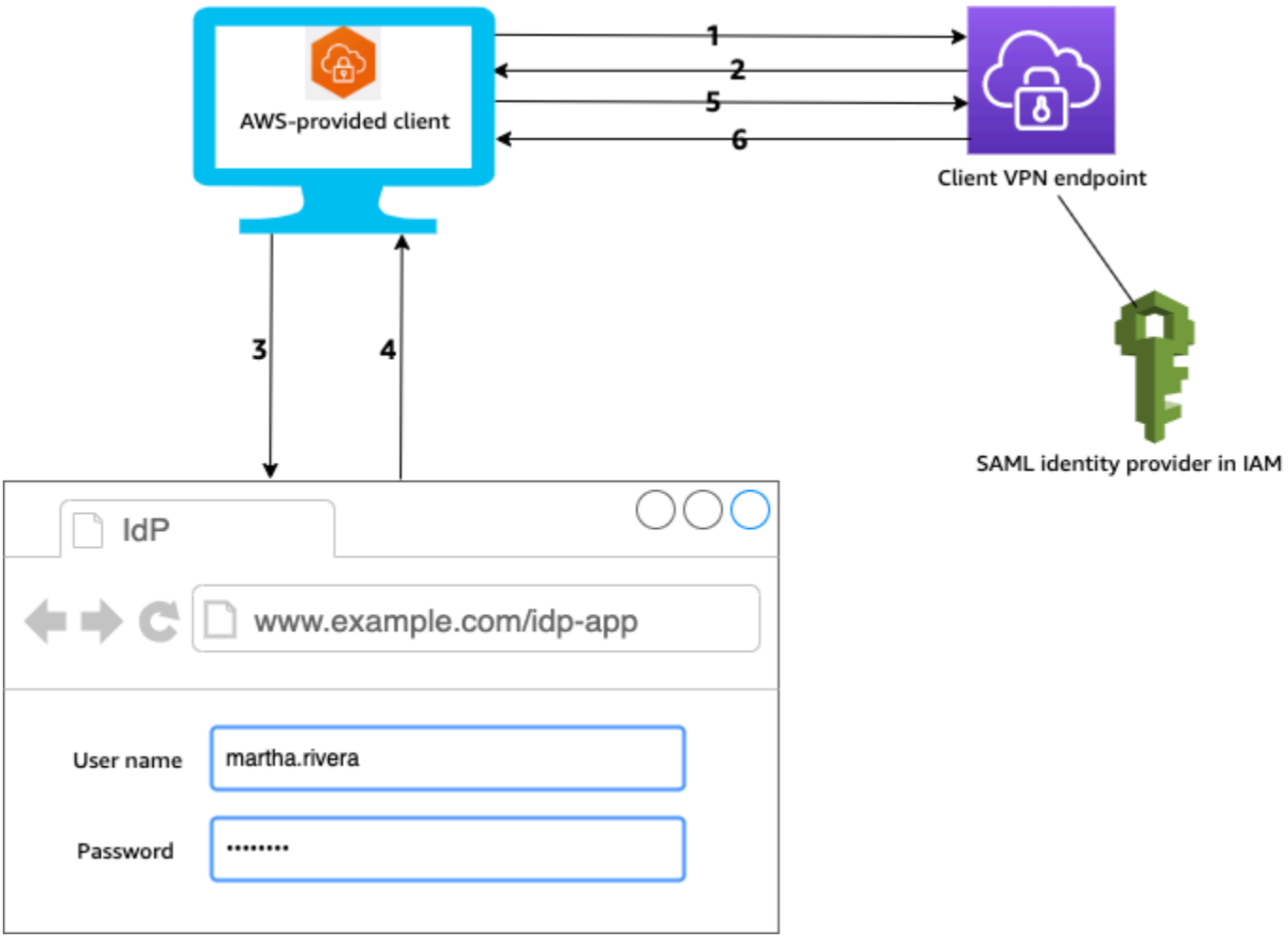
3. Dans votre fournisseur d'identité, générez et téléchargez un document de métadonnées de fédération qui décrit votre organisation en tant que fournisseur d'identité. Ce document XML signé est utilisé pour établir la relation de confiance entre AWS et l'IdP.
4. Créez un fournisseur d'identité IAM SAML sur le même AWS compte que le point de terminaison VPN du Client. Le fournisseur d'identité IAM SAML définit la relation IDP àAWS confiance de votre organisation à l'aide du document de métadonnées généré par l'IdP. Pour plus d'informations, consultez Création de fournisseurs d'identité SAML IAM dans le Guide de l'utilisateur IAM. Si vous mettez à jour ultérieurement la configuration de l'application dans le fournisseur d'identité, générez un nouveau document de métadonnées et mettez à jour votre fournisseur d'identité SAML IAM.

> **Note**
>
> Vous n'avez pas besoin de créer un rôle IAM pour utiliser le fournisseur d'identité SAML IAM.

5. Créez un point de terminaison VPN Client. Spécifiez l'authentification fédérée comme type d'authentification et spécifiez le fournisseur d'identité SAML IAM que vous avez créé. Pour plus d'informations, consultez Créer un point de terminaison VPN Client.
6. Exportez le fichier de configuration du client et distribuez-le à vos utilisateurs. Demandez à vos utilisateurs de télécharger la dernière version du client fourni AWS et de l'utiliser pour charger le fichier de configuration et se connecter au point de terminaison VPN Client. Sinon, si vous avez activé le portail en libre-service pour votre point de terminaison VPN client, demandez à vos utilisateurs d'accéder au portail en libre-service pour obtenir le fichier de configuration et AWS le client fourni. Pour plus d'informations, consultez Accéder au portail en libre-service.

Flux de travail d'authentification

Le schéma suivant fournit une vue d'ensemble du flux de travail d'authentification pour un point de terminaison VPN Client qui utilise l'authentification fédérée basée sur SAML. Lorsque vous créez et configurez le point de terminaison VPN Client, vous spécifiez le fournisseur d'identité SAML IAM.



1. L'utilisateur ouvre le client AWS fourni sur son appareil et établit une connexion avec le point de terminaison VPN du Client.
2. Le point de terminaison VPN Client renvoie une URL de fournisseur d'identité et une demande d'authentification au client, en fonction des informations fournies dans le fournisseur d'identité SAML IAM.
3. Le client AWS fourni ouvre une nouvelle fenêtre de navigateur sur l'appareil de l'utilisateur. Le navigateur fait une demande au fournisseur d'identité et affiche une page de connexion.
4. L'utilisateur saisit ses informations d'identification sur la page de connexion et le fournisseur d'identité envoie une assertion SAML signée au client.
5. Le client AWS fourni envoie l'assertion SAML au point de terminaison VPN du Client.
6. Le point de terminaison VPN Client valide l'assertion et autorise ou refuse l'accès à l'utilisateur.

Les exigences et les observations relatives à l'authentification fédérée basée sur SAML

Voici les exigences et les considérations relatives à l'authentification fédérée basée sur SAML.

- Pour connaître les quotas et les règles de configuration des utilisateurs et des groupes dans un IdP basé sur SAML, consultez Quotas d'utilisateurs et de groupes.
- L'assertion SAML et les documents SAML doivent être signés.
- AWS Client VPN ne prend en charge que les conditions « » NotBefore et NotOnOrAfter « » dans les assertions SAML. AudienceRestriction
- La taille maximale prise en charge pour les réponses SAML est de 128 Ko.
- AWS Client VPN ne fournit pas de demandes d'authentification signées.
- La déconnexion unique SAML n'est pas prise en charge. Les utilisateurs peuvent se déconnecter en se déconnectant du client AWS fourni, ou vous pouvez mettre fin aux connexions.
- Un point de terminaison VPN Client prend uniquement en charge une seule IdP.
- L'authentification multifacteur (MFA) est prise en charge lorsqu'elle est activée dans votre IdP.
- Les utilisateurs doivent utiliser le client AWS fourni pour se connecter au point de terminaison VPN du Client. Ils doivent utiliser la version 1.2.0 ou une version ultérieure. Pour plus d'informations, voir Connect à l'aide du client AWS fourni.
- Les navigateurs suivants sont pris en charge pour l'authentification IdP: Apple Safari, Google Chrome, Microsoft Edge et Mozilla Firefox.
- Le client AWS fourni réserve le port TCP 35001 sur les appareils des utilisateurs pour la réponse SAML.
- La mise à jour du document de métadonnées du fournisseur d'identité SAML IAM avec une URL erronée ou malveillante peut entraîner des problèmes d'authentification pour les utilisateurs ou des attaques de phishing. Par conséquent, nous vous recommandons d'utiliser AWS CloudTrail pour surveiller les mises à jour du fournisseur d'identité SAML IAM. Pour plus d'informations, consultez Journalisation des appels d'IAM et AWS STS avec AWS CloudTrail dans le Guide de l'utilisateur IAM.
- AWS Client VPN envoie une requête AuthN à l'IdP via une liaison de redirection HTTP. Par conséquent, l'IdP doit prendre en charge la liaison de redirection HTTP et elle doit être présente dans le document de métadonnées de l'IdP.
- Pour l'assertion SAML, vous devez utiliser un format d'adresse e-mail pour l'attribut `NameID`.

Ressources de configuration d'un IdP basé sur SAML

Le tableau suivant répertorie les solutions basées sur le protocole SAML IdPs que nous avons testées pour être utilisées AWS Client VPN, ainsi que les ressources qui peuvent vous aider à configurer l'IdP.

IdP	Ressource
Okta	Authentifier les AWS Client VPN utilisateurs avec SAML
Microsoft Azure Active Directory (Azure AD)	Pour plus d'informations, consultez Tutoriel : intégration de l'authentification unique (SSO) Azure Active Directory à AWS ClientVPN sur le site Web de documentation de Microsoft.
JumpCloud	Authentification unique (SSO) avec AWS Client VPN
AWS IAM Identity Center	Utilisation d'IAM Identity Center AWS Client VPN pour l'authentification et l'autorisation

Informations sur le fournisseur de services pour la création d'une application

Pour créer une application basée sur SAML à l'aide d'un IdP qui n'est pas répertorié dans le tableau précédent, utilisez les informations suivantes pour configurer les informations du AWS Client VPN fournisseur de services.

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

Au moins un attribut doit être inclus dans la réponse SAML de l'IdP. Voici quelques exemples d'attributs.

Attribut	Description
`FirstName`	Le prénom de l'utilisateur.

Attribut	Description
`LastName`	Le nom de famille de l'utilisateur.
`memberOf`	Le ou les groupes dont fait partie l'utilisateur.

> **Note**
>
> L'attribut `memberOf` est requis pour utiliser les règles d'autorisation basées sur des groupes Active Directory ou IdP SAML. Il est également sensible à la casse et doit être configuré exactement comme spécifié. Pour plus d'informations, consultez Autorisation basée sur le réseau et Règles d'autorisation.

Prise en charge du portail en libre-service

Si vous activez le portail en libre-service pour votre point de terminaison VPN Client, les utilisateurs se connectent au portail à l'aide de leurs informations d'identification IdP basées sur SAML.

Si votre IdP prend en charge plusieurs URL Assertion Consumer Service (ACS), ajoutez l'URL ACS suivante à votre application.

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

Si vous utilisez le point de terminaison Client VPN dans une GovCloud région, utilisez plutôt l'URL ACS suivante. Si vous utilisez la même application IDP pour vous authentifier à la fois pour la norme et pour les GovCloud régions, vous pouvez ajouter les deux URL.

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

Si votre IdP ne prend pas en charge plusieurs URL ACS, procédez comme suit :

1. Créez une application SAML supplémentaire dans votre IdP et spécifiez l'URL ACS suivante.

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

2. Générez et téléchargez un document de métadonnées de fédération.

3. Créez un fournisseur d'identité IAM SAML sur le même AWS compte que le point de terminaison VPN du Client. Pour plus d'informations, consultez Création de fournisseurs d'identité SAML IAM dans le Guide de l'utilisateur IAM.

   > **Note**
   >
   > Vous créez ce fournisseur d'identité SAML IAM en plus de celui que vous créez pour l'application principale.

4. Créez le point de terminaison VPN Client et spécifiez les deux fournisseurs d'identité SAML IAM que vous avez créés.

Autorisation client

Le VPN Client prend en charge deux types d'autorisation client : les autorisations de groupes de sécurité et les autorisations basées sur le réseau (utilisant des règles d'autorisation).

Groupes de sécurité

Lorsque vous créez un point de terminaison VPN Client, vous pouvez spécifier les groupes de sécurité d'un VPC spécifique à appliquer au point de terminaison VPN Client. Lorsque vous associez un sous-réseau à un point de terminaison VPN Client, nous appliquons automatiquement le groupe de sécurité par défaut du VPC. Vous pouvez modifier les groupes de sécurité après avoir créé le point de terminaison VPN Client. Pour plus d'informations, consultez Application d'un groupe de sécurité à un réseau cible. Les groupes de sécurité sont associés aux interfaces réseau VPN Client.

Vous pouvez autoriser les utilisateurs VPN Client à accéder à vos applications dans un VPC en ajoutant une règle aux groupes de sécurité de votre application pour autoriser le trafic à partir du groupe de sécurité qui a été appliqué à l'association.

Pour ajouter une règle qui autorise le trafic en provenance du groupe de sécurité du point de terminaison VPN Client

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes de sécurité.
3. Choisissez le groupe de sécurité associé à votre ressource ou votre application, puis choisissez Actions, Modifier les règles entrantes.
4. Choisissez Ajouter une règle.

5. Pour Type, sélectionnez Tout le trafic. Vous pouvez également restreindre l'accès à un type spécifique de trafic, par exemple SSH.

   Pour Source, spécifiez l'ID du groupe de sécurité associé au réseau cible (sous-réseau) pour le point de terminaison VPN Client.
6. Sélectionnez Enregistrer les règles.

À l'inverse, vous pouvez restreindre l'accès des utilisateurs Client VPN en ne spécifiant pas le groupe de sécurité qui a été appliqué à l'association, ou en supprimant la règle qui fait référence au groupe de sécurité du point de terminaison VPN Client. Les règles du groupe de sécurité dont vous avez besoin peuvent également dépendre du type d'accès VPN que vous souhaitez configurer. Pour plus d'informations, consultez Scénarios et exemples pour AWS Client VPN.

Pour plus d'informations sur les groupes de sécurité, consultez Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon VPC.

Autorisation basée sur le réseau

L'autorisation basée sur le réseau est mise en œuvre à l'aide de règles d'autorisation. Pour chaque réseau dont vous souhaitez activer l'accès, vous devez configurer des règles d'autorisation qui limitent les utilisateurs y ayant accès. Pour un réseau spécifié, vous configurez le groupe Active Directory ou fournisseur d'identité (IdP) basé sur SAML qui est autorisé à accéder. Seuls les utilisateurs qui appartiennent au groupe spécifié peuvent accéder au réseau spécifié. Si vous n'utilisez pas Active Directory ou l'authentification fédérée basée sur SAML, ou si vous souhaitez ouvrir l'accès à tous les utilisateurs, vous pouvez spécifier une règle qui accorde l'accès à tous les clients. Pour plus d'informations, consultez Règles d'autorisation.

Autorisation de connexion

Vous pouvez configurer un gestionnaire de connexion client pour votre point de terminaison Client VPN. Ce gestionnaire vous permet d'exécuter une logique personnalisée qui autorise une nouvelle connexion, en fonction des attributs de périphérique, d'utilisateur et de connexion. Le gestionnaire de connexion client (Client Connect Handler) s'exécute une fois que le service Client VPN a authentifié le périphérique et l'utilisateur.

Pour configurer un gestionnaire de connexion client pour votre point de terminaison Client VPN, créez une fonction AWS Lambda qui prend les attributs de périphérique, d'utilisateur et de connexion comme entrées, et renvoie la décision au service Client VPN d'autoriser ou de refuser une nouvelle

connexion. Vous spécifiez la fonction Lambda dans votre point de terminaison Client VPN. Lorsque les périphériques se connectent à votre point de terminaison Client VPN, le service Client VPN appelle la fonction Lambda en votre nom. Seules les connexions autorisées par la fonction Lambda sont autorisées à se connecter au point de terminaison Client VPN.

> **Note**
>
> Actuellement, le seul type de gestionnaire de connexion client pris en charge est une fonction Lambda.

Exigences et considérations

Voici les exigences et considérations relatives au gestionnaire de connexion client :

- Le nom de la fonction Lambda doit commencer par le préfixe `AWSClientVPN-`.
- Les fonctions Lambda qualifiées sont prises en charge.
- La fonction Lambda doit se trouver dans la même AWS région et sur le même AWS compte que le point de terminaison VPN du Client.
- La fonction Lambda expire après 30 secondes. Cette valeur ne peut pas être modifiée.
- La fonction Lambda est appelée de manière synchrone. Elle est appelée après l'authentification du périphérique et de l'utilisateur, et avant l'évaluation des règles d'autorisation.
- Si la fonction Lambda est appelée pour une nouvelle connexion et que le service Client VPN n'obtient pas de réponse attendue de la fonction, le service Client VPN refuse la demande de connexion. Par exemple, ceci peut se produire si la fonction Lambda est limitée, expire ou rencontre d'autres erreurs inattendues, ou si la réponse de la fonction n'est pas dans un format valide.
- Nous vous recommandons de configurer la simultanéité allouée pour la fonction Lambda afin qu'elle puisse être mise à l'échelle sans fluctuations de latence.
- Si vous mettez à jour votre fonction Lambda, les connexions existantes au point de terminaison Client VPN ne sont pas affectées. Vous pouvez résilier les connexions existantes, puis demander à vos clients d'établir de nouvelles connexions. Pour plus d’informations, consultez Mettre fin à une connexion client.
- Si les clients utilisent le client AWS fourni pour se connecter au point de terminaison VPN du Client, ils doivent utiliser la version 1.2.6 ou ultérieure pour Windows, et la version 1.2.4 ou ultérieure pour macOS. Pour plus d'informations, consultez Se connecter à l'aide d'un client fourni par AWS.

Interface Lambda

La fonction Lambda prend les attributs de périphérique, les attributs utilisateur et les attributs de connexion comme entrées du service Client VPN. Elle doit ensuite renvoyer une décision au service Client VPN : autoriser ou refuser la connexion.

Schéma de la demande

La fonction Lambda prend un blob JSON contenant les champs suivants en entrée.

```
{
    "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` — ID de la connexion client au point de terminaison Client VPN.
- `endpoint-id` — ID du point de terminaison Client VPN.
- `common-name` — Identifiant du périphérique. Dans le certificat client que vous créez pour le périphérique, le nom commun identifie le périphérique de manière unique.
- `username` — Identifiant de l'utilisateur, le cas échéant. Pour l'authentification Active Directory, il s'agit du nom d'utilisateur. Pour l'authentification fédérée basée sur SAML, il s'agit de `NameID`. Pour l'authentification mutuelle, ce champ est vide.
- `platform` — Plateforme du système d'exploitation client.
- `platform-version` — Version du système d'exploitation. Le service Client VPN fournit une valeur lorsque la directive `--push-peer-info` est présente dans la configuration du client OpenVPN, lorsque les clients se connectent à un point de terminaison Client VPN et lorsque le client exécute la plateforme Windows.
- `public-ip` — Adresse IP publique du périphérique qui se connecte.
- `client-openvpn-version` — Version OpenVPN utilisée par le client.

- `aws-client-version`— La version AWS du client.
- `groups` — Identifiant du groupe, le cas échéant. Pour l'authentification Active Directory, il s'agit d'une liste de groupes Active Directory. Pour l'authentification fédérée basée sur SAML, il s'agit d'une liste de groupes de fournisseurs d'identité (IdP). Pour l'authentification mutuelle, ce champ est vide.
- `schema-version` — Version du schéma. La valeur par défaut est `v3`.

Schéma de la réponse

La fonction Lambda doit renvoyer les champs suivants.

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

- `allow` — Obligatoire. Booléen (`true` | `false`) qui indique s'il faut autoriser ou refuser la nouvelle connexion.
- `error-msg-on-denied-connection` — Obligatoire. Chaîne de 255 caractères maximum qui peut être utilisée pour fournir des étapes et des conseils aux clients si la connexion est refusée par la fonction Lambda. En cas d'échec lors de l'exécution de la fonction Lambda (par exemple, en raison de la limitation), le message par défaut suivant est renvoyé aux clients.

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

- `posture-compliance-statuses` — Obligatoire. Si vous utilisez la fonction Lambda pour évaluer la posture, ceci est une liste des états pour le périphérique qui se connecte. Vous définissez les noms d'états en fonction de vos catégories d'évaluation de posture pour les périphériques, par exemple `compliant`, `quarantined`, `unknown`, etc. Chaque nom peut contenir jusqu'à 255 caractères. Vous pouvez spécifier jusqu'à 10 statuts.
- `schema-version` — Obligatoire. Version du schéma. La valeur par défaut est `v3`.

Vous pouvez utiliser la même fonction Lambda pour plusieurs points de terminaison Client VPN dans la même région.

Pour plus d'informations sur la création d'une fonction Lambda, consultez Mise en route avec AWS Lambda dans le Guide du développeur AWS Lambda .

Utilisation du gestionnaire de connexion client pour l'évaluation de la posture

Vous pouvez utiliser le gestionnaire de connexion client pour intégrer votre point de terminaison Client VPN à votre solution existante de gestion de périphériques afin d'évaluer la conformité de posture des périphériques qui se connectent. Pour que la fonction Lambda fonctionne comme gestionnaire d'autorisation de périphérique, utilisez l'authentification mutuelle pour votre point de terminaison Client VPN. Créez un certificat client unique et une clé pour chaque client (périphérique) qui se connectera au point de terminaison Client VPN. La fonction Lambda peut utiliser le nom commun unique du certificat client (transmis par le service Client VPN) pour identifier le périphérique et récupérer son état de conformité de posture à partir de votre solution de gestion des périphériques. Vous pouvez utiliser l'authentification mutuelle combinée à l'authentification basée sur l'utilisateur.

Vous pouvez également effectuer une évaluation de la posture de base dans la fonction Lambda elle-même. Par exemple, vous pouvez évaluer les champs `platform` et `platform-version` qui sont transmis à la fonction Lambda par le service Client VPN.

> **Note**
>
> Bien que le gestionnaire de connexion puisse être utilisé pour imposer une version minimale de AWS Client VPN l'application, le champ `aws-client-version` du gestionnaire de connexion ne s'applique qu'à l' AWS Client VPN application et est renseigné à partir de variables d'environnement sur l'appareil utilisateur.

Activation du gestionnaire de connexion client

Pour activer le gestionnaire de connexion client, créez ou modifiez un point de terminaison Client VPN et spécifiez l’ARN (Amazon Resource Name) de la fonction Lambda. Pour de plus amples informations, veuillez consulter Créer un point de terminaison VPN Client et Modifier un point de terminaison VPN Client.

Rôle lié à un service

AWS Client VPN crée automatiquement un rôle lié à un service dans votre compte appelé. AWSServiceRoleForClientVPNConnections Le rôle dispose des autorisations pour appeler la

fonction Lambda lorsqu'une connexion est établie au point de terminaison Client VPN. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour Client VPN.

Surveillance des échecs d'autorisation de connexion

Vous pouvez afficher l'état d'autorisation de connexion des connexions au point de terminaison Client VPN. Pour plus d'informations, consultez Afficher les connexions client.

Lorsque le gestionnaire de connexion client est utilisé pour évaluer la posture, vous pouvez également afficher les états de conformité de posture des périphériques qui se connectent à votre point de terminaison Client VPN dans les journaux de connexion. Pour plus d'informations, consultez Journalisation des connexions.

Si un périphérique échoue l'autorisation de connexion, le champ `connection-attempt-failure-reason` dans les journaux de connexion renvoie l'une des raisons d'échec suivantes :

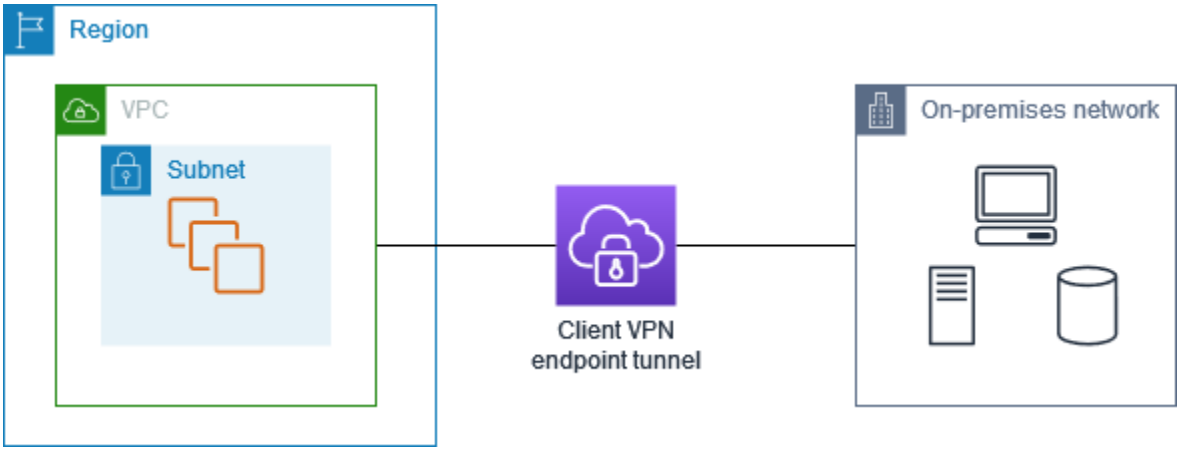
- `client-connect-failed` — La fonction Lambda a empêché l'établissement de la connexion.
- `client-connect-handler-timed-out` — La fonction Lambda a expiré.
- `client-connect-handler-other-execution-error` — La fonction Lambda a rencontré une erreur inattendue.
- `client-connect-handler-throttled` — La fonction Lambda a été limitée.
- `client-connect-handler-invalid-response` — La fonction Lambda a renvoyé une réponse non valide.
- `client-connect-handler-service-error` — Une erreur côté service s'est produite lors de la tentative de connexion.

Tunnel partagé sur les points de terminaison AWS Client VPN

Par défaut, lorsque vous disposez d'un point de terminaison Client VPN, tout le trafic provenant des clients est acheminé via le tunnel Client VPN. Lorsque vous activez le tunnel partagé sur le point de terminaison Client VPN, nous poussons les routes sur la table de routage des points de terminaison Client VPN vers le périphérique connecté au point de terminaison Client VPN. Cela garantit que seul le trafic avec une destination vers le réseau correspondant à une route à partir de la table de routage du point de terminaison Client VPN est acheminé via le tunnel Client VPN.

Vous pouvez utiliser un point de terminaison Client VPN à tunnel partagé lorsque vous ne souhaitez pas que tout le trafic utilisateur soit acheminé via le point de terminaison Client VPN.

Dans l'exemple suivant, le tunnel partagé est activé sur le point de terminaison Client VPN. Seul le trafic destiné au VPC (`172.31.0.0/16`) est acheminé via le tunnel Client VPN. Le trafic destiné aux ressources sur site n'est pas acheminé via le tunnel Client VPN.



Avantages du tunnel partagé

Les points de terminaison Client VPN à tunnel partagé offrent les avantages suivants :

- Vous pouvez optimiser le routage du trafic à partir des clients en faisant en sorte que seul le trafic destiné à AWS traverse le tunnel VPN.
- Vous pouvez réduire le volume du trafic sortant d'AWS, et ainsi réduire le coût du transfert des données.

Considérations relatives au routage

- Lorsque vous utilisez le tunnel partagé, toutes les routes qui se trouvent dans les tables de routage du point de terminaison VPN Client sont ajoutées à la table de routage client lorsque le VPN est établi. Cette opération est différente du comportement par défaut, qui remplace la table de routage client par l'entrée `0.0.0.0/0` pour acheminer tout le trafic via le VPN.

  > **Note**
  >
  > Il n'est pas recommandé d'ajouter un routage `0.0.0.0/0` vers la table de routage du point de terminaison Client VPN lorsque vous utilisez le mode Split-tunnel.

- Lorsque le mode tunnel partagé est activé, toute modification apportée à la table de routage du point de terminaison Client VPN entraîne la réinitialisation de toutes les connexions client.

Activation du tunnel partagé

Vous pouvez activer le tunnel partagé sur un point de terminaison Client VPN nouveau ou existant. Pour plus d'informations, consultez les rubriques suivantes :

- Créer un point de terminaison VPN Client
- Modifier un point de terminaison VPN Client

Journalisation des connexions

La journalisation des connexions est une fonction de AWS Client VPN qui vous permet de capturer des journaux de connexion pour votre point de terminaison VPN Client.

Un journal de connexion contient des entrées de journal de connexion. Chaque entrée de journal de connexion contient des informations sur un événement de connexion, c'est-à-dire lorsqu'un client (utilisateur final) se connecte, tente de se connecter ou se déconnecte de votre point de terminaison VPN Client. Vous pouvez utiliser ces informations pour exécuter des analyses judiciaires, analyser l'utilisation de votre point de terminaison VPN Client ou débugger des problèmes de connexion.

La journalisation des connexions est disponible dans toutes les régions où AWS le VPN Client est disponible. Les journaux de connexion sont publiés dans un groupe de journaux CloudWatch Logs de votre compte.

> **Note**
>
> Les tentatives d'authentification mutuelle qui ont échoué ne sont pas enregistrées.

Entrées du journal de connexion

Une entrée de journal de connexion est un blob au format JSON de paires valeur-clé. Voici un exemple d'entrée de journal de connexion.

```
{
    "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"
    }
```

Une entrée de journal de connexion contient les clés suivantes :

- `connection-log-type` - Type d'entrée du journal de connexion (`connection-attempt` ou `connection-reset`).
- `connection-attempt-status` - Statut de la demande de connexion (`successful`, `failed`, `waiting-for-assertion` ou `NA`).
- `connection-reset-status` - État d'un événement de réinitialisation de connexion (`NA` ou `assertion-received`).
- `connection-attempt-failure-reason` - Motif de l'échec de la connexion, le cas échéant.
- `connection-id` - ID de la connexion.
- `client-vpn-endpoint-id` - ID du point de terminaison VPN Client auquel la connexion a été établie.
- `transport-protocol` - Protocole de transport utilisé pour la connexion.
- `connection-start-time` - Heure de début de la connexion.
- `connection-last-update-time` - Heure de la dernière mise à jour de la connexion. Cette valeur est périodiquement mise à jour dans les journaux.
- `client-ip` - Adresse IP du client, qui est allouée à partir de la plage CIDR IPv4 du client pour le point de terminaison VPN Client.
- `common-name` - Nom commun du certificat utilisé pour l'authentification basée sur un certificat.
- `device-type` - Type de périphérique utilisé pour la connexion par l'utilisateur final.

- `device-ip` - Adresse IP publique du périphérique.
- `port` - Numéro de port de la connexion.
- `ingress-bytes` - Nombre d'octets entrants pour la connexion. Cette valeur est périodiquement mise à jour dans les journaux.
- `egress-bytes` - Nombre d'octets sortants pour la connexion. Cette valeur est périodiquement mise à jour dans les journaux.
- `ingress-packets` - Nombre de paquets entrants pour la connexion. Cette valeur est périodiquement mise à jour dans les journaux.
- `egress-packets` - Nombre de paquets sortants pour la connexion. Cette valeur est périodiquement mise à jour dans les journaux.
- `connection-end-time` - Heure de fin de la connexion. La valeur est `NA` si la connexion est toujours en cours ou si la tentative de connexion a échoué.
- `posture-compliance-statuses` - Les statuts de conformité de posture renvoyés par le gestionnaire de connexion client, le cas échéant.
- `username` — Le nom d'utilisateur est enregistré lorsque l'authentification basée sur l'utilisateur (AD ou SAML) est utilisée pour le point de terminaison.
- `connection-duration-seconds` — Durée d'une connexion en secondes. Égale à la différence entre « connection-start-time » et « connection-end-time ».

Pour plus d'informations sur l'activation de la journalisation des connexions, consultez Utilisation des journaux de connexion.

Considérations relatives à la mise à l'échelle Client VPN

Lorsque vous créez un point de terminaison Client VPN, tenez compte du nombre maximal de connexions VPN simultanées que vous envisagez de prendre en charge. Vous devez prendre en compte le nombre de clients que vous prenez actuellement en charge et si votre point de terminaison Client VPN peut répondre à une demande supplémentaire si nécessaire.

Les facteurs suivants affectent le nombre maximal de connexions VPN simultanées pouvant être prises en charge sur un point de terminaison Client VPN.

Taille de la plage CIDR client

Lorsque vous créez un point de terminaison Client VPN, vous devez spécifier une plage CIDR client, qui est un bloc CIDR IPv4 entre un masque réseau en /12 et en /22. Chaque connexion

VPN au point de terminaison Client VPN se voit attribuer une adresse IP unique à partir de la plage CIDR client. Un certain nombre d'adresses de la plage CIDR client sont également utilisées pour prendre en charge le modèle de disponibilité du point de terminaison Client VPN et ne peuvent pas être affectées aux clients. Vous ne pouvez pas modifier la plage CIDR client après avoir créé le point de terminaison Client VPN.

En général, nous vous recommandons de spécifier une plage CIDR client contenant deux fois le nombre d'adresses IP (par conséquent, de connexions simultanées) que vous prévoyez de prendre en charge sur le point de terminaison Client VPN.

Nombre de sous-réseaux associés

Lorsque vous associez un sous-réseau à un point de terminaison Client VPN, vous autorisez les utilisateurs à établir des séances VPN sur le point de terminaison Client VPN. Vous pouvez associer plusieurs sous-réseaux à un point de terminaison Client VPN pour une haute disponibilité et pour activer une capacité de connexion supplémentaire.

Voici le nombre de connexions VPN simultanées prises en charge en fonction du nombre d'associations de sous-réseaux pour le point de terminaison Client VPN.

Associations de sous-réseaux	Nombre de connexions prises en charge
1	7 000
2	36 500
3	66 500
4	96 500
5	126 000

Vous ne pouvez pas associer plusieurs sous-réseaux de la même zone de disponibilité à un point de terminaison Client VPN. Par conséquent, le nombre d'associations de sous-réseaux dépend également du nombre de zones de disponibilité disponibles dans une région AWS.

Par exemple, si vous prévoyez de prendre en charge 8 000 connexions VPN à votre point de terminaison Client VPN, spécifiez une taille minimale de plage CIDR client de `/18` (16 384 adresses IP) et associez au moins 2 sous-réseaux au point de terminaison Client VPN.

Si vous ne savez pas quel est le nombre de connexions VPN attendues pour votre point de terminaison Client VPN, nous vous recommandons de spécifier un bloc CIDR de taille `/16` ou plus élevée.

Pour en savoir plus sur les règles et limitations relatives à l'utilisation des plages CIDR clients et des réseaux cibles, consultez Règles et bonnes pratiques de AWS Client VPN.

Pour en savoir sur les quotas de votre point de terminaison Client VPN, consultez AWS Quotas VPN pour les clients.

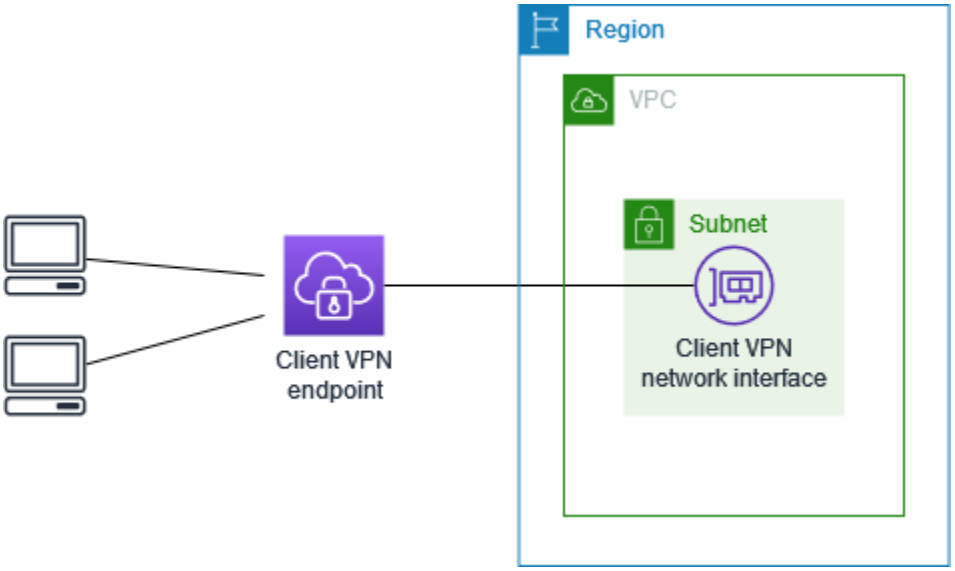
Scénarios et exemples pour AWS Client VPN

Cette section fournit des exemples de création et de configuration d'accès VPN Client pour vos clients.

Table des matières

Accès à un VPC avec AWS Client VPN

La configuration de ce scénario comprend un VPC cible unique. Nous vous recommandons cette configuration si vous avez besoin de donner accès aux ressources d'un VPC unique à des clients.



Avant de commencer, vous devez exécuter les actions suivantes :

- Créez ou identifiez un VPC avec au moins un sous-réseau. Identifiez le sous-réseau du VPC à associer au point de terminaison VPN Client et notez ses plages CIDR d'adresses IPv4.

- Identifiez une plage CIDR appropriée pour les adresses IP du client qui ne recouvre pas le CIDR du VPC.
- Examinez les règles et limitations pour les points de terminaison VPN Client dans Règles et bonnes pratiques de AWS Client VPN.

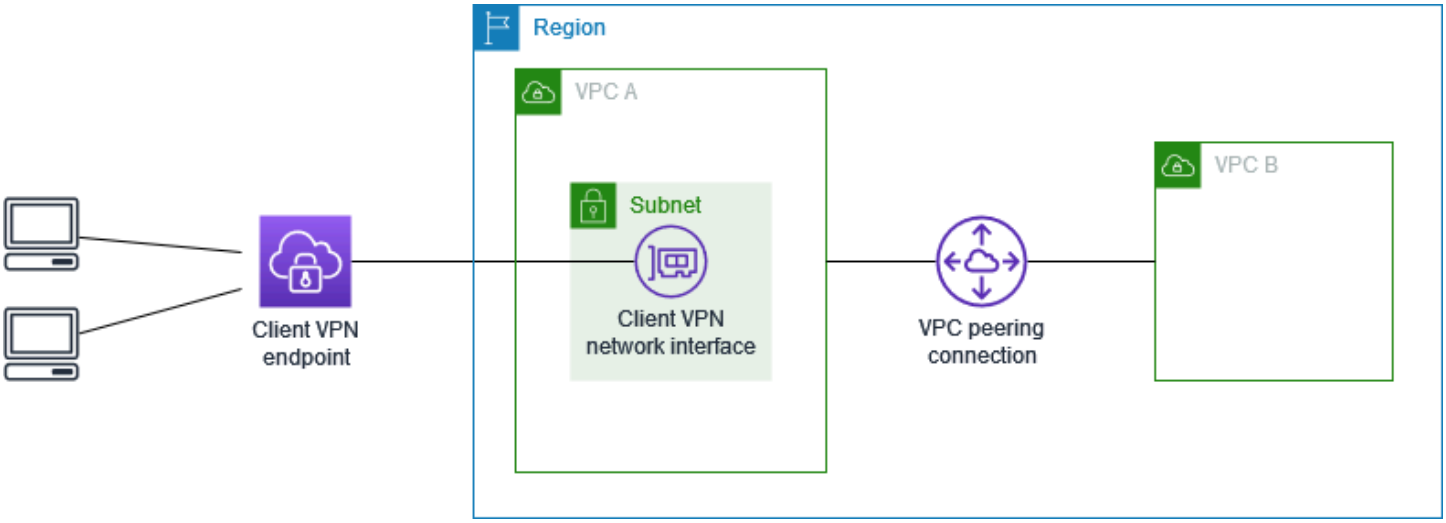
Pour mettre en œuvre cette configuration

1. Créez un point de terminaison VPN Client dans la même région que le VPC. Pour ce faire, effectuez les étapes décrites dans Créer un point de terminaison VPN Client.
2. Associez le sous-réseau au point de terminaison VPN Client. Pour y parvenir, effectuez les étapes décrites dans Associer un réseau cible à un point de terminaison Client VPN., puis sélectionnez le sous-réseau et le VPC que vous avez identifiés précédemment.
3. Ajouter une règle d'autorisation pour permettre aux clients d'accéder au VPC. Pour y parvenir, exécutez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Destination network (Réseau de destination), saisir la plage d'adresse CIDR IPv4 du VPC.
4. Ajouter une règle aux groupes de sécurité de vos ressources pour autoriser le trafic en provenance du groupe de sécurité qui a été appliqué à l'association du sous-réseau lors de l'étape 2. Pour plus d'informations, consultez Groupes de sécurité.

Accès à un VPC appairé avec AWS Client VPN

La configuration de ce scénario inclut un VPC cible (VPC A) qui est appairé avec un VPC supplémentaire (VPC B). Nous vous recommandons cette configuration si vous avez besoin de donner aux clients l'accès aux ressources d'un VPC cible et d'autres VPC appairés à celui-ci (par ex. le VPC B).

> **Note**
>
> La procédure d'autorisation d'accéder à un VPC appairé décrite ci-dessous n'est requise que si le point de terminaison VPN Client a été configuré en mode Split-tunnel (Canal partagé). En mode full-tunnel (canal complet), l'accès au VPC appairé est autorisé par défaut.



Avant de commencer, vous devez exécuter les actions suivantes :

- Créez ou identifiez un VPC avec au moins un sous-réseau. Identifiez le sous-réseau du VPC à associer au point de terminaison VPN Client et notez ses plages CIDR d'adresses IPv4.
- Identifiez une plage CIDR appropriée pour les adresses IP du client qui ne recouvre pas le CIDR du VPC.
- Examinez les règles et limitations pour les points de terminaison VPN Client dans Règles et bonnes pratiques de AWS Client VPN.

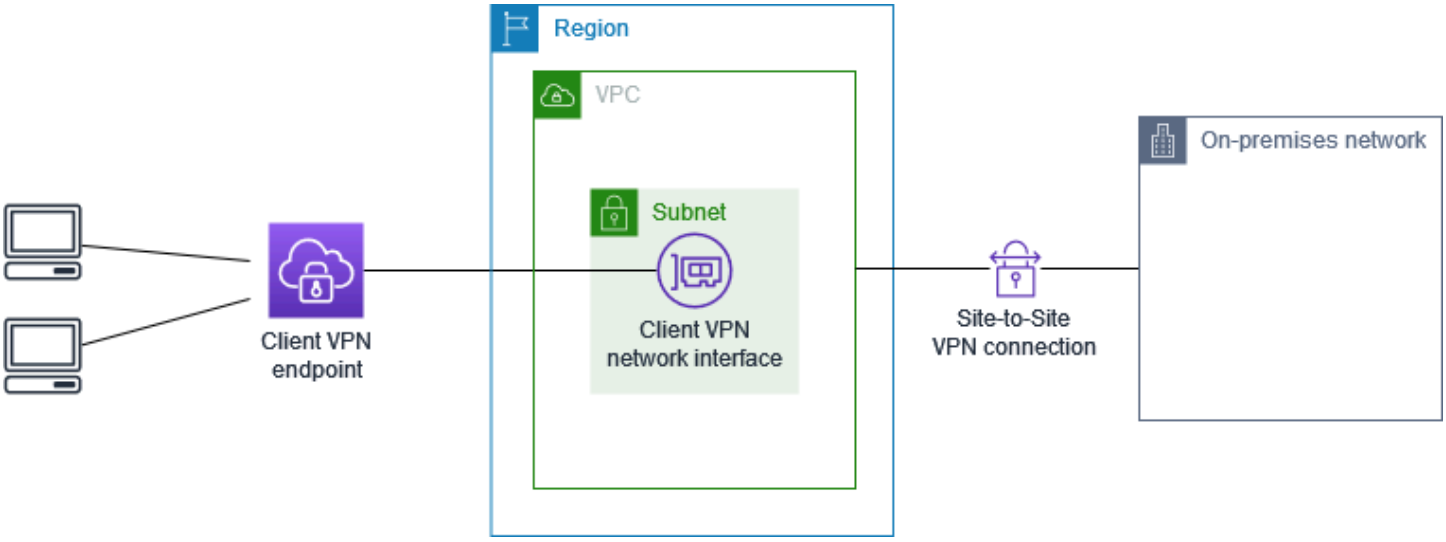
Pour mettre en œuvre cette configuration

1. Établissez la connexion d'appairage de VPC entre les VPC. Suivez les étapes de la page Création et acceptation d'une connexion d'appairage de VPC dans le Guide d'appairage Amazon VPC. Vérifiez que les instances du VPC A peuvent communiquer avec les instances du VPC B via la connexion appairage.
2. Créez un point de terminaison VPN Client dans la même région que le VPC cible. Dans le diagramme, il s'agit du VPC A. Effectuez les étapes décrites dans Créer un point de terminaison VPN Client.
3. Associez le sous-réseau que vous avez identifié avec le point de terminaison VPN Client que vous avez créé. Pour y arriver, effectuez les étapes décrites dans Associer un réseau cible à un point de terminaison Client VPN., puis sélectionnez le VPC et le sous-réseau. Par défaut, nous associons le groupe de sécurité par défaut du VPC au point de terminaison VPN Client. Vous pouvez associer un autre groupe de sécurité en suivant les étapes décrites dans the section called “Application d'un groupe de sécurité à un réseau cible”.

4. Ajouter une règle d'autorisation pour permettre aux clients d'accéder au VPC cible. Pour y arriver, effectuez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Activer le réseau de destination, saisissez la plage d'adresse CIDR IPv4 du VPC.
5. Ajoutez une route pour diriger le trafic vers le VPC appairé. Dans le diagramme, il s'agit du VPC B. Pour ce faire, effectuez les étapes décrites dans Création d'un acheminement de point de terminaison. Pour Destination de la route, saisissez la plage CIDR IPv4 du VPC appairé. Pour ID du sous-réseau VPC cible, sélectionnez le sous-réseau associé au point de terminaison VPN Client.
6. Ajoutez une règle d'autorisation pour donner aux clients l'accès au VPC appairé. Pour y arriver, effectuez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Réseau de destination, saisissez la plage d'adresse CIDR IPv4 du VPC appairé.
7. Ajoutez une règle aux groupes de sécurité pour vos instances dans le VPC A et le VPC B pour autoriser le trafic en provenance du groupe de sécurité qui a été appliqué au point de terminaison VPN Client à l'étape 3. Pour plus d'informations, consultez Groupes de sécurité.

Accès à un réseau sur site avec AWS Client VPN

La configuration de ce scénario comprend un accès à un réseau sur site uniquement. Nous vous recommandons cette configuration si vous devez permettre aux clients d'accéder aux ressources d'un réseau sur site uniquement.



Avant de commencer, vous devez exécuter les actions suivantes :

- Créez ou identifiez un VPC avec au moins un sous-réseau. Identifiez le sous-réseau du VPC à associer au point de terminaison VPN Client et notez ses plages CIDR d'adresses IPv4.
- Identifiez une plage CIDR appropriée pour les adresses IP du client qui ne recouvre pas le CIDR du VPC.
- Examinez les règles et limitations pour les points de terminaison VPN Client dans Règles et bonnes pratiques de AWS Client VPN.

Pour mettre en œuvre cette configuration

1. Activez la communication entre le VPC et votre propre réseau sur site via une connexion AWS Site-to-Site VPN. Pour y arriver, exécutez les étapes décrites dans la section Démarrage du Guide de l'utilisateur AWS Site-to-Site VPN.

   > **Note**
   >
   > Vous pouvez également implémenter ce scénario en utilisant une connexion AWS Direct Connect entre votre VPC et votre réseau local. Pour plus informations, veuillez consulter le Guide de l'utilisateur AWS Direct Connect.

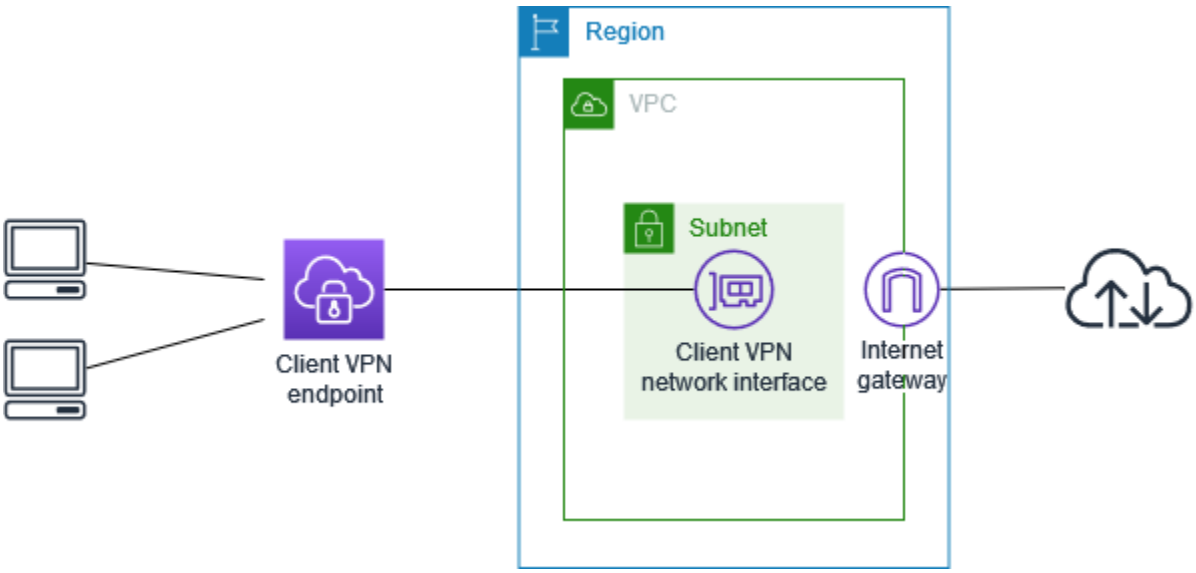
2. Testez la connexion AWS Site-to-Site VPN que vous avez créée à l'étape précédente. Pour y arriver, effectuez les étapes décrites dans la section Test de la connexion Site-to-Site VPN du Guide de l'utilisateur AWS Site-to-Site VPN. Si la connexion VPN fonctionne comme prévu, passez à l'étape suivante.
3. Créez un point de terminaison VPN Client dans la même région que le VPC. Pour y arriver, effectuez les étapes décrites dans Créer un point de terminaison VPN Client.
4. Associez le sous-réseau que vous avez identifié précédemment au point de terminaison VPN Client. Pour y arriver, effectuez les étapes décrites dans Associer un réseau cible à un point de terminaison Client VPN., puis sélectionnez le VPC et le sous-réseau.
5. Ajoutez un acheminement qui permet d'accéder à la connexion AWS Site-to-Site VPN. Pour y arriver, exécutez les étapes décrites dans Création d'un acheminement de point de terminaison. Pour Destination de l'acheminement, saisir la plage d'adresses CIDR IPv4 de la connexion AWS Site-to-Site VPN, et pour ID de sous-réseau de VPC cible, sélectionnez le sous-réseau que vous avez associé au point de terminaison VPN Client.
6. Ajoutez une règle d'autorisation pour donner aux clients l'accès à la connexion AWS Site-to-Site VPN. Pour ce faire, exécutez les étapes décrites dans Ajouter une règle d'autorisation à un point

de terminaison VPN Client. Pour Réseau de destination, saisir la plage d'adresses CIDR IPv4 de la connexion AWS Site-to-Site VPN.

Accès à Internet avec AWS Client VPN

La configuration de ce scénario comprend un VPC cible unique et l'accès à Internet. Nous vous recommandons cette configuration si vous avez besoin de donner aux clients l'accès aux ressources d'un VPC cible unique et d'autoriser l'accès à Internet.

Si vous avez effectué le didacticiel Mise en route avec AWS Client VPN, vous avez déjà implémenté ce scénario.



Avant de commencer, vous devez exécuter les actions suivantes :

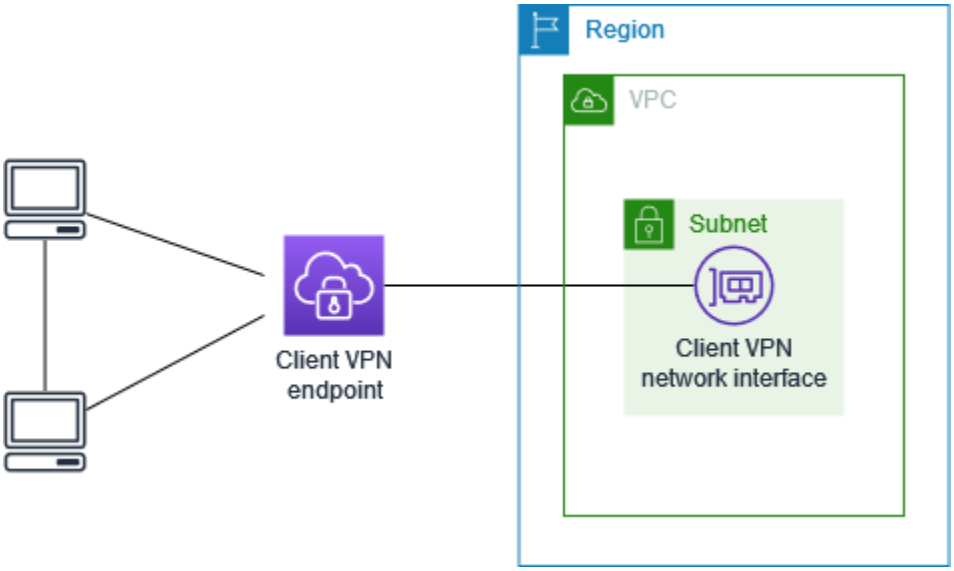
- Créez ou identifiez un VPC avec au moins un sous-réseau. Identifiez le sous-réseau du VPC à associer au point de terminaison VPN Client et notez ses plages CIDR d'adresses IPv4.
- Identifiez une plage CIDR appropriée pour les adresses IP du client qui ne recouvre pas le CIDR du VPC.
- Examinez les règles et limitations pour les points de terminaison VPN Client dans Règles et bonnes pratiques de AWS Client VPN.

Pour mettre en œuvre cette configuration

1. Assurez-vous que le groupe de sécurité que vous allez utiliser pour le point de terminaison VPN Client autorise le trafic sortant vers Internet. Pour y arriver, ajouter des règles sortantes pour autoriser le trafic vers 0.0.0.0/0 pour le trafic HTTP et HTTPS.
2. Créez une passerelle Internet et attachez-la à votre VPC. Pour plus d'informations, consultez Création et attachement d'une passerelle Internet dans le Guide de l'utilisateur Amazon VPC.
3. Rendez public votre sous-réseau en ajoutant une route vers la passerelle Internet à sa table de routage. Dans la console VPC, choisir Sous-réseaux, sélectionnez le sous-réseau que vous souhaitez associer au point de terminaison VPN Client, choisir Table de routage, puis sélectionnez l'ID de la table de routage. Choisir Actions, Modifier les routes, puis Ajouter un acheminement. Pour Destination, saisir `0.0.0.0/0`, et pour Cible, choisir la passerelle Internet de l'étape précédente.
4. Créez un point de terminaison VPN Client dans la même région que le VPC. Pour y arriver, effectuez les étapes décrites dans Créer un point de terminaison VPN Client.
5. Associez le sous-réseau que vous avez identifié précédemment au point de terminaison VPN Client. Pour y arriver, effectuez les étapes décrites dans Associer un réseau cible à un point de terminaison Client VPN., puis sélectionnez le VPC et le sous-réseau.
6. Ajouter une règle d'autorisation pour permettre aux clients d'accéder au VPC. Pour y arriver, effectuez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Réseau de destination à activer, saisir la plage CIDR d'adresses IPv4 du VPC.
7. Ajoutez une route qui autorise le trafic vers Internet. Pour y arriver, effectuez les étapes décrites dans Création d'un acheminement de point de terminaison. Pour Destination de l'acheminement, saisir `0.0.0.0/0`, et pour ID de sous-réseau de VPC cible, sélectionnez le sous-réseau que vous avez associé au point de terminaison VPN Client.
8. Ajoutez une règle d'autorisation pour permettre aux clients d'accéder à Internet. Pour y arriver, exécutez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Réseau de destination, saisir `0.0.0.0/0`.
9. Assurez-vous que les groupes de sécurité pour les ressources de votre VPC disposent d'une règle qui autorise l'accès à partir du groupe de sécurité associé au point de terminaison VPN client. Cela permet à vos clients d'accéder aux ressources de votre VPC.

lient-to-client Accès C à l'aide AWS du Client VPN

La configuration de ce scénario permet aux clients d'accéder à un seul VPC et d'acheminer le trafic entre eux. Nous recommandons cette configuration si les clients qui se connectent au même point de terminaison VPN Client doivent également communiquer entre eux. Les clients peuvent communiquer entre eux à l'aide de l'adresse IP unique qui leur est attribuée à partir de la plage d'adresses CIDR client lorsqu'ils se connectent au point de terminaison VPN Client.



Avant de commencer, vous devez exécuter les actions suivantes :

- Créez ou identifiez un VPC avec au moins un sous-réseau. Identifiez le sous-réseau du VPC à associer au point de terminaison VPN Client et notez ses plages CIDR d'adresses IPv4.
- Identifiez une plage CIDR appropriée pour les adresses IP du client qui ne recouvre pas le CIDR du VPC.
- Examinez les règles et limitations pour les points de terminaison VPN Client dans Règles et bonnes pratiques de AWS Client VPN.

> **Note**
>
> Les règles d'autorisation réseau utilisant des groupes Active Directory ou des groupes d'IdP basés sur SAML ne sont pas prises en charge dans ce scénario.

Pour mettre en œuvre cette configuration

1. Créez un point de terminaison VPN Client dans la même région que le VPC. Pour y arriver, effectuez les étapes décrites dans Créer un point de terminaison VPN Client.
2. Associez le sous-réseau que vous avez identifié précédemment au point de terminaison VPN Client. Pour y arriver, effectuez les étapes décrites dans Associer un réseau cible à un point de terminaison Client VPN., puis sélectionnez le VPC et le sous-réseau.
3. Ajouter un acheminement au réseau local dans la table de routage. Pour y arriver, effectuez les étapes décrites dans Création d'un acheminement de point de terminaison. Pour la Destination de l'acheminement, saisissez la plage d'adresse CIDR client et, pour ID de sous-réseau VPC cible, spécifiez `local`.
4. Ajouter une règle d'autorisation pour permettre aux clients d'accéder au VPC. Pour y arriver, effectuez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Activer le réseau de destination, saisissez la plage d'adresse CIDR IPv4 du VPC.
5. Ajoutez une règle d'autorisation pour permettre aux clients d'accéder à la plage d'adresse CIDR client. Pour y arriver, effectuez les étapes décrites dans Ajouter une règle d'autorisation à un point de terminaison VPN Client. Pour Activer le réseau de destination, saisissez la plage d'adresse CIDR client.

Restriction de l'accès à votre réseau avec AWS Client VPN

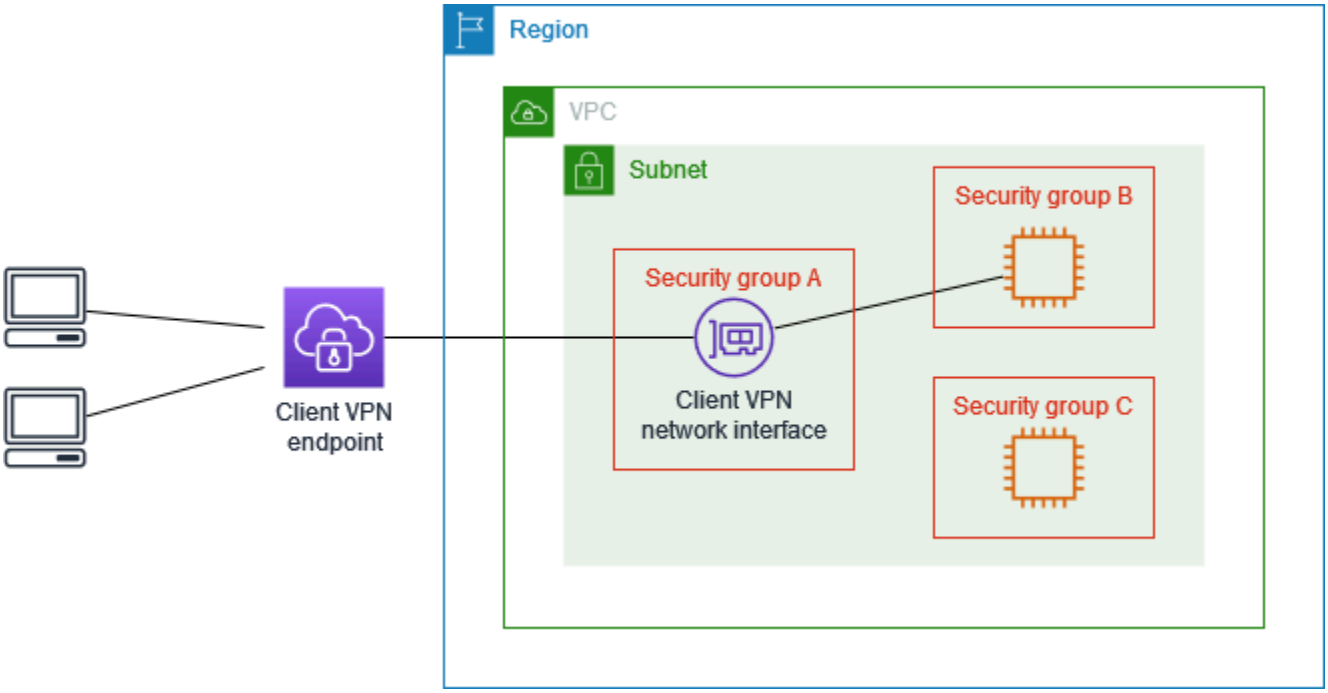
Vous pouvez configurer votre point de terminaison Client VPN pour restreindre l'accès à certaines ressources spécifiques de votre VPC. Pour l'authentification basée sur l'utilisateur, vous pouvez également restreindre l'accès à des parties de votre réseau, en fonction du groupe d'utilisateurs qui accède au point de terminaison VPN Client.

Restreindre l'accès à l'aide des groupes de sécurité

Vous pouvez accorder ou rejeter l'accès à certaines ressources spécifiques dans votre VPC en ajoutant ou en supprimant des règles de groupe de sécurité qui font référence au groupe de sécurité qui a été appliqué à l'association de réseau cible (le groupe de sécurité VPN Client). Cette configuration s'appuie sur le scénario décrit dans Accès à un VPC avec AWS Client VPN. Cette configuration s'applique en complément de la règle d'autorisation configurée dans ce scénario.

Pour accorder l'accès à une ressource spécifique, identifiez le groupe de sécurité associé à l'instance sur laquelle votre ressource s'exécute. Ensuite, créez une règle qui autorise le trafic à partir du groupe de sécurité VPN Client.

Dans le schéma suivant, le groupe de sécurité A est le groupe de sécurité Client VPN, le groupe de sécurité B est associé à une instance EC2 et le groupe de sécurité C est associé à une instance EC2. Si vous ajoutez une règle au groupe de sécurité B qui autorise l'accès depuis le groupe de sécurité A, les clients peuvent accéder à l'instance associée au groupe de sécurité B. Si le groupe de sécurité C ne dispose pas d'une règle autorisant l'accès depuis le groupe de sécurité A, les clients ne peuvent pas accéder à l'instance associée au groupe de sécurité C.



Avant de commencer, vérifier si le groupe de sécurité VPN Client est associé à d'autres ressources de votre VPC. Si vous ajoutez ou supprimez des règles qui font référence au groupe de sécurité VPN Client, vous pouvez également accorder ou rejeter l'accès aux autres ressources associées. Pour éviter cela, utilisez un groupe de sécurité spécialement créé pour une utilisation avec votre point de terminaison VPN Client.

Pour créer un groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
3. Choisissez le groupe de sécurité associé à l'instance sur laquelle votre ressource s'exécute.
4. Choisissez Actions, Modifier les règles entrantes.

5. Choisissez Ajouter une règle et procédez comme suit :
   - Dans Type, choisissez Tout le trafic ou choisissez un type de trafic spécifique que vous souhaitez autoriser.
   - Pour Source, choisir Personnalisé, puis saisir ou choisissez l'ID du groupe de sécurité VPN Client.
6. Choisir Enregistrer les règles.

Pour supprimer l'accès à une ressource spécifique, vérifiez le groupe de sécurité associé à l'instance sur laquelle votre ressource s'exécute. S'il existe une règle qui autorise le trafic à partir du groupe de sécurité VPN Client, supprimez-la.

Pour vérifier les règles de votre groupe de sécurité

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
3. Choisissez Règles entrantes.
4. Passez en revue la liste des règles. S'il existe une règle dans laquelle Source est le groupe de sécurité VPN Client, choisir Modifier les règles et choisir Supprimer (icône x) pour la règle. Sélectionnez Enregistrer les règles.

Restreindre l'accès en fonction des groupes d'utilisateurs

Si votre point de terminaison VPN Client est configuré pour l'authentification basée sur l'utilisateur, vous pouvez accorder à des groupes spécifiques d'utilisateurs d’accéder à des parties spécifiques de votre réseau. Pour y arriver, exécutez les étapes suivantes.

1. Configurez les utilisateurs et les groupes dans AWS Directory Service ou votre IdP. Pour plus d'informations, consultez les rubriques suivantes :
   - Authentification Active Directory
   - Les exigences et les observations relatives à l'authentification fédérée basée sur SAML
2. Créez une règle d'autorisation pour votre point de terminaison VPN Client qui permet à un groupe spécifié d'accéder à tout ou partie de votre réseau. Pour de plus amples informations, veuillez consulter Règles d'autorisation.

Si votre point de terminaison VPN Client est configuré pour l'authentification mutuelle, vous ne pouvez pas configurer de groupes d'utilisateurs. Lorsque vous créez une règle d'autorisation, vous devez accorder l'accès à tous les utilisateurs. Pour permettre à des groupes d'utilisateurs spécifiques d'accéder à certaines parties spécifiques de votre réseau, vous pouvez créer plusieurs points de terminaison VPN Client. Par exemple, pour chaque groupe d'utilisateurs qui accède à votre réseau, procédez comme suit :

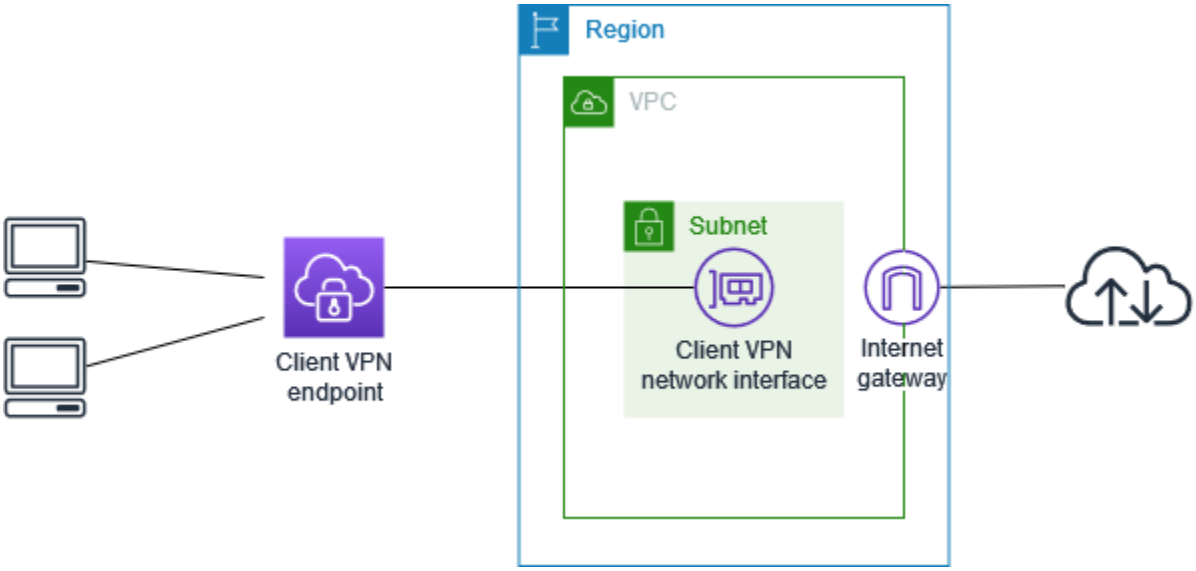
1. Créez un ensemble de certificats et de clés de serveur et de client pour ce groupe d'utilisateurs. Pour plus informations, veuillez consulter Authentification mutuelle.
2. Créez un point de terminaison VPN Client. Pour plus informations, veuillez consulter Créer un point de terminaison VPN Client.
3. Créez une règle d'autorisation qui accorde l'accès à tout ou partie de votre réseau. Par exemple, pour un point de terminaison VPN Client utilisé par les administrateurs, vous pouvez créer une règle d'autorisation d’accéder à l'ensemble du réseau. Pour plus informations, veuillez consulter Ajouter une règle d'autorisation à un point de terminaison VPN Client.

Mise en route avec AWS Client VPN

Dans ce didacticiel, vous allez créer un point de terminaison Client VPN qui :

- Fournit à tous les clients l'accès à un VPC unique.
- Fournit à tous les clients l'accès à Internet.
- Utilise l'authentification mutuelle.

Le diagramme suivant représente la configuration de votre VPC et de votre point de terminaison Client VPN à la fin de ce didacticiel.



Étapes

- Prérequis
- Étape 1 : Générer des certificats et des clés de serveur et client
- Étape 2 : Créer un point de terminaison Client VPN
- Étape 3 : Associer un réseau cible
- Étape 4 : Ajouter une règle d'autorisation pour le VPC
- Étape 5 : Fournir l'accès à Internet.
- Étape 6 : Vérifier les exigences requises pour les groupes de sécurité
- Étape 7 : Télécharger le fichier de configuration du point de terminaison Client VPN
- Étape 8 : Se connecter au point de terminaison VPN client

Prérequis

Avant de commencer ce didacticiel de démarrage, assurez-vous de disposer des éléments suivants :

- Les autorisations requises pour travailler avec les points de terminaison Client VPN.
- Les autorisations requises pour importer des certificats dans AWS Certificate Manager.
- VPC avec au moins un sous-réseau et une passerelle Internet. La table de routage associée à votre sous-réseau doit avoir une route vers la passerelle Internet.

Étape 1 : Générer des certificats et des clés de serveur et client

Ce didacticiel utilise l'authentification mutuelle. Avec l'authentification mutuelle, le VPN Client utilise des certificats pour procéder à l'authentification entre le client et le serveur. Vous devrez créer un certificat et une clé de serveur, et au moins un certificat client et une clé. Au minimum, le certificat de serveur devra être importé dans AWS Certificate Manager (ACM) et spécifié lorsque vous créez le point de terminaison Client VPN. L'importation du certificat client dans ACM est facultative.

Si vous ne disposez pas déjà de certificats à utiliser à cette fin, ils peuvent être créés à l'aide de l'utilitaire OpenVPN easy-rsa. Pour obtenir une présentation détaillée des étapes requises pour générer les certificats et les clés de serveur et client à l'aide de l'utilitaire Easy RSA OpenVPN et les importer dans ACM, consultez Authentification mutuelle.

> **Note**
>
> Le certificat de serveur doit être provisionné ou importé dans AWS Certificate Manager (ACM) dans la même région AWS où vous créez le point de terminaison Client VPN.

Étape 2 : Créer un point de terminaison Client VPN

Le point de terminaison VPN Client est la ressource que vous créez et configurez pour activer et gérer des sessions VPN Client. Il s'agit du point de terminaison pour toutes les sessions VPN client.

Pour créer un point de terminaison Client VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Client VPN Endpoints (Points de terminaison Client VPN), puis choisissez Create Client VPN Endpoint (Créer un point de terminaison Client VPN).

3. (Facultatif) Fournissez une balise de nom et une description pour le point de terminaison Client VPN.
4. Pour CIDR IPv4 client, spécifiez une plage d'adresses IP, en notation CIDR, à partir de laquelle attribuer des adresses IP client.

   > **Note**
   >
   > La plage d'adresses ne peut pas chevaucher le réseau cible, la plage d'adresses VPC ou les routes qui seront associées au point de terminaison Client VPN. La plage d'adresses du client doit être au minimum /22 et ne doit pas dépasser la taille de bloc CIDR /12. Vous ne pouvez pas modifier la plage d'adresses client après avoir créé le point de terminaison Client VPN.

5. Pour Server certificate ARN (ARN du certificat de serveur), sélectionnez l'ARN du certificat de serveur que vous avez généré lors de l'Étape 1.
6. Sous Authentication options (Options d'authentification), choisissez Use mutual authentication (Utiliser l'authentification mutuelle), puis pour Client certificate ARN (ARN de certificat client), sélectionnez l'ARN du certificat à utiliser comme certificat client.

   Si les certificats du serveur et du client ont été émis par la même autorité de certification (CA), vous pouvez utiliser l'ARN du certificat du serveur à la fois pour les certificats de serveur et de client. Dans ce scénario, tout certificat client correspondant au certificat de serveur peut être utilisé pour s'authentifier.
7. Vous pouvez conserver le reste des paramètres par défaut, puis sélectionner Créer un point de terminaison Client VPN.

Après avoir créé le point de terminaison Client VPN, son état est `pending-associate`. Les clients peuvent établir une connexion VPN seulement après que vous avez associé au moins un réseau cible.

Pour plus d'informations sur les options que vous pouvez spécifier pour un point de terminaison Client VPN, consultez Créer un point de terminaison VPN Client.

Étape 3 : Associer un réseau cible

Pour permettre aux clients d'établir une session VPN, vous associez un réseau cible au point de terminaison Client VPN. Un réseau cible est un sous-réseau dans un VPC.

Pour associer un réseau cible à un point de terminaison Client VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN que vous avez créé dans la procédure précédente, puis choisissez (Target netwok associations (Associations de réseau cible), Associate target network (Associer le réseau cible).
4. Pour VPC, choisissez le VPC dans lequel le sous-réseau est situé.
5. Pour Choose a subnet to associate (Choisir un sous-réseau à associer), choisissez le sous-réseau à associer au point de terminaison Client VPN.
6. Choisissez Associate target network (Associer le réseau cible).
7. Si les règles d'autorisation le permettent, une association de sous-réseau suffit pour que les clients puissent accéder à l'ensemble du réseau d'un VPC. Vous pouvez associer des sous-réseaux supplémentaires pour fournir une haute disponibilité au cas où une zone de disponibilité tombe en panne.

Lorsque vous associez le premier sous-réseau au point de terminaison Client VPN, ce qui suit se produit :

- L'état du point de terminaison Client VPN devient `available`. Les clients peuvent désormais établir une connexion VPN, mais ils ne peuvent pas accéder aux ressources du VPC tant que vous n'avez pas ajouté les règles d'autorisation.
- La route locale du VPC est automatiquement ajoutée à la table de routage du point de terminaison Client VPN.
- Le groupe de sécurité par défaut du VPC est automatiquement appliqué au point de terminaison du VPN client.

Étape 4 : Ajouter une règle d'autorisation pour le VPC

Pour que les clients puissent accéder au VPC, il doit y avoir une route vers le VPC dans la table de routage du point de terminaison Client VPN et une règle d'autorisation. L'itinéraire a déjà été ajouté automatiquement à l'étape précédente. Dans ce didacticiel, nous accordons l'accès à tous les utilisateurs.

Pour ajouter une règle d'autorisation pour le VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client auquel ajouter la règle d'autorisation. Choisissez Authorization rules (Règles d'autorisation), puis choisissez Ajouter une règle d'autorisation.
4. Pour Destination network to enable access (Réseau de destination pour autoriser l'accès), entrez le CIDR du réseau pour lequel vous souhaitez autoriser l'accès. Par exemple, pour autoriser l'accès à l'ensemble du VPC, spécifiez le bloc CIDR IPv4 du VPC.
5. Pour Accorder l'accès à, choisissez Autoriser l'accès à tous les utilisateurs.
6. (Facultatif) Pour Description, saisissez une brève description de la règle d'autorisation.
7. Choisir Ajouter une règle d'autorisation.

Étape 5 : Fournir l'accès à Internet.

Vous pouvez fournir l'accès à des réseaux supplémentaires connectés au VPC, comme des services AWS, des VPC appairés, des réseaux sur site et Internet. Pour chaque réseau supplémentaire, vous ajoutez une route vers le réseau dans la table de routage du point de terminaison VPN client et vous configurez une règle d'autorisation pour accorder l'accès aux clients.

Pour ce tutoriel, nous souhaitons accorder à tous les utilisateurs l'accès à Internet et au VPC. Vous avez déjà configuré l'accès au VPC. Cette étape concerne donc l'accès à Internet.

Pour fournir l'accès à Internet.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client que vous avez créé pour ce didacticiel. Choisissez Route Table (Table de routage), puis Create Route (Créer un routage).
4. Pour Route destination (Destination de route), saisissez `0.0.0.0/0`. Pour Subnet ID for target network association (ID de sous-réseau pour l'association de réseau cible), spécifiez l'ID du sous-réseau par lequel le trafic sera acheminé.
5. Choisir Créer un acheminement.
6. Choisissez Authorization rules (Règles d'autorisation), puis Add authorization rule (Ajouter une règle d'autorisation).

7. Pour Destination network to enable access (Réseau de destination pour activer l'accès), entrez `0.0.0.0/0` et choisissez Allow access to all users (Autoriser l'accès à tous les utilisateurs).
8. Choisir Ajouter une règle d’autorisation.

Étape 6 : Vérifier les exigences requises pour les groupes de sécurité

Dans ce didacticiel, aucun groupe de sécurité n'a été spécifié lors de la création du point de terminaison VPN client à l'étape 2. Cela signifie que le groupe de sécurité par défaut du VPC est automatiquement appliqué au point de terminaison VPN client lorsqu'un réseau cible est associé. Par conséquent, le groupe de sécurité par défaut pour le VPC doit désormais être associé au point de terminaison VPN client.

Vérifier les exigences suivantes pour les groupes de sécurité

- Que le groupe de sécurité associé au sous-réseau via lequel vous acheminez le trafic (dans ce cas, le groupe de sécurité VPC par défaut) autorise le trafic sortant vers Internet. Pour ce faire, ajoutez une règle sortante qui autorise tout le trafic vers la destination `0.0.0.0/0`.
- Les groupes de sécurité pour les ressources de votre VPC disposent d'une règle qui autorise l'accès à partir du groupe de sécurité appliqué au point de terminaison Client VPN (dans ce cas, le groupe de sécurité VPC par défaut). Cela permet à vos clients d'accéder aux ressources de votre VPC.

Pour plus d’informations, consultez Groupes de sécurité.

Étape 7 : Télécharger le fichier de configuration du point de terminaison Client VPN

L'étape suivante consiste à télécharger et à préparer le fichier de configuration du point de terminaison VPN client. Le fichier de configuration inclut le point de terminaison VPN client et les informations de certificat requises pour établir une connexion VPN. Vous pouvez fournir ce fichier aux clients finaux qui ont besoin de se connecter au point de terminaison VPN client. L'utilisateur final utilise le fichier pour configurer son application cliente VPN.

Pour télécharger et préparer le fichier de configuration du point de terminaison Client VPN

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN que vous avez créé pour ce didacticiel, puis Download client configuratoin (Télécharger la configuration client).
4. Recherchez le certificat client et la clé générés lors de l'étape 1. le certificat et la clé de client sont disponibles aux emplacements suivants dans le référentiel cloné easy-rsa OpenVPN :

   - Certificat de client — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Clé de client — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Ouvrez le fichier de configuration du point de terminaison VPN Client à l'aide de votre éditeur de texte préféré. Ajoutez les balise `<cert></cert>` et `<key></key>` au fichier. Placez le contenu du certificat de client et le contenu de la clé privée entre les balises correspondantes, comme suit :

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

   <key>
   Contents of private key (.key) file
   </key>
   ```
6. Enregistrez et fermez le fichier de configuration du point de terminaison Client VPN.
7. Distribuez le fichier de configuration du point de terminaison VPN client à vos clients finaux.

Pour plus d'informations sur le fichier de configuration du point de terminaison Client VPN, consultez Exporter et configurer le fichier de configuration du client.

Étape 8 : Se connecter au point de terminaison VPN client

Vous pouvez vous connecter au point de terminaison VPN client à l'aide du client fourni par AWS ou d'une autre application cliente OpenVPN et du fichier de configuration que vous venez de créer. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS Client VPN.

Utilisation d'AWS Client VPN

Les rubriques suivantes expliquent comment utiliser Client VPN.

Table des matières

Accéder au portail en libre-service

Si vous avez activé le portail en libre-service pour votre point de terminaison VPN Client, vous pouvez fournir à vos clients une URL du portail en libre-service. Les clients peuvent accéder au portail dans un navigateur Web et utiliser leurs informations d'identification utilisateur pour se connecter. Dans le portail, les clients peuvent télécharger le fichier de configuration du point de terminaison VPN Client et télécharger la dernière version du AWS client fourni.

Les règles suivantes s'appliquent :

- Le portail libre-service n'est pas disponible pour les clients qui s'authentifient à l'aide d'une authentification mutuelle.
- Le fichier de configuration disponible dans le portail en libre-service est le même fichier de configuration que vous exportez à l'aide de la console Amazon VPC ou de la AWS CLI. Si vous devez personnaliser le fichier de configuration avant de le distribuer aux clients, vous devez le distribuer vous-même aux clients.

- Vous devez activer l'option de portail en libre-service pour votre point de terminaison VPN Client, sinon les clients ne peuvent pas accéder au portail. Si cette option n'est pas activée, vous pouvez modifier votre point de terminaison VPN Client pour l'activer.

Après avoir activé l'option de portail en libre-service, fournissez à vos clients l'une des URL suivantes :

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

  Si les clients accèdent au portail à l'aide de cette URL, ils doivent saisir l'ID du point de terminaison VPN Client avant de pouvoir se connecter.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  Remplacez *<endpoint-id>* dans l'URL précédente par l'ID de votre point de terminaison VPN Client, par exemple, `cvpn-endpoint-0123456abcd123456`.

Vous pouvez également afficher l'URL du portail en libre-service dans la sortie de la commande describe-client-vpn-endpoints AWS CLI. L'URL est également disponible dans l'onglet Détails de la page Points de terminaison VPN Client dans la console Amazon VPC.

Pour plus d'informations sur la configuration du portail en libre-service pour une utilisation avec l'authentification fédérée, consultez Prise en charge du portail en libre-service.

Règles d'autorisation

Les règles d'autorisation agissent comme des règles de pare-feu qui accordent l'accès aux réseaux. En ajoutant des règles d'autorisation, vous accordez à des clients spécifiques l'accès au réseau spécifié. Vous devez disposer d'une règle d'autorisation pour chaque réseau auquel vous souhaitez accorder l'accès. Vous pouvez ajouter des règles d'autorisation à un point de terminaison VPN Client à l'aide de la console et de la AWS CLI.

> **Note**
>
> En outre, Client VPN utilise la correspondance de préfixe la plus longue lors de l'évaluation des règles d'autorisation. Consultez la rubrique de dépannageLes règles d'autorisation pour les groupes Active Directory ne fonctionnent pas comme prévuetPriorité d'acheminementdans le Vérification Guide de l'utilisateur Amazon VPC pour plus de détails.

Table des matières

Ajouter une règle d'autorisation à un point de terminaison VPN Client

Ajouter une règle d'autorisation à un point de terminaison VPN Client (AWS Management Console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client auquel ajouter la règle d'autorisation, choisissez Authorization rules (Règles d'autorisation), puis Add authorization rule (Ajouter une règle d'autorisation).
4. Pour Destination network to enable access (Réseau de destination pour autoriser l'accès), entrez l'adresse IP, en notation CIDR, du réseau auquel les utilisateurs doivent accéder (par exemple, le bloc d'adresses CIDR de votre VPC).
5. Spécifiez les clients autorisés à accéder au réseau spécifié. Pour Pour accorder l'accès à, effectuez l'une des actions suivantes :

   - Pour accorder l'accès à tous les clients, choisissez Autoriser l'accès à tous les utilisateurs.
   - Pour restreindre l'accès à des clients spécifiques, choisissez Autoriser l'accès aux utilisateurs d'un groupe d'accès spécifique, puis, pour ID de groupe d'accès, saisissez l'ID du groupe auquel accorder l'accès. Par exemple, l'identificateur de sécurité (SID) d'un groupe Active Directory ou l'ID/le nom d'un groupe défini dans un fournisseur d'identité (IdP) basé sur SAML.
     - (Active Directory) Pour obtenir le SID, vous pouvez utiliser l'applet de commande Microsoft Powershell Get-ADGroup, par exemple :

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

       Vous pouvez également ouvrir l'outil Utilisateurs et ordinateurs Active Directory, afficher les propriétés du groupe, accéder à l'onglet Éditeur d'attributs et obtenir la valeur pour `objectSID`. Si nécessaire, choisissez d'abord Affichage, Fonctionnalités avancées pour activer l'onglet Éditeur d'attributs.

- (Authentification fédérée basée sur SAML) L'ID ou le nom du groupe doit correspondre aux informations d'attribut de groupe renvoyées dans l'assertion SAML.

6. Pour Description, saisissez une brève description de la règle d'autorisation.
7. Choisir Ajouter une règle d’autorisation.

Ajouter une règle d'autorisation à un point de terminaison VPN Client (AWS CLI)

Utilisez la commande authorize-client-vpn-ingress.

Supprimer une règle d'autorisation d'un point de terminaison VPN Client

En supprimant une règle d’autorisation, vous supprimez l'accès au réseau spécifié.

Vous pouvez supprimer des règles d'autorisation à un point de terminaison VPN Client à l'aide de la console et de la AWS CLI.

Pour supprimer une règle d'autorisation d’un point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client auquel la règle d'autorisation est ajoutée et choisissez Authorization rule (Règle d'autorisation).
4. Sélectionnez la règle d'autorisation à supprimer, choisissez Remove authorization rule (Supprimer la règle d'autorisation), puis Remove authorization rule (Supprimer la règle d'autorisation).

Supprimer une règle d'autorisation d'un point de terminaison VPN Client (AWS CLI)

Utilisez la commande revoke-client-vpn-ingress.

Affichage des règles d'autorisation

Vous pouvez afficher les règles d'autorisation d'un point de terminaison VPN Client spécifique à l'aide de la console et de la AWS CLI.

Pour afficher les règles d'autorisation (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client pour lequel vous souhaitez afficher les règles d'autorisation et choisir Autorization rules (Règles d'autorisation).

Pour afficher les règles d'autorisation (AWS CLI)

Utilisez la commande describe-client-vpn-authorization-rules.

Exemples de scénario pour les règles d'autorisation

Cette section décrit le fonctionnement des règles d'autorisation pour AWS Client VPN. Elle contient des points clés relatifs à la compréhension des règles d'autorisation, un exemple d'architecture et une discussion d'exemples de scénario correspondant à l'exemple d'architecture.

Table des matières

Points clés relatifs à la compréhension des règles d'autorisation

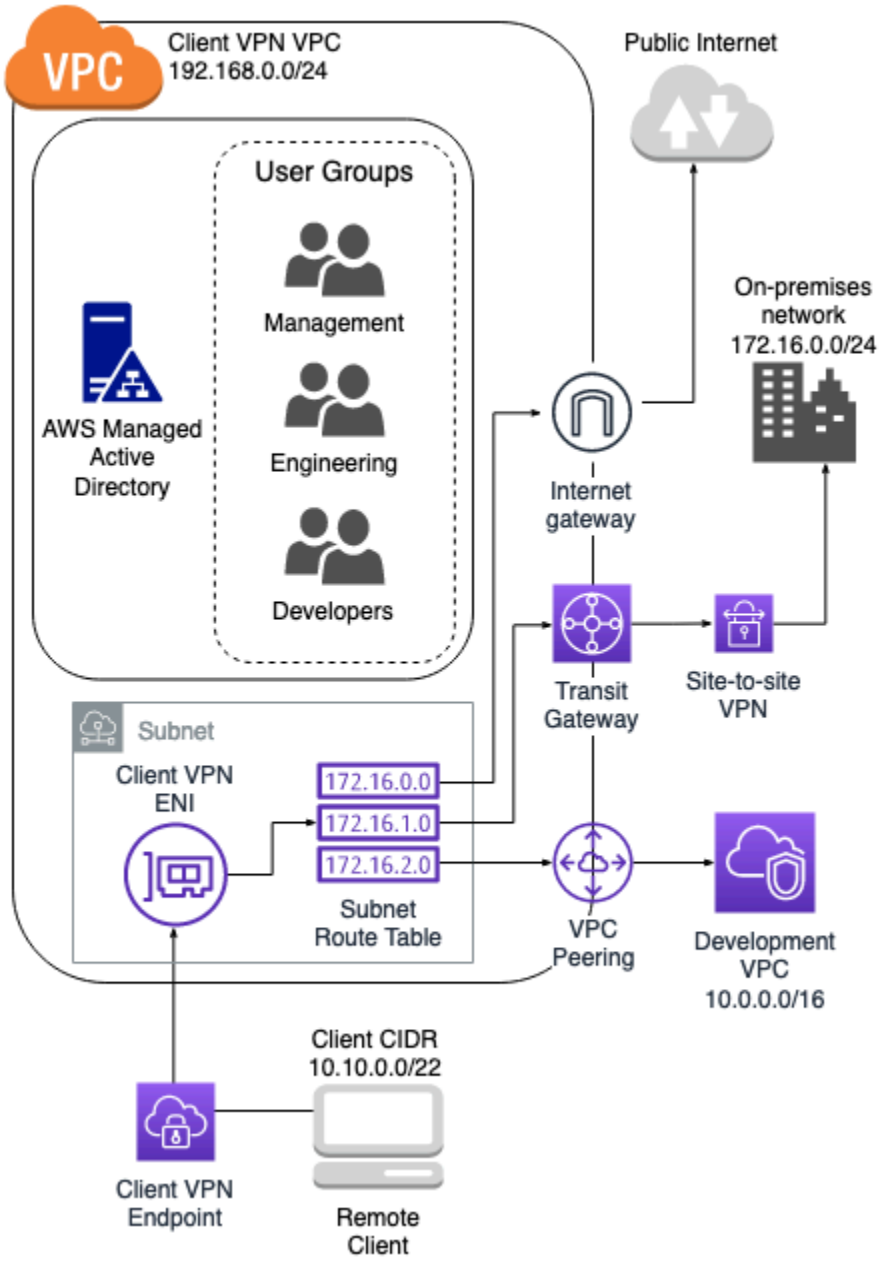
Les points suivants expliquent certains comportements des règles d'autorisation :

- Pour autoriser l'accès à un réseau de destination, une règle d'autorisation doit être explicitement ajoutée. Le comportement par défaut consiste à refuser l'accès.
- Vous ne pouvez pas ajouter de règle d'autorisation pour restreindre l'accès à un réseau de destination.
- Le CIDR `0.0.0.0/0` est traité comme un cas spécial. Il est traité en dernier, quel que soit l'ordre de création des règles d'autorisation.

- Le CIDR `0.0.0.0/0` peut être considéré comme « n'importe quelle destination » ou « toute destination non définie par d'autres règles d'autorisation ».
- La correspondance de préfixe le plus long est la règle qui prévaut.

Exemple d'architecture pour les scénarios de règle d'autorisation

Le schéma suivant montre l'exemple d'architecture utilisé pour les exemples de scénario présentés dans cette section.



Scénario 1 : Accès à une destination unique

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès au VPC du VPN client	S-xxxxx16	False	192.168.0.0/24

Comportement obtenu

- Le groupe d'ingénierie peut accéder uniquement à `172.16.0.0/24`.
- Le groupe de développement peut accéder uniquement à `10.0.0.0/16`.
- Le groupe de gestionnaires peut accéder uniquement à `192.168.0.0/24`.
- Tout le reste du trafic est supprimé par le point de terminaison du VPN client.

> **Note**
>
> Dans ce scénario, aucun groupe d'utilisateurs n'a accès à l'Internet public.

Scénario 2 : Utilisation de n'importe quel CIDR de destination (0.0.0.0/0)

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0

Comportement obtenu

- Le groupe d'ingénierie peut accéder uniquement à `172.16.0.0/24`.
- Le groupe de développement peut accéder uniquement à `10.0.0.0/16`.
- Le groupe de gestionnaires peut accéder à l'Internet public et à `192.168.0.0/24`, mais ne peut pas accéder à `172.16.0.0/24` ou à `10.0.0/16`.

> **Note**
>
> Dans ce scénario, aucune règle ne faisant référence à `192.168.0.0/24`, l'accès à ce réseau est également fourni par la règle `0.0.0.0/0`.
> Une règle contenant `0.0.0.0/0` est toujours évaluée en dernier, quel que soit l'ordre dans lequel les règles ont été créées. Pour cette raison, gardez à l'esprit que les règles évaluées

avant `0.0.0.0/0` jouent un rôle pour déterminer les réseaux auxquels `0.0.0.0/0` donne accès.

Scénario 3 : Correspondance de préfixe IP plus long

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès à un seul hôte dans le VPC de développement	S-xxxxx16	False	10.0.1.66/32

Comportement obtenu

- Le groupe d'ingénierie peut accéder uniquement à `172.16.0.0/24`.
- Le groupe de développement peut accéder à `10.0.0.0/16`, sauf pour l'hôte unique `10.0.2.119/32`.

- Le groupe de gestionnaires peut accéder à l'Internet public, `192.168.0.0/24`, et à un hôte unique (`10.0.2.119/32`) au sein du VPC de développement, mais n'a accès ni à `172.16.0.0/24` ni à aucun des hôtes restants du VPC de développement.

> **Note**
>
> Vous pouvez voir ici comment une règle avec un préfixe IP plus long est prioritaire par rapport à une règle avec un préfixe IP plus court. Si vous souhaitez que le groupe de développement ait accès à `10.0.2.119/32`, une règle supplémentaire autorisant l'équipe de développement à accéder à `10.0.2.119/32` doit être ajoutée.

Scénario 4 : Chevauchement de CIDR (même groupe)

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès à un hôte	S-xxxxx16	False	10.0.1.66/32

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
unique dans le VPC de développement			
Fournir au groupe d'ingénierie un accès à un sous-réseau plus petit au sein du réseau sur site	S-xxxxx14	False	172,16,0,128/25

Comportement obtenu

- Le groupe de développement peut accéder à `10.0.0.0/16`, sauf pour l'hôte unique `10.0.2.119/32`.
- Le groupe de gestionnaires peut accéder à l'Internet public, `192.168.0.0/24`, et à un hôte unique (`10.0.2.119/32`) au sein du réseau `10.0.0.0/16`, mais ne peut accéder ni à `172.16.0.0/24` ni à aucun des hôtes restants du réseau `10.0.0.0/16`.
- Le groupe d'ingénierie a accès à `172.16.0.0/24`, notamment au sous-réseau plus spécifique `172.16.0.128/25`.

Scénario 5 : Règle 0.0.0.0/0 supplémentaire

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement	S-xxxxx15	False	10.0.0.0/16

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
un accès au VPC de développement			
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès à un hôte unique dans le VPC de développement	S-xxxxx16	False	10.0.1.66/32
Fournir au groupe d'ingénierie un accès à un sous-réseau plus petit au sein du réseau sur site	S-xxxxx14	False	172,16,0,128/25
Fournir au groupe d'ingénieurs un accès à n'importe quelle destination	S-xxxxx14	False	0.0.0.0/0

Comportement obtenu

- Le groupe de développement peut accéder à `10.0.0.0/16`, sauf pour l'hôte unique `10.0.2.119/32`.
- Le groupe de gestionnaires peut accéder à l'Internet public, `192.168.0.0/24`, et à un seul hôte (`10.0.2.119/32`) au sein du réseau `10.0.0.0/16`, mais n'a accès ni à `172.16.0.0/24` ni à aucun des hôtes restants du réseau `10.0.0.0/16`.

- Le groupe d'ingénierie peut accéder à l'Internet public, `192.168.0.0/24`, et à `172.16.0.0/24`, dont le sous-réseau plus spécifique `172.16.0.128/25`.

> **Note**
>
> Notez que les groupes d'ingénierie et de gestion peuvent désormais accéder à `192.168.0.0/24`. Cela est dû au fait que les deux groupes ont accès à `0.0.0.0/0` (n'importe quelle destination) et qu'aucune autre règle ne fait référence à `192.168.0.0/24`.

Scénario 6 : Ajout d'une règle pour 192.168.0.0/24

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès à un hôte unique dans le VPC de développement	S-xxxxx16	False	10.0.1.66/32

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès à un sous-réseau du réseau sur site	S-xxxxx14	False	172,16,0,128/25
Fournir au groupe d'ingénieurs un accès à n'importe quelle destination	S-xxxxx14	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès au VPC du VPN client	S-xxxxx16	False	192.168.0.0/24

Comportement obtenu

- Le groupe de développement peut accéder à `10.0.0.0/16`, sauf pour l'hôte unique `10.0.2.119/32`.
- Le groupe de gestionnaires peut accéder à l'Internet public, `192.168.0.0/24`, et à un hôte unique (`10.0.2.119/32`) au sein du réseau `10.0.0.0/16`, mais n'a accès ni à `172.16.0.0/24` ni à aucun des hôtes restants du réseau `10.0.0.0/16`.
- Le groupe d'ingénierie peut accéder à l'Internet public, `172.16.0.0/24`, et à `172.16.0.128/25`.

> **Note**
>
> Notez comment l'ajout de la règle permettant au groupe de gestionnaires d'accéder à `192.168.0.0/24` fait que le groupe de développement n'a plus accès à ce réseau de destination.

Scénario 7 : Accès pour tous les groupes d'utilisateurs

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe d'ingénierie un accès au réseau sur site	S-xxxxx14	False	172.16.0.0/24
Fournir au groupe de développement un accès au VPC de développement	S-xxxxx15	False	10.0.0.0/16
Fournir au groupe de gestionnaires un accès à n'importe quelle destination	S-xxxxx16	False	0.0.0.0/0
Fournir au groupe de gestionnaires un accès à un hôte unique dans le VPC de développement	S-xxxxx16	False	10.0.1.66/32
Fournir au groupe d'ingénierie un accès à un sous-réseau du réseau sur site	S-xxxxx14	False	172,16,0,128/25
Fournir au groupe d'ingénierie un accès à tous les réseaux	S-xxxxx14	False	0.0.0.0/0

Description de la règle	ID du groupe	Autoriser l'accès à tous les utilisateurs	CIDR de destination
Fournir au groupe de gestionnaires un accès au VPC du VPN client	S-xxxxx16	False	192.168.0.0/24
Fournir un accès à tous les groupes	N/A	True	0.0.0.0/0

Comportement obtenu

- Le groupe de développement peut accéder à `10.0.0.0/16`, sauf pour l'hôte unique `10.0.2.119/32`.
- Le groupe de gestionnaires peut accéder à l'Internet public, `192.168.0.0/24`, et à un hôte unique (`10.0.2.119/32`) au sein du réseau `10.0.0.0/16`, mais n'a accès ni à `172.16.0.0/24` ni à aucun des hôtes restants du réseau `10.0.0.0/16`.
- Le groupe d'ingénierie peut accéder à l'Internet public, `172.16.0.0/24`, et à `172.16.0.128/25`.
- Tout autre groupe d'utilisateurs, par exemple le « groupe d'administrateurs », peut accéder à l'Internet public, mais à aucun des autres réseaux de destination définis dans les autres règles.

Listes de révocation des certificats de client

Vous pouvez utiliser les listes de révocation de certificats clients pour révoquer l'accès à un point de terminaison Client VPN pour des certificats de client spécifiques.

> **Note**
>
> Pour plus d'informations sur la génération de certificats et de clés de serveur et de client, consultez Authentification mutuelle

Pour plus d'informations sur le nombre d'entrées que vous pouvez ajouter à une liste de révocation de certificats clients, consultez Quotas Client VPN.

Table des matières

Générer une liste de révocation des certificats de client

Linux/macOS

Dans la procédure suivante, vous générez une liste de révocation des certificats de client par l'intermédiaire de l'utilitaire de ligne de commande OpenVPN easy-rsa.

Pour générer une liste de révocation des certificats de client via OpenVPN easy-rsa

1. Connectez-vous au serveur hébergeant l'installation easy-rsa utilisée pour générer le certificat.
2. Accédez au dossier `easy-rsa/easyrsa3` de votre référentiel local.

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

3. Révoquez le certificat de client et générez la liste de révocation du client.

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

Tapez `yes` lorsque vous y êtes invité.

Windows

La procédure suivante utilise le logiciel OpenVPN pour générer une liste de révocation de clients. Elle suppose que vous avez suivi les étapes d'utilisation du logiciel OpenVPN pour générer les certificats et clés client et serveur.

Pour générer une liste de révocation des certificats de client à l'aide d'EasyRSA version 3.x.x

1. Ouvrez une invite de commande et accédez au répertoire EasyRSA-3.x.x, en fonction de son emplacement d'installation sur votre système.

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

2. Exécutez le fichier « EasyRSA-Start.bat » pour démarrer le shell EasyRSA.

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

3. Dans le shell EasyRSA, révoquez le certificat client.

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

4. Saisissez « Yes » lorsque vous y êtes invité.
5. Générez la liste de révocation du client.

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

6. La liste de révocation du client sera créée à l'emplacement suivant :

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

Pour générer une liste de révocation des certificats de client à l'aide des précédentes versions d'EasyRSA

1. Ouvrez une invite de commande et accédez au répertoire OpenVPN.

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

2. Exécutez le fichier `vars.bat`.

```
C:\> vars
```

3. Révoquez le certificat de client et générez la liste de révocation du client.

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

Importer une liste de révocation des certificats de client

Vous devez disposer d'un fichier de liste de révocation de certificats de client à importer. Pour plus d'informations sur la création d'une liste de révocation des certificats de client, consultez Générer une liste de révocation des certificats de client.

Vous pouvez importer une liste de révocation des certificats de client à l'aide de la console et de la AWS CLI.

Pour importer une liste de révocation des certificats de client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN pour lequel importer la liste de révocation des certificats de client.
4. Choisissez Actions, puis Import Client Certificate CRL (Importer une liste de révocation des certificats de client).
5. Pour Certificate Révocation List (Liste de révocation des certificats), saisissez le contenu du fichier de liste de révocation des certificats de client, puis choisissez Import client certificate CRL (Importer une CRL de certificat client).

Pour importer une liste de révocation des certificats de client (AWS CLI)

Utilisez la commande import-client-vpn-client-certificate-revocation-list.

```
$ 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
```

Exporter une liste de révocation des certificats de client

Vous pouvez exporter des listes de révocation des certificats de client à l'aide de la console et de la AWS CLI.

Pour exporter une liste de révocation des certificats de client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.

3. Sélectionnez le point de terminaison Client VPN pour lequel exporter la liste de révocation des certificats de client.
4. Choisissez Actions, Export Client Certificate CRL (Exporter une liste de révocation des certificats de client), puis choisissez Export Client Certificate CRL (Exporter un CRL de certificat client).

Pour exporter une liste de révocation des certificats de client (AWS CLI)

Utilisez la commande export-client-vpn-client-certificate-revocation-list.

Connexions client

Les connexions sont des sessions VPN qui ont été établies par des clients. Une connexion est établie lorsqu'un client se connecte avec succès à un point de terminaison Client VPN.

Table des matières

Afficher les connexions client

Vous pouvez afficher les connexions client à l'aide de la console et de la AWS CLI. Les informations de connexion incluent l'adresse IP attribuée à partir de la plage CIDR client.

Pour afficher les connexions client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN pour lequel vous souhaitez afficher les connexions client.
4. Choisissez l'onglet Connections (Connexions). L'onglet Connections (Connexions) répertorie toutes les connexions client actives et interrompues.

Pour afficher les connexions client (AWS CLI)

Utilisez la commande describe-client-vpn-connections.

Mettre fin à une connexion client

Lorsque vous arrêtez une connexion client, la session VPN prend fin.

Vous pouvez arrêter des connexions client à l'aide de la console et de la AWS CLI.

Pour arrêter une connexion client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN auquel le client est connecté et choisissez Connections (Connexions).
4. Sélectionnez la connexion à arrêter, choisissez Terminate Connection (Arrêter une connexion), puis choisissez Terminate Connection (Arrêter une connexion).

Pour arrêter une connexion client (AWS CLI)

Utilisez la commande terminate-client-vpn-connections.

Bannière de connexion client

AWS Client VPN permet d'afficher une bannière texte sur des applications de bureau Client VPN fournies par AWS lorsqu'une session VPN est établie. Vous pouvez définir le contenu de la bannière texte de manière à ce qu'il réponde à vos besoins réglementaires et de conformité. Un maximum de 1 400 caractères codés UTF-8 peuvent être utilisés.

> **Note**
>
> Lorsqu'une bannière de connexion client a été activée, elle s'affiche uniquement sur les nouvelles sessions VPN. Les sessions VPN existantes ne sont pas interrompues, mais la bannière s'affiche lorsqu'une session existante est rétablie.

Consultez Notes de mise à jour pour le client fourni par AWSdans le Guide de l'utilisateur AWS Client VPN pour plus de détails sur les applications clientes de bureau.

Table des matières

Configurer une bannière de connexion client lors de la création d'un point de terminaison Client VPN

Pour obtenir des étapes détaillées sur l'activation d'une bannière de connexion client lors de la création d'un point de terminaison Client VPN, consultez Créer un point de terminaison VPN Client.

Configurer une bannière de connexion client pour un point de terminaison Client VPN existant

Suivez les étapes suivantes afin de configurer une bannière de connexion client pour un point de terminaison Client VPN existant.

Activer la bannière de connexion client sur un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez modifier, choisissez Actions, puis Modify Client VPN Endpoint (Modifier le point de terminaison VPN Client).
4. Faites défiler la page jusqu'à la section Other parameters (Autres paramètres).
5. Activez Enable client login banner (Activer la bannière de connexion client).
6. Pour Client Login Banner Text (Texte de la bannière de connexion client), saisissez le texte qui sera affiché dans une bannière sur les clients fournis par AWS lorsqu'une session VPN sera établie. Utilisez uniquement des caractères codés UTF-8. Un maximum de 1 400 caractères est autorisé.
7. Choisir Modifiy Client VPN endpoint (Modifier le point de terminaison VPN client).

Activer la bannière de connexion client sur un point de terminaison Client VPN (AWS CLI)

Utilisez la commande modify-client-vpn-endpoint.

Désactiver une bannière de connexion client pour un point de terminaison Client VPN existant

Suivez les étapes suivantes afin de désactiver une bannière de connexion client pour un point de terminaison Client VPN existant.

Désactiver la bannière de connexion client sur un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez modifier, choisissez Actions, puis Modify Client VPN endpoint (Modifier le point de terminaison VPN Client).
4. Faites défiler la page jusqu'à la section Other parameters (Autres paramètres).
5. Désactivez Enable client login banner? (Activer la bannière de connexion client ?).
6. Choisissez Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Désactiver la bannière de connexion client sur un point de terminaison VPN client (AWS CLI)

Utilisez la commande modify-client-vpn-endpoint.

Modifier le texte de bannière existant sur un point de terminaison Client VPN

Suivez les étapes suivantes pour modifier le texte existant sur une bannière de connexion client.

Modifier le texte de bannière existant sur un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez modifier, choisissez Actions, puis Modify Client VPN point de terminaison (Modifier le point de terminaison VPN client).
4. Pour Enable client login banner (Activer la bannière de connexion client ?), vérifiez qu'elle est activée.
5. Pour Client login banner text (Texte de la bannière de connexion client), remplacez le texte existant par le texte que vous souhaitez afficher dans une bannière sur les clients fournis par

AWS lorsqu'une session VPN sera établie. Utilisez uniquement des caractères codés UTF-8 et un maximum de 1 400 caractères.

6. Choisissez Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Modifier la bannière de connexion client sur un point de terminaison Client VPN (AWS CLI)

Utilisez la commande modify-client-vpn-endpoint.

Afficher la bannière de connexion actuellement configurée

Procédez comme suit pour afficher une bannière de connexion actuellement configurée.

Afficher la bannière de connexion actuelle pour un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez afficher.
4. Vérifiez que l'onglet Summary (Récapitulatif) est sélectionné.
5. Affichez le texte de la bannière de connexion actuellement configurée à côté de Client login banner text (Texte de la bannière de connexion client).

Afficher la bannière de connexion actuellement configurée pour un point de terminaison Client VPN (AWS CLI)

Utilisez la commande describe-client-vpn-endpoints.

Points de terminaison VPN Client

Toutes les sessions VPN Client sont résiliés au point de terminaison VPN Client. Vous configurez le point de terminaison VPN Client pour gérer et contrôler toutes les sessions VPN client.

Table des matières

Créer un point de terminaison VPN Client

Créez un point de terminaison VPN Client pour permettre à vos clients d'établir une session VPN.

Le VPN Client doit être créé dans le même AWS compte que celui dans lequel le réseau cible est alloué.

Prérequis

Avant de commencer, veillez à effectuer les opérations suivantes :

- Passez en revue les règles et les limitations dans Règles et bonnes pratiques de AWS Client VPN.
- Générez le certificat du serveur et, si nécessaire, le certificat du client. Pour plus d'informations, veuillez consulter . Authentification client.

Pour créer un point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Client VPN Endpoints (Points de terminaison Client VPN), puis choisissez Create Client VPN Endpoint (Créer un point de terminaison Client VPN).
3. (Facultatif) Fournissez une balise de nom et une description pour le point de terminaison Client VPN.
4. Pour Client IPv4 CIDR (CIDR IPv4 client), spécifiez une plage d'adresses IP, en notation CIDR, à partir de laquelle attribuer des adresses IP client. Par exemple, `10.0.0.0/22`.

   > **Note**
   >
   > La plage d'adresses ne peut pas chevaucher la plage d'adresses du réseau cible, la plage d'adresses VPC ou les routes qui seront associées au point de terminaison VPN client. La plage d'adresses du client doit être au minimum /22 et ne doit pas dépasser la taille de bloc CIDR /12. Vous ne pouvez pas modifier la plage d'adresses client après avoir créé le point de terminaison VPN client.

5. Pour ARN du certificat du serveur), spécifiez l'ARN du certificat TLS que le serveur devra utiliser. Les clients utilisent le certificat de serveur pour authentifier le point de terminaison VPN Client auquel ils se connectent.

> **Note**
>
> Le certificat de serveur doit être présent dansAWS Certificate Manager (ACM) dans la région où vous créez le point de terminaison VPN Client. Le certificat peut être provisionné avec ACM ou importé dans ACM.

6. Spécifiez la méthode d'authentification à utiliser pour authentifier les clients lorsqu'ils établissent une connexion VPN. Vous devez sélectionner une méthode d'authentification.

   - Pour utiliser l'authentification basée sur l'utilisateur, sélectionnez Utiliser l'authentification basée sur l'utilisateur, puis choisissez l'une des options suivantes :
     - Authentification Active Directory : choisissez cette option pour l'authentification Active Directory. Pour le répertoire ID, spécifiez l'ID d'Active Directory à utiliser.
     - Authentification fédérée : choisissez cette option pour l'authentification fédérée basée sur SAML.

       Pour l'ARN du fournisseur SAML, spécifiez l'ARN du fournisseur d'identité SAML IAM.

       (Facultatif) Pour ARN du fournisseur SAML en libre-service, spécifiez l'ARN du fournisseur d'identité SAML IAM que vous avez créé pour prendre en charge le portail en libre-service, le cas échéant.
   - Pour utiliser une authentification de certificat mutuelle, sélectionnez Utiliser une authentification mutuelle, puis pour ARN du certificat client, spécifiez l'ARN du certificat client alloué dans AWS Certificate Manager (ACM).

   > **Note**
   >
   > Si les certificats du serveur et du client ont été émis par la même autorité de certification (CA), vous pouvez utiliser l'ARN du certificat du serveur pour le serveur et le client. Si le certificat client a été émis par une autre autorité de certification (CA), l'ARN du certificat client doit être spécifié.

7. (Facultatif) Pour la journalisation des connexions, spécifiez si vous souhaitez enregistrer les données relatives aux connexions des clients à l'aide d'Amazon CloudWatch Logs. Activez Enable log details on client connections (Activer les détails du journal sur les connexions clientes). Pour Nom du groupe de CloudWatch journaux, entrez le nom du groupe de journaux à

utiliser. Pour le nom du flux de journal des CloudWatch journaux, entrez le nom du flux de journal à utiliser ou laissez cette option vide pour que nous puissions créer un flux de journal pour vous.

8. (Facultatif) Pour le gestionnaire de connexion client, activez Enable client connect handler (Activer le gestionnaire de connexion client) pour exécuter un code personnalisé qui autorise ou refuse une nouvelle connexion au point de terminaison VPN client. Pour le gestionnaire de connexion client ARN, spécifiez le Amazon Resource Name (ARN) de la fonction de type Lambda contenant la logique qui autorise ou rejette les connexions.
9. (Facultatif) Spécifiez les serveurs DNS à utiliser pour la résolution DNS. Pour utiliser des serveurs DNS personnalisés, pour Adresse IP serveur DNS 1 et Adresse IP serveur DNS 2, spécifiez les adresses IP des serveurs DNS à utiliser. Pour utiliser un serveur DNS de VPC, pour les champs Adresse IP serveur DNS 1) ou Adresse IP serveur DNS 2, spécifiez les adresses IP et ajouter l'adresse IP du serveur DNS VPC.

   > **Note**
   >
   > Assurez-vous que les serveurs DNS peuvent être atteints par les clients.

10. (Facultatif) Par défaut, le point de terminaison VPN client utilise le protocole de transport UDP. Pour utiliser le protocole de transport TCP à la place, pour Protocole de transport, sélectionnez TCP.

    > **Note**
    >
    > UDP offre généralement des performances supérieures à TCP. Vous ne pouvez pas modifier le protocole de transport après avoir créé le point de terminaison VPN Client.

11. (Facultatif) Pour que le point de terminaison soit un point de terminaison de Client VPN à tunnel partagé, sélectionnez Enable split-tunnel (Activer le tunnel partagé). Cette fonctionnalité est désactivée par défaut sur un point de terminaison Client VPN.
12. (Facultatif) Pour le champ ID du VPC, choisir le VPC à associer au point de terminaison VPN Client. Pour le champ ID de groupe de sécurité, choisir un ou plusieurs groupes de sécurité du VPC à appliquer au point de terminaison VPN Client.
13. (Facultatif) Pour le champ Port VPN, choisir le numéro de port VPN. La valeur par défaut est 443.
14. (Facultatif) Pour générer une URL de portail libre-service pour les clients, activez Enable self-service portal (Activer le portail en libre-service).

15. (Facultatif) Pour Session timeout hours (Durée de la session en heures), choisissez la durée maximale de session VPN souhaitée en heures parmi les options disponibles, ou laissez la durée par défaut de 24 heures.
16. (Facultatif) Spécifiez si le texte de la bannière de connexion client doit être activé. Activez Enable client login banner (Activer la bannière de connexion cliente). Ensuite, pour Client Login Banner Text (Texte de la bannière de connexion client), saisissez le texte qui sera affiché dans une bannière sur les clients fournis par AWS lorsqu'une session VPN sera établie. Caractères codés UTF-8 uniquement. 1 400 caractères maximum.
17. Sélectionnez Create Client VPN endpoint (Créer un point de terminaison VPN client).

Après avoir créé le point de terminaison VPN Client, procédez comme suit pour terminer la configuration et permettre aux clients de se connecter :

- L'état initial du point de terminaison VPN Client est `pending-associate`. Les clients peuvent uniquement se connecter au point de terminaison VPN Client une fois que vous avez associé le premier réseau cible.
- Créez une règle d'autorisation de manière à spécifier les clients qui ont accès au réseau.
- Télécharger et préparez le fichier de configuration du point de terminaison VPN Client à distribuer à vos clients.
- Demandez à vos clients d'utiliser le client AWS fourni par ou une autre application cliente OpenVPN pour se connecter au point de terminaison VPN Client. Pour plus d’informations, consultez le Guide de l’utilisateur AWS Client VPN.

Pour créer un point de terminaison VPN Client (AWS CLI)

Utilisez la commande create-client-vpn-endpoint.

Modifier un point de terminaison VPN Client

Après la création d'un VPN Client, vous pouvez modifier l'un des paramètres suivants :

- La description
- Le certificat du serveur
- Les options de journalisation de la connexion client
- L'option du gestionnaire de connexion du client

- Les serveurs DNS
- L'option de tunnel partagé
- Les routages (lors de l'utilisation de l'option de tunnel partagé)
- La liste de révocation de certificats (CRL)
- Règles d'autorisation
- Les associations de VPC et de groupes de sécurité
- Le numéro de port VPN
- L'option de portail libre-service
- Durée maximale de la session VPN
- Activer ou désactiver le texte de la bannière de connexion client
- Texte de la bannière de connexion client

> **Note**
>
> Les modifications apportées aux points de terminaison Client VPN, y compris les modifications apportées à la liste de révocation de certificats (CRL), prendront effet jusqu'à 4 heures après l'acceptation d'une demande par le service Client VPN.
> Vous ne pouvez pas modifier la plage CIDR IPv4 du client, les options d'authentification, le certification du client ou le protocole de transport après la création du point de terminaison VPN Client.

Lorsque vous modifiez l'un des paramètres suivants sur un point de terminaison VPN Client, la connexion se réinitialise :

- Le certificat du serveur
- Les serveurs DNS
- L'option de tunnel partagé (activation ou désactivation du support)
- Les routages (lorsque vous utilisez l'option de tunnel partagé)
- La liste de révocation de certificats (CRL)
- Règles d'autorisation
- Le numéro de port VPN

Vous pouvez modifier un point de terminaison VPN Client à l'aide de la console ou de la AWS CLI.

Pour modifier un point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client à modifier, choisir Actions, puis choisir Modify Client VPN endpoint (Modifier le point de terminaison VPN client).
4. Dans le champ Description, saisir une brève description pour le point de terminaison VPN Client.
5. Pour ARN du certificat du serveur), spécifiez l'ARN du certificat TLS que le serveur devra utiliser. Les clients utilisent le certificat de serveur pour authentifier le point de terminaison VPN Client auquel ils se connectent.

   > **Note**
   >
   > Le certificat de serveur doit être présent dansAWS Certificate Manager (ACM) dans la région où vous créez le point de terminaison VPN Client. Le certificat peut être provisionné avec ACM ou importé dans ACM.

6. Spécifiez si vous souhaitez enregistrer les données relatives aux connexions des clients à l'aide d'Amazon CloudWatch Logs. Pour Enable log details on client connections (Activer les détails de journalisation sur les connexions client), effectuez l'une des actions suivantes :

   - Pour activer la journalisation de la connexion client, choisissez Enable log details on client connections (Activer les détails du journal sur les connexions client). Pour Nom du groupe de CloudWatch journaux, sélectionnez le nom du groupe de journaux à utiliser. Pour le nom du flux de journal des CloudWatch journaux, sélectionnez le nom du flux de journal à utiliser ou laissez cette option vide pour nous permettre de créer un flux de journal pour vous.
   - Pour désactiver la journalisation de la connexion client, désactivez Enable log details on client connections (Activer les détails du journal sur les connexions client).

7. Pour Client connect handler (Gestionnaire de connexions client), pour activer le Gestionnaire de connexions client, activez Enable Client Connect Handler (Activer le gestionnaire de connexions client). Pour le gestionnaire de connexion client ARN, spécifiez le Amazon Resource Name (ARN) de la fonction de type Lambda contenant la logique qui autorise ou rejette les connexions.
8. Activez ou désactivez Enable DNS servers (Activer les serveurs DNS). Pour utiliser des serveurs DNS personnalisés, pour Adresse IP serveur DNS 1 et Adresse IP serveur DNS 2, spécifiez les adresses IP des serveurs DNS à utiliser. Pour utiliser un serveur DNS de VPC, pour les champs

Adresse IP serveur DNS 1) ou Adresse IP serveur DNS 2, spécifiez les adresses IP et ajouter l'adresse IP du serveur DNS VPC.

> **Note**
>
> Assurez-vous que les serveurs DNS peuvent être atteints par les clients.

9. Activez ou désactivez Enable split-tunnel (Activer le tunnel partagé). Cette fonctionnalité est désactivée par défaut sur un point de terminaison VPN.
10. Pour le champ VPC ID) (ID du VPC, choisissez le VPC à associer au point de terminaison VPN client. Pour le champ ID de groupe de sécurité, choisir un ou plusieurs groupes de sécurité du VPC à appliquer au point de terminaison VPN Client.
11. Pour le champ Port VPN, choisissez le numéro de port VPN. La valeur par défaut est 443.
12. Pour générer une URL de portail libre-service pour les clients, choisissez Enable self-service portal (Activer le portail en libre-service).
13. Pour Session timeout hours (Durée de la session en heures), choisissez la durée maximale de session VPN souhaitée en heures parmi les options disponibles, ou laissez la durée par défaut de 24 heures.
14. Activez ou désactivez Enable client login banner (Activer la bannière de connexion client). Si vous souhaitez utiliser le texte de la bannière de connexion client, saisissez le texte qui sera affiché dans une bannière sur les clients fournis par AWS lorsqu'une session VPN sera établie. Caractères codés UTF-8 uniquement. 1 400 caractères maximum.
15. Choisissez Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Pour modifier un point de terminaison VPN Client (AWS CLI)

Utilisez la commande modify-client-vpn-endpoint.

Afficher les points de terminaison VPN Client

Vous pouvez afficher des informations sur les points de terminaison VPN Client à l'aide de la console ou de la AWS CLI.

Pour afficher les points de terminaison VPN client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le panneau de navigation, choisissez Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client à afficher.
4. Utilisez les onglets Details (Détails), Target network associations (Associations de réseau cible), Security groups (Groupes de sécurité), Authorization rules (Règles d'autorisation), Route table (Table de routage), Connections (Connexions) et Tags (Balises) pour afficher les informations sur les points de terminaison VPN client existants.

   Vous pouvez également utiliser des filtres pour affiner votre recherche.

Pour afficher les points de terminaison VPN client (AWS CLI)

Utilisez la commande describe-client-vpn-endpoints.

Supprimer un point de terminaison VPN Client

Vous devrez dissocier tous les réseaux cibles associés avant de pouvoir supprimer un point de terminaison VPN client. Lorsque vous supprimez un point de terminaison VPN Client, son état devient `deleting` et les clients ne peuvent plus s'y connecter.

Vous pouvez supprimer un point de terminaison VPN Client à l'aide de la console ou de la AWS CLI.

Pour supprimer un point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client à supprimer. Choisissez Actions, Delete Client VPN endpoint (Supprimer le point de terminaison VPN client).
4. Entrez delete dans la fenêtre de confirmation, puis choisissez Delete (Supprimer).

Supprimer un point de terminaison VPN Client (AWS CLI)

Utilisez la commande delete-client-vpn-endpoint.

Utilisation des journaux de connexion

Vous pouvez activer la journalisation des connexions pour un point de terminaison Client VPN nouveau ou existant et commencer à capturer les journaux de connexion.

Avant de commencer, vous devez disposer d'un groupe de journaux CloudWatch Logs dans votre compte. Pour plus d'informations, consultez Gestion des groupes de journaux et des flux de journaux dans le Guide de l'utilisateur Amazon CloudWatch Logs. Des frais s'appliquent pour l'utilisation de CloudWatch Logs. Pour de plus amples informations, consultez Tarification Amazon CloudWatch.

Lorsque vous activez la journalisation des connexions, vous pouvez spécifier le nom d'un flux de journaux dans le groupe de journaux. Si vous ne spécifiez pas de flux de journal, le service Client VPN en crée un pour vous.

Activer la journalisation des connexions pour un nouveau point de terminaison Client VPN

Vous pouvez activer la journalisation des connexions lorsque vous créez un point de terminaison Client VPN à l'aide de la console ou de la ligne de commande.

Pour activer la journalisation des connexions pour un nouveau point de terminaison Client VPN à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Client VPN Endpoints (Points de terminaison Client VPN), puis choisissez Create Client VPN endpoint (Créer un point de terminaison VPN client).
3. Remplissez les options jusqu'à ce que vous atteigniez la section Enregistrement des connexions. Pour plus d'informations sur ces options, consultez Créer un point de terminaison VPN Client.
4. Sous Connection logging (Journalisation des connexions), activez Enable log details on client connections (Activer les détails du journal sur les connexions clientes).
5. Pour le Nom du groupe de journaux CloudWatch Logs, choisissez le nom du groupe de journaux CloudWatch Logs.
6. (Facultatif) Pour Nom du flux de journaux CloudWatch Logs, choisissez le nom du flux de journaux CloudWatch Logs.
7. Sélectionnez Create Client VPN endpoint (Créer un point de terminaison VPN client).

Pour activer la journalisation des connexions pour un nouveau point de terminaison Client VPN à l'aide de la AWS CLI

Utilisez la commande create-client-vpn-endpoint et spécifiez le paramètre `--connection-log-options`. Vous pouvez spécifier les informations des journaux de connexion au format JSON, comme illustré dans l'exemple suivant.

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

Activer la journalisation des connexions pour un point de terminaison Client VPN existant

Vous pouvez activer la journalisation des connexions pour un point de terminaison Client VPN existant à l'aide de la console ou de la ligne de commande.

Pour activer la journalisation des connexions pour un point de terminaison Client VPN existant à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN, choisissez Actions, puis Modify Client VPN endpoint (Modifier le point de terminaison VPN client).
4. Sous Connection loggin (Journalisation des connexions), Activez Enable log details on client connections (Activer les détails du journal sur les connexions clientes).
5. Pour le Nom du groupe de journaux CloudWatch Logs, choisissez le nom du groupe de journaux CloudWatch Logs.
6. (Facultatif) Pour Nom du flux de journaux CloudWatch Logs, choisissez le nom du flux de journaux CloudWatch Logs.
7. Choisir Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Pour activer la journalisation des connexions pour un point de terminaison Client VPN existant à l'aide de la AWS CLI

Utilisez la commande modify-client-vpn-endpoint et spécifiez le paramètre `--connection-log-options`. Vous pouvez spécifier les informations des journaux de connexion au format JSON, comme illustré dans l'exemple suivant.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
```

```
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Afficher les journaux de connexion

Vous pouvez afficher vos journaux de connexion à l'aide de la console CloudWatch Logs.

Pour afficher vos journaux de connexion à l'aide de la console

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, choisissez Groupes de journaux, puis sélectionnez le groupe de journaux contenant vos journaux de connexion.
3. Sélectionnez le flux de journaux pour votre point de terminaison Client VPN.

> **Note**
>
> La colonne Horodatage affiche l'heure à laquelle le journal de connexion a été publié sur CloudWatch Logs, et non l'heure de la connexion.

Pour plus d'informations sur la recherche de données de journaux, consultez Recherche dans des données de journaux au moyen de modèles de filtres dans le Guide de l'utilisateur Amazon CloudWatch Logs.

Désactiver la journalisation de la connexion

Vous pouvez désactiver la journalisation des connexions pour un point de terminaison VPN client à l'aide de la console ou de la ligne de commande. Lorsque vous désactivez la journalisation des connexions, les journaux de connexion existants dans CloudWatch Logs ne sont pas supprimés.

Pour désactiver l'enregistrement des connexions à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client, choisissez Actions, puis Modify Client VPN endpoint (Modifier le point de terminaison VPN client).
4. Sous Connection logging (Journalisation des connexions), désactivez Enable log details on client connections (Activer les détails du journal sur les connexions clientes).

5. Choisir Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Pour désactiver les journaux à l'aide de la console

Utilisez la commande modify-client-vpn-endpoint et spécifiez le paramètre `--connection-log-options`. Assurez-vous que cette valeur `Enabled` est définie sur `false`.

Exporter et configurer le fichier de configuration du client

Le fichier de configuration de point de terminaison VPN Client est le fichier que les clients (utilisateurs) utilisent pour établir une connexion VPN avec le point de terminaison VPN Client. Vous devez télécharger (exporter) ce fichier et le distribuer à tous les clients qui ont besoin d'accéder au VPN. Sinon, si vous avez activé le portail en libre-service pour votre point de terminaison VPN Client, les clients peuvent se connecter au portail et télécharger le fichier de configuration eux-mêmes. Pour plus d'informations, veuillez consulter . Accéder au portail en libre-service.

Si votre point de terminaison VPN Client utilise l'authentification mutuelle, vous devez ajouter le certificat du client et la clé privée du client au fichier de configuration .ovpn que vous téléchargez. Une fois que vous avez ajouté ces informations, les clients peuvent importer le fichier .ovpn dans le logiciel client OpenVPN.

> **Important**
>
> Si vous n'ajoutez pas le certificat du client et les informations de clé privée du client au fichier, les clients qui s'authentifient via une authentification mutuelle ne peuvent pas se connecter au point de terminaison VPN Client.

Par défaut, l'option « remote-random-hostname » dans la configuration du client OpenVPN active le DNS générique. le DNS à caractère de remplacement étant activé, le client ne met pas en cache l'adresse IP du point de terminaison et vous ne pourrez pas faire un ping au nom DNS du point de terminaison.

Si votre point de terminaison VPN Client utilise l'authentification Active Directory et si vous activez l'authentification multi-facteur (MFA) sur votre répertoire après avoir distribué le fichier de configuration client, vous devez télécharger un nouveau fichier et le redistribuer à vos clients. Les clients ne peuvent pas utiliser le fichier de configuration précédent pour se connecter au point de terminaison VPN Client.

Exporter le fichier de configuration du client

Vous pouvez exporter la configuration du client à l'aide de la console ou de la AWS CLI.

Pour exporter la configuration du client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client pour lequel télécharger la configuration du client et choisir Télécharger la configuration du client.

Pour exporter la configuration du client (AWS CLI)

Utilisez la commande export-client-vpn-client-configuration et spécifiez le nom du fichier de sortie.

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

Ajouter le certificat du client et les informations de clé (authentification mutuelle)

Si votre point de terminaison VPN Client utilise l'authentification mutuelle, vous devez ajouter le certificat du client et la clé privée du client au fichier de configuration .ovpn que vous téléchargez.

Vous ne pouvez pas modifier le certificat du client lorsque vous utilisez l'authentification mutuelle.

Pour ajouter le certificat du client et les informations du clé (authentification mutuelle)

Vous pouvez utiliser l'une des options suivantes.

(Option 1) Distribuer le certificat et la clé du client aux clients, ainsi que le fichier de configuration du point de terminaison VPN Client. Dans ce cas, spécifiez le chemin d'accès au certificat et à la clé dans le fichier de configuration. Ouvrez le fichier de configuration avec l'éditeur de texte de votre choix et ajoutez le texte suivant à la fin du fichier. Remplacez */path/* par l'emplacement du certificat et de la clé client (l'emplacement concerne le client qui se connecte au point de terminaison).

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

(Option 2) Ajoutez le contenu du certificat de client entre les balises <cert></cert> et le contenu de la clé privée entre les balises <key></key> dans le fichier de configuration. Si vous choisissez cette option, vous ne distribuez que le fichier de configuration à vos clients.

Si vous avez généré des certificats client et des clés distincts pour chaque utilisateur qui se connectera au point de terminaison VPN Client, répétez cette étape pour chacun d'eux.

Voici un exemple du format d'un fichier de configuration VPN Client qui inclut le certificat client et la clé.

```
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
```

Acheminements

Chaque point de terminaison du VPN client a une table de routage qui décrit la les acheminements réseau de destination disponibles. Chaque acheminement dans la table de routage détermine où le trafic réseau est dirigé. Vous devez configurer des règles d'autorisation pour chaque acheminement de point de terminaison VPN Client pour spécifier les clients qui ont accès au réseau de destination.

Lorsque vous associez un sous-réseau d'un VPC à un point de terminaison VPN Client, un acheminement du VPC est automatiquement ajoutée à la table de routage du point de terminaison VPN Client. Pour activer l'accès à d'autres réseaux, tels que des VPC appairés, des réseaux sur site, le réseau local (pour permettre aux clients de communiquer entre eux) ou Internet, vous devez ajouter manuellement un acheminement vers la table de routage du point de terminaison VPN Client.

> **Note**
>
> Si vous associez plusieurs sous-réseaux au point de terminaison VPN Client, vous devez vous assurer de créer un acheminement pour chaque sous-réseau, comme décrit ici L'accès à un VPC appairé, à Amazon S3 ou à Internet est intermittent. Chaque sous-réseau associé doit comporter un ensemble d'acheminements identique.

Table des matières

Considérations relatives au tunnel partagé sur les points de terminaison VPN Client

Lorsque vous utilisez le tunnel partagé sur un point de terminaison VPN Client, toutes les routes qui se trouvent dans les tables de routage VPN Client sont ajoutées à la table de routage client lorsque le VPN est établi. Si vous ajoutez un acheminement après l'établissement du VPN, vous devez réinitialiser la connexion afin que la nouvelle route soit envoyée au client.

Nous vous recommandons de prendre en compte le nombre d’acheminement que le périphérique client peut gérer avant de modifier la table de routage des points de terminaison VPN Client.

Création d'un acheminement de point de terminaison

Lorsque vous créez un acheminement, vous spécifiez la manière dont le trafic vers le réseau de destination doit être dirigé.

Pour autoriser les clients d'accéder à Internet, ajouter un acheminement de destination `0.0.0.0/0`.

Vous pouvez ajouter des acheminements vers un point de terminaison VPN Client à l'aide de la console et de AWS CLI.

Pour créer un acheminement de point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN client auquel vous souhaitez ajouter la route, choisissez Route table (Table de routage), puis Create route (Créer la route).
4. Pour Destination de l'acheminement, spécifiez la plage CIDR IPv4 pour le réseau de destination. Par exemple :

   - Pour ajouter une route pour le VPC du point de terminaison VPN client, saisissez la plage d'adresses CIDR IPv4 du VPC.
   - Pour ajouter un acheminement pour l'accès à Internet, saisir `0.0.0.0/0`.
   - Pour ajouter un acheminement pour un VPC appairé, saisissez la plage d'adresses CIDR IPv4 du VPC appairé.
   - Pour ajouter un acheminement pour un réseau sur site, saisir la plage CIDR IPv4 de la connexion AWS Site-to-Site VPN.
5. Pour Subnet ID for target network association (ID de sous-réseau de l'association réseau cible), sélectionnez le sous-réseau associé au point de terminaison VPN client.

   Sinon, si vous ajoutez une route pour le réseau du point de terminaison VPN client local, sélectionnez `local`.
6. Pour Description, entrez une brève description de la route.
7. Choisissez Create Route (Créer un itinéraire).

Pour créer un acheminement de point de terminaison VPN Client (AWS CLI)

Utilisez la commande create-client-vpn-route.

Affichage d'acheminements de points de terminaison

Vous pouvez afficher les acheminements d'un point de terminaison VPN Client spécifique à l'aide de la console ou de AWS CLI.

Pour afficher les acheminements de point de terminaison VPN Client (console)

1. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
2. Sélectionnez le point de terminaison VPN Client pour lequel vous souhaitez afficher les acheminements, puis choisissez Route table (Table de routage.

Pour afficher les acheminements de point de terminaison VPN Client (AWS CLI)

Utilisez la commande describe-client-vpn-routes.

Suppression d'un acheminement de point de terminaison

Vous pouvez uniquement supprimer des acheminements que vous avez ajoutées manuellement. Vous ne pouvez pas supprimer les acheminementss ajoutées automatiquement lors de l'association d'un sous-réseau au point de terminaison VPN Client. Pour supprimer les routes qui ont été ajoutées automatiquement, vous devez dissocier le sous-réseau qui a initié leur création à partir du point de terminaison VPN Client.

Vous pouvez supprimer un acheminement d'un point de terminaison VPN Client à l'aide de la console ou de AWS CLI.

Pour supprimer un acheminement de point de terminaison VPN Client (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client à partir duquel vous souhaitez supprimer la route, puis choisissez Route table (Table de routage).
4. Sélectionnez la route à supprimer, choisissez Delete route (Supprimer la route), puis Delete route (Supprimer la route).

Pour supprimer un acheminement de point de terminaison VPN Client (AWS CLI)

Utilisez la commande delete-client-vpn-route.

Réseaux cibles

Un réseau cible est un sous-réseau dans un VPC. Un point de terminaison Client VPN doit avoir au moins un réseau cible pour permettre aux clients de se connecter et d'établir une connexion VPN.

Pour plus d’informations sur les types d'accès que vous pouvez configurer (par exemple, permettre à vos clients d'accéder à Internet), consultez Scénarios et exemples pour AWS Client VPN.

Table des matières

Associer un réseau cible à un point de terminaison Client VPN.

Vous pouvez associer un ou plusieurs réseaux cibles (sous-réseaux) à un point de terminaison Client VPN.

Les règles suivantes s'appliquent :

- Le sous-réseau doit avoir un bloc d'adresse CIDR avec au moins un masque de bits /27, par exemple 10.0.0.0/27. Le sous-réseau doit également disposer d'au moins 20 adresses IP disponibles à tout moment.
- Le bloc d'adresse CIDR du sous-réseau ne peut pas chevaucher la plage CIDR client du point de terminaison Client VPN.
- Si vous associez plusieurs sous-réseaux à un point de terminaison Client VPN, chaque sous-réseau doit se trouver dans une zone de disponibilité différente. Nous vous recommandons d'associer au moins deux sous-réseaux pour fournir la redondance de zone de disponibilité.
- Si vous avez spécifié un VPC lorsque vous avez créé le point de terminaison Client VPN, le sous-réseau doit se trouver dans le même VPC. Si vous n'avez pas encore associé un VPC au point de terminaison Client VPN, vous pouvez choisir n'importe quel sous-réseau dans n'importe quel VPC.

  Toutes les futures associations de sous-réseau doivent se trouver dans le même VPC. Pour associer un sous-réseau à partir d'un autre VPC, vous devez d'abord modifier le point de terminaison Client VPN et modifier le VPC qui lui est associé. Pour de plus amples informations, veuillez consulter Modifier un point de terminaison VPN Client.

Lorsque vous associez un sous-réseau à un point de terminaison Client VPN, nous ajoutons automatiquement la route locale du VPC dans lequel le sous-réseau associé est alloué à la table de routage du point de terminaison Client VPN.

> **Note**
>
> Après l'association de vos réseaux cibles, lorsque vous ajoutez ou supprimez des CIDR supplémentaires à votre VPC connecté, vous devez effectuer l'une des opérations suivantes pour mettre à jour la route locale de la table de routage du point de terminaison Client VPN :
>
> - Dissociez votre point de terminaison Client VPN du réseau cible, puis associez-le à nouveau.
> - Ajoutez manuellement la route vers la table de routage du point de terminaison Client VPN client ou supprimez-la.

Après avoir associé le premier sous-réseau au point de terminaison Client VPN, l'état du point de terminaison Client VPN passe de `pending-associate` à `available` et les clients sont en mesure d'établir une connexion VPN.

Pour associer un réseau cible à un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN auquel associer le réseau cible, choisissez Target network associations (Associations du réseau cible), puis choisissez Associate target network (Associer le réseau cible).
4. Pour VPC, choisissez le VPC dans lequel le sous-réseau est situé. Si vous avez spécifié un VPC lorsque vous avez créé le point de terminaison Client VPN ou si vous disposez d'associations de sous-réseau précédentes, il doit se trouver dans le même VPC.
5. Pour Choose a subnet to associate (Choisir un sous-réseau à associer), choisissez le sous-réseau à associer au point de terminaison Client VPN.
6. Choisissez Associate target network (Associer le réseau cible).

Pour associer un réseau cible à un point de terminaison Client VPN (AWS CLI)

Utilisez la commande associate-client-vpn-target-network.

Application d'un groupe de sécurité à un réseau cible

Lorsque vous créez un point de terminaison Client VPN, vous pouvez spécifier les groupes de sécurité à appliquer au réseau cible. Lorsque vous associez le premier réseau cible à un point de terminaison Client VPN, nous appliquons automatiquement le groupe de sécurité par défaut du VPC dans lequel le sous-réseau associé est situé. Pour de plus amples informations, veuillez consulter Groupes de sécurité.

Vous pouvez modifier les groupes de sécurité du point de terminaison Client VPN. Les règles de groupe de sécurité dont vous avez besoin dépendent du type d'accès VPN que vous souhaitez configurer. Pour de plus amples informations, veuillez consulter Scénarios et exemples pour AWS Client VPN.

Pour appliquer un groupe de sécurité à un réseau cible (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN auquel vous souhaitez appliquer les groupes de sécurité.
4. Choisissez Security Groups (Groupes de sécurité), puis choisissez Create security group (Créer un groupe de sécurité).
5. Sélectionnez les groupes de sécurité appropriés dans Security group IDs (ID de groupe de sécurité).
6. Choisissez Apply Security Groups (Appliquer les groupes de sécurité).

Pour appliquer un groupe de sécurité à un réseau cible (AWS CLI)

Utilisez la commande apply-security-groups-to-client-vpn-target-network.

Dissocier un réseau cible d'un point de terminaison Client VPN

Lorsque vous dissociez un réseau cible, les routes qui ont été ajoutées manuellement à la table de routage du point de terminaison Client VPN sont supprimées, ainsi que la route qui a été créée automatiquement lors de l'association du réseau cible (la route locale du VPC). Si vous dissociez tous les réseaux cible d'un point de terminaison Client VPN, les clients ne peuvent plus établir de connexion VPN.

Pour dissocier un réseau cible d'un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN avec lequel le réseau cible est associé et choisissez Target network associations (Associations de réseau cible).
4. Sélectionnez le réseau cible à dissocier, choisissez Disassociate (Dissocier), puis choisissez Disassociate target network (Dissocier le réseau cible).

Pour dissocier un réseau cible d'un point de terminaison Client VPN (AWS CLI)

Utilisez la commande disassociate-client-vpn-target-network.

Affichage des réseaux cibles

Vous pouvez afficher les cibles associées à un point de terminaison Client VPN à l'aide de la console ou de la AWS CLI.

Pour afficher les réseaux cibles (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison Client VPN et choisissez Target network associations (Associations de réseau cible).

Pour afficher les réseaux cibles à l'aide de la AWS CLI

Utilisez la commande describe-client-vpn-target-networks.

Durée maximale de session VPN

AWS Client VPN propose plusieurs options pour la durée maximale de session VPN. Vous pouvez configurer une durée maximale de session VPN plus courte pour répondre aux exigences de sécurité et de conformité. Par défaut, la durée maximale de session VPN est de 24 heures.

> **Note**
>
> Lorsque la valeur maximale de la durée de session VPN est réduite, les sessions VPN actives antérieures à la nouvelle valeur de durée sont déconnectées.

Consultez Notes de mise à jour pour le client fourni par AWSdans le Guide de l'utilisateur AWS Client VPN pour plus de détails sur les applications clientes de bureau.

Table des matières

Configurer une durée maximale de session VPN lors de la création d'un point de terminaison Client VPN

Pour obtenir des étapes détaillées sur la configuration d'une durée maximale de session VPN lors de la création d'un point de terminaison Client VPN, consultez Créer un point de terminaison VPN Client.

Afficher la durée maximale de session VPN actuelle

Procédez comme suit pour afficher la durée maximale de session VPN actuelle.

Afficher la durée maximale de session VPN actuelle pour un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisir Points de terminaison VPN Client.
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez afficher.
4. Vérifiez que l'onglet Summary (Récapitulatif) est sélectionné.
5. Affichez la durée maximale de session VPN actuelle à côté deSession timeout hours (Durée de la session en heures).

Afficher la durée maximale de session VPN actuelle pour un point de terminaison Client VPN (AWS CLI)

Utilisez la commande describe-client-vpn-endpoints.

Modifier de la durée maximale de session VPN

Procédez comme suit pour modifier une durée maximale de session VPN existante.

Modifier une durée maximale de session VPN existante pour un point de terminaison Client VPN (console)

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Client VPN endpoints (Points de terminaison VPN client).
3. Sélectionnez le point de terminaison VPN Client que vous souhaitez modifier, choisissez Actions, puis Modify Client VPN Endpoint (Modifier le point de terminaison VPN Client).
4. Pour Session timeout hours (Durée de la session en heures), choisissez la durée maximale de session VPN souhaitée en heures.
5. Choisissez Modify Client VPN endpoint (Modifier le point de terminaison VPN client).

Modifier une durée maximale de session VPN existante pour un point de terminaison Client VPN (AWS CLI)

Utilisez la commande modify-client-vpn-endpoint.

Sécurité dans AWS Client VPN

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Client VPN, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le AWSservice que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

AWS Client VPN fait partie du service Amazon VPC. Pour plus d'informations sur la sécurité dans Amazon VPC, consultez Sécurité dans le Guide de l'utilisateur Amazon VPC.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisez Client VPN. Les rubriques suivantes vous montrent comment configurer Client VPN pour répondre à vos objectifs de sécurité et de conformité. Vous découvrirez également comment utiliser d'autres services AWS qui vous permettent de surveiller et de sécuriser vos ressources Client VPN.

Table des matières

Protection des données dans AWS Client VPN

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Client VPN. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour les Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que

le champ Name (Nom). Cela s'applique aussi lorsque vous utilisez Client VPN ou d'autres Services AWS à l'aide de la console, de l'API, d'AWS CLI ou des kits SDK AWS. Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement en transit

AWS Client VPN fournit des connexions sécurisées à partir de n'importe quel emplacement à l'aide du protocole TLS (Transport Layer Security) version 1.2 ou ultérieure.

Confidentialité du trafic inter-réseau

Activation de l'accès inter-réseaux

Vous pouvez permettre aux clients de se connecter à votre VPC et à d'autres réseaux via un point de terminaison Client VPN. Pour plus d'informations et d'exemples, consultez Scénarios et exemples pour AWS Client VPN.

Restriction de l'accès aux réseaux

Vous pouvez configurer votre point de terminaison Client VPN pour restreindre l'accès à certaines ressources spécifiques de votre VPC. Pour l'authentification basée sur l'utilisateur, vous pouvez également restreindre l'accès à des parties de votre réseau, en fonction du groupe d'utilisateurs qui accède au point de terminaison Client VPN. Pour plus d'informations, consultez Restriction de l'accès à votre réseau avec AWS Client VPN.

Authentification des clients

L'authentification est implémentée au niveau du premier point d'entrée dans le cloud AWS. Elle est utilisée pour déterminer si les clients sont autorisés à se connecter au point de terminaison VPN Client. Si l'authentification aboutit, les clients se connectent au point de terminaison VPN Client et établissent une session VPN. Si l'authentification échoue, la connexion est refusée et le client n'est pas autorisé à établir une session VPN.

Le VPN Client offre les types d'authentification client suivants:

- Authentification Active Directory (basée sur l'utilisateur)
- Authentification mutuelle (basée sur un certificat)

- Authentification unique (authentification fédérée basée sur SAML) (basée sur l'utilisateur)

Gestion des identités et des accès pour AWS le Client VPN

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources Client VPN. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Client VPN.

Utilisateur du service – Si vous utilisez le service Client VPN pour accomplir votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctions Client VPN pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Client VPN, consultez Résolution des problèmes liés à l'identité et à l'accès VPN du AWS Client.

Administrateur du service – Si vous êtes le responsable des ressources Client VPN de votre entreprise, vous bénéficiez probablement d'un accès total à Client VPN. Votre responsabilité est de déterminer les fonctionnalités et les ressources Client VPN auxquelles les utilisateurs de votre service

doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Client VPN, veuillez consulter AWS Fonctionnement du Client VPN avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à Client VPN. Pour voir des exemples de politiques Client VPN basées sur l'identité que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour AWS le Client VPN.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir

plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous

vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d’utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d’autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d’un compte différent d’accéder aux ressources de votre compte. Les rôles constituent le principal moyen d’accorder l’accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d’appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d’autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d’accès.
  - Rôle de service : il s’agit d’un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d’effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage

des clés d’accès au sein de l’instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d’instance contient le rôle et permet aux programmes qui s’exécutent sur l’instance EC2 d’obtenir des informations d’identification temporaires. Pour plus d’informations, consultez Utilisation d’un rôle IAM pour accorder des autorisations à des applications s’exécutant sur des instances Amazon EC2 dans le Guide de l’utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d’un utilisateur) dans le Guide de l’utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d’une action, quelle que soit la méthode que vous utilisez pour exécuter l’opération. Par exemple, supposons que vous disposiez d’une politique qui autorise l’action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l’identité

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces

politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser

une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

AWS Fonctionnement du Client VPN avec IAM

Avant d'utiliser IAM pour gérer l'accès à Client VPN, découvrez les fonctions IAM que vous pouvez utiliser avec Client VPN.

Fonctionnalités IAM que vous pouvez utiliser avec le AWS Client VPN

Fonction IAM	Prise en charge de Client VPN
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont le Client VPN et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Client VPN

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Client VPN

Pour voir des exemples de politiques basées sur l'identité Client VPN, veuillez consulter Exemples de politiques basées sur l'identité pour AWS le Client VPN.

Politiques basées sur les ressources dans Client VPN

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions de politique pour Client VPN

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions du Client VPN, consultez la section Actions définies par le AWS Client VPN dans la Référence d'autorisation de service.

Les actions de politique dans Client VPN utilisent le préfixe suivant avant l'action :

```
ec2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples de politiques basées sur l'identité Client VPN, veuillez consulter Exemples de politiques basées sur l'identité pour AWS le Client VPN.

Ressources de politique pour Client VPN

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources VPN du client et de leurs ARN, consultez la section Ressources définies par le VPN AWS client dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS le Client VPN.

Pour voir des exemples de politiques basées sur l'identité Client VPN, veuillez consulter Exemples de politiques basées sur l'identité pour AWS le Client VPN.

Clés de condition de politique pour Client VPN

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition du VPN client, consultez la section Clés de condition AWS du VPN client dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par AWS le Client VPN.

Pour voir des exemples de politiques basées sur l'identité Client VPN, veuillez consulter Exemples de politiques basées sur l'identité pour AWS le Client VPN.

ACL dans Client VPN

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Client VPN

Prise en charge d'ABAC (identifications dans les politiques)	Non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les

étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Utilisation des informations d'identification temporaires avec Client VPN

Prend en charge les informations d’identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d’informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l’utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM.

Autorisations de principal entre services pour Client VPN

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal

appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Client VPN

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'une fonction de service peut altérer la fonctionnalité de Client VPN. Ne modifiez des fonctions du service que quand Client VPN vous le conseille.

Rôles liés à un service pour Client VPN

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS le Client VPN

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources Client VPN. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l’identité IAM à l’aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l’onglet JSON dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par le VPN client, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour le VPN AWS client dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Client VPN dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l’identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d’informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l’utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l’exécution d’une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des

ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "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": "*"
        }
    ]
}
```

Résolution des problèmes liés à l'identité et à l'accès VPN du AWS Client

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Client VPN et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Client VPN
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources VPN de mon Client

Je ne suis pas autorisé à effectuer une action dans Client VPN

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `ec2:`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ec2:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour afin de vous permettre de transmettre un rôle à Client VPN.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans Client VPN. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources VPN de mon Client

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Client VPN prend en charge ces fonctionnalités, consultez AWS Fonctionnement du Client VPN avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation de rôles liés à un service pour Client VPN

AWS Client VPN utilise des rôles AWS Identity and Access Management (IAM) liés aux services. Un rôle lié à un service est un type unique de rôle IAM lié directement à Client VPN. Les rôles liés à un service sont prédéfinis par Client VPN et incluent toutes les autorisations requises par le service pour appeler d'autres services AWS en votre nom.

Rubriques

- Utilisation de rôles pour Client VPN
- Utilisation de rôles pour l'autorisation de connexion

Utilisation de rôles pour Client VPN

AWS Client VPN utilise des rôles AWS Identity and Access Management (IAM) liés aux services. Un rôle lié à un service est un type unique de rôle IAM lié directement à Client VPN. Les rôles liés à un service sont prédéfinis par Client VPN et incluent toutes les autorisations requises par le service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service simplifie la configuration de Client VPN, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Client VPN définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Client VPN peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources Client VPN sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour Client VPN

Client VPN utilise le rôle lié à un service nommé AWSServiceRoleForClientVPN – Autoriser Client VPN pour créer et gérer les ressources liées à vos connexions VPN.

Le rôle lié à un service AWSServiceRoleForClientVPN approuve le service suivant pour assumer le rôle :

- `clientvpn.amazonaws.com`

La politique d'autorisations de rôle nommée ClientVPNServiceRolePolicy permet à Client VPN de réaliser les actions suivantes sur les ressources spécifiées :

- Action : `ec2:CreateNetworkInterface` sur `Resource: "*"`
- Action : `ec2:CreateNetworkInterfacePermission` sur `Resource: "*"`
- Action : `ec2:DescribeSecurityGroups` sur `Resource: "*"`

- Action : `ec2:DescribeVpcs` sur `Resource: "*"`
- Action : `ec2:DescribeSubnets` sur `Resource: "*"`
- Action : `ec2:DescribeInternetGateways` sur `Resource: "*"`
- Action : `ec2:ModifyNetworkInterfaceAttribute` sur `Resource: "*"`
- Action : `ec2:DeleteNetworkInterface` sur `Resource: "*"`
- Action : `ec2:DescribeAccountAttributes` sur `Resource: "*"`
- Action : `ds:AuthorizeApplication` sur `Resource: "*"`
- Action : `ds:DescribeDirectories` sur `Resource: "*"`
- Action : `ds:GetDirectoryLimits` sur `Resource: "*"`
- Action : `ds:UnauthorizeApplication` sur `Resource: "*"`
- Action : `logs:DescribeLogStreams` sur `Resource: "*"`
- Action : `logs:CreateLogStream` sur `Resource: "*"`
- Action : `logs:PutLogEvents` sur `Resource: "*"`
- Action : `logs:DescribeLogGroups` sur `Resource: "*"`
- Action : `acm:GetCertificate` sur `Resource: "*"`
- Action : `acm:DescribeCertificate` sur `Resource: "*"`
- Action : `iam:GetSAMLProvider` sur `Resource: "*"`
- Action : `lambda:GetFunctionConfiguration` sur `Resource: "*"`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d’un rôle lié à un service pour Client VPN

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez le premier point de terminaison Client VPN dans votre compte avec AWS Management Console, AWS CLI ou l’API AWS, Client VPN crée le rôle lié à un service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez le premier point de terminaison Client VPN dans votre compte, Client VPN crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Client VPN

Client VPN ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForClientVPN. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Client VPN

Si vous n'avez plus besoin d'utiliser Client VPN, nous vous recommandons de supprimer le rôle lié à un service AWSServiceRoleForClientVPN.

Vous devez d'abord supprimer les ressources Client VPN associées. Ainsi, vous ne risquez pas de supprimer involontairement l'autorisation d'accéder aux ressources.

Utilisez la console IAM, l'interface de ligne de commande IAM ou l'API IAM pour supprimer les rôles liés à un service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Client VPN

Client VPN prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Utilisation de rôles pour l'autorisation de connexion

AWS Client VPN utilise des rôles AWS Identity and Access Management (IAM) liés aux services. Un rôle lié à un service est un type unique de rôle IAM lié directement à Client VPN. Les rôles liés à un service sont prédéfinis par Client VPN et incluent toutes les autorisations requises par le service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service simplifie la configuration de Client VPN, car vous n’avez pas besoin d’ajouter manuellement les autorisations requises. Client VPN définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Client VPN peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources Client VPN sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour Client VPN

Client VPN utilise le rôle lié à un service nommé AWSServiceRoleForClientVPNConnections – Rôle lié à un service pour les connexions Client VPN.

Le rôle lié à un service AWSServiceRoleForClientVPNConnections approuve les services suivants pour assumer le rôle :

- `clientvpn-connections.amazonaws.com`

La politique d'autorisations de rôle nommée ClientVPNServiceConnectionsRolePolicy permet à Client VPN de réaliser les actions suivantes sur les ressources spécifiées :

- Action : `lambda:InvokeFunction` sur `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d’un rôle lié à un service pour Client VPN

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez le premier point de terminaison Client VPN dans votre compte avec AWS Management Console, AWS CLI ou l’API AWS, Client VPN crée le rôle lié à un service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez le premier point de terminaison Client VPN dans votre compte, Client VPN crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Client VPN

Client VPN ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForClientVPNConnections. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle.

Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Client VPN

Si vous n'avez plus besoin d'utiliser Client VPN, nous vous recommandons de supprimer le rôle lié à un service AWSServiceRoleForClientVPNConnections.

Vous devez d'abord supprimer les ressources Client VPN associées. Ainsi, vous ne risquez pas de supprimer involontairement l'autorisation d'accéder aux ressources.

Utilisez la console IAM, l'interface de ligne de commande IAM ou l'API IAM pour supprimer les rôles liés à un service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Client VPN

Client VPN prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Résilience dans AWS Client VPN

L'infrastructure mondiale d'AWS repose sur des Régions et des zones de disponibilité AWS. Les Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour de plus amples informations sur les Régions et les zones de disponibilité AWS, veuillez consulter Infrastructure mondiale AWS.

Outre l'infrastructure globale d'AWS, AWS Client VPN propose différentes fonctions qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

Plusieurs réseaux cibles pour une haute disponibilité

Vous associez un réseau cible à un point de terminaison Client VPN pour permettre aux clients d'établir des sessions VPN. Les réseaux cibles sont des sous-réseaux dans votre VPC. Chaque sous-réseau que vous associez au point de terminaison Client VPN doit appartenir à une zone de

disponibilité différente. Vous pouvez associer plusieurs sous-réseaux à un point de terminaison Client VPN pour bénéficier d'une haute disponibilité.

Sécurité de l'infrastructure dans AWS Client VPN

En tant que service géré, AWS Client VPN est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous pouvez utiliser les appels d'API publiés par AWS pour accéder à Client VPN via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Bonnes pratiques de sécurité pour AWS Client VPN

AWS Client VPN fournit différentes fonctions de sécurité à prendre en compte lorsque vous développez et implémentez vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Règles d'autorisation

Utilisez des règles d'autorisation pour restreindre les utilisateurs qui peuvent accéder à votre réseau. Pour de plus amples informations, veuillez consulter Règles d'autorisation.

Groupes de sécurité

Utilisez des groupes de sécurité pour contrôler les ressources auxquelles les utilisateurs peuvent accéder dans votre VPC. Pour de plus amples informations, veuillez consulter Groupes de sécurité.

Listes de révocation des certificats de client

Vous pouvez utiliser les listes de révocation de certificats clients pour révoquer l'accès à un point de terminaison Client VPN pour certains certificats de client spécifiques. Par exemple, lorsqu'un utilisateur quitte votre organisation. Pour de plus amples informations, veuillez consulter Listes de révocation des certificats de client.

Outils de surveillance

Utilisez des outils de surveillance pour assurer le suivi de la disponibilité et les performances de vos points de terminaison Client VPN. Pour de plus amples informations, veuillez consulter Surveillance d'AWS Client VPN.

Gestion des identités et des accès

Gérez l'accès aux ressources Client VPN et aux API à l'aide de stratégies IAM pour vos utilisateurs IAM et vos rôles IAM. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour AWS le Client VPN.

Considérations relatives à IPv6 pour AWS Client VPN

Actuellement, le service Client VPN ne prend pas en charge l'acheminement du trafic IPv6 via le tunnel VPN. Cependant, dans certains cas, le trafic IPv6 doit être acheminé dans le tunnel VPN pour éviter les fuites IPv6. Une fuite IPv6 peut se produire lorsque IPv4 et IPv6 sont activés et connectés au VPN, mais que le VPN n'achemine pas le trafic IPv6 dans son tunnel. Dans ce cas, lorsque vous vous connectez à une destination IPv6 activée, vous continuez à vous connecter avec votre adresse IPv6 fournie par votre fournisseur de services Internet. Cela va entraîner une fuite de votre adresse IPv6 réelle. Les instructions ci-dessous expliquent comment acheminer le trafic IPv6 dans le tunnel VPN.

Les directives IPv6 suivantes doivent être ajoutées à votre fichier de configuration Client VPN pour éviter les fuites IPv6 :

```
ifconfig-ipv6 arg0 arg1
```

```
route-ipv6 arg0
```

On pourrait utiliser l'exemple suivant :

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

Dans cet exemple,`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` définit l'adresse IPv6 du périphérique de tunnel local sur `fd15:53b6:dead::2` et l'adresse IPv6 du point de terminaison VPN distant sur `fd15:53b6:dead::1`.

Avec la commande suivante, `route-ipv6 2000::/4` acheminera les adresses IPv6 depuis `2000:0000:0000:0000:0000:0000:0000:0000` vers `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` dans la connexion VPN.

> **Note**
>
> Pour l'acheminement de périphérique « TAP » dans Windows par exemple, le deuxième paramètre de `ifconfig-ipv6` sera utilisé comme cible d'acheminement pour `--route-ipv6`.

Les organisations doivent configurer les deux paramètres de `ifconfig-ipv6` elles-mêmes, et peuvent utiliser des adresses dans `100::/64` (de `0100:0000:0000:0000:0000:0000:0000:0000` vers `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) ou `fc00::/7` (de `fc00:0000:0000:0000:0000:0000:0000:0000` vers `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` est le bloc d'adresses ignorées uniquement, et `fc00::/7` est local uniquement.

Voici un autre exemple :

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

Dans cet exemple, la configuration achemine tout le trafic IPv6 actuellement alloué vers la connexion VPN.

Vérification

Votre organisation aura probablement ses propres tests. Une vérification de base consiste à configurer une connexion VPN de tunnel complet, puis à exécuter ping6 sur un serveur IPv6 à l'aide de l'adresse IPv6. L'adresse IPv6 du serveur doit se situer dans la plage spécifiée par la commande `route-ipv6`. Ce test ping devrait échouer. Toutefois, cela peut changer si la prise en charge IPv6 est ajoutée au service Client VPN à l'avenir. Si le ping réussit et que vous êtes en mesure d'accéder à des sites publics lorsque vous êtes connecté en mode tunnel complet, vous devrez peut-être effectuer un dépannage supplémentaire. Vous pouvez également effectuer le test en utilisant des outils accessibles au public tels que ipleak.org.

Surveillance d'AWS Client VPN

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'AWS Client VPN et de vos autres solutions AWS. Vous pouvez utiliser les fonctions suivantes pour surveiller vos points de terminaison Client VPN, analyser les modèles de trafic et résoudre les problèmes liés à vos points de terminaison Client VPN.

Amazon CloudWatch

Surveille vos ressources AWS et les applications que vous exécutez sur AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez faire en sorte que CloudWatch assure le suivi de l'utilisation du processeur ou d'autres métriques de vos instances Amazon EC2 et démarre automatiquement de nouvelles instances lorsque cela est nécessaire. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon CloudWatch.

AWS CloudTrail

Capture les appels d'API et les événements associés créés par ou au nom de votre compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Amazon CloudWatch Logs

Permet de surveiller les tentatives de connexion effectuées à votre point de terminaison AWS Client VPN. Vous pouvez afficher les tentatives de connexion et les réinitialisations de connexion pour les connexions Client VPN. Pour les tentatives de connexion, vous pouvez voir les tentatives de connexion ayant réussi et celles ayant échoué. Vous pouvez spécifier le flux de journaux CloudWatch Logs pour consigner les détails de connexion. Pour plus d'informations, consultez Journalisation des connexions et le Guide de l'utilisateur Amazon CloudWatch Logs.

Métriques CloudWatch pour AWS Client VPN

AWS Client VPN publie les métriques suivantes dans Amazon CloudWatch pour vos points de terminaison Client VPN. Les métriques sont publiées dans Amazon CloudWatch toutes les cinq minutes.

Métrique	Description
ActiveConnectionsCount	Nombre de connexions actives au point de terminaison Client VPN. Unités : nombre
AuthenticationFailures	Nombre d'échecs d'authentification pour le point de terminaison Client VPN. Unités : nombre
CrlDaysToExpiry	Nombre de jours avant l'expiration de la liste de révocation de certificats (CRL) configurée sur le point de terminaison Client VPN. Unités : Jours
EgressBytes	Nombre d'octets envoyés depuis le point de terminaison Client VPN. Unités : octets
EgressPackets	Nombre de paquets envoyés depuis le point de terminaison Client VPN. Unités : nombre
IngressBytes	Nombre d'octets reçus par le point de terminais on Client VPN. Unités : octets
IngressPackets	Nombre de paquets reçus par le point de terminaison Client VPN. Unités : nombre
SelfServicePortalClientConfigurationDownloads	Nombre de téléchargements du fichier de configuration du point de terminaison Client VPN depuis le portail en libre-service.

Métrique	Description
	Unité : nombre

AWS Client VPN publie les métriques d'évaluation de posture suivantes pour vos points de terminaison Client VPN.

Métrique	Description
ClientConnectHandlerTimeouts	Le nombre de délais d'attente lors de l'appel du gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre
ClientConnectHandlerInvalidResponses	Le nombre de réponses invalides retournées par le gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre
ClientConnectHandlerOtherExecutionErrors	Le nombre d'erreurs inattendues lors de l'exécution du gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre
ClientConnectHandlerThrottlingErrors	Le nombre d'erreurs de limitation lors de l'appel du gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre
ClientConnectHandlerDeniedConnections	Le nombre de connexions refusées par le gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre

Métrique	Description
ClientConnectHandlerFailedServiceErrors	Le nombre d'erreurs côté service lors de l'exécution du gestionnaire de connexion client pour les connexions au point de terminaison Client VPN. Unités : nombre

Vous pouvez filtrer les métriques de votre point de terminaison Client VPN par point de terminaison.

CloudWatch vous permet de récupérer des statistiques relatives à ces points de données sous la forme d'un ensemble classé de données en séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une alarme CloudWatch pour surveiller une métrique spécifiée et initier une action (par exemple, l'envoi d'une notification à une adresse e-mail) si la métrique sort de ce que vous considérez comme une plage acceptable.

Pour plus d'informations, consultez le Guide de l'utilisateur Amazon CloudWatch.

Afficher toutes les métriques CloudWatch

Vous pouvez afficher les métriques pour votre point de terminaison Client VPN comme suit.

Pour afficher les métriques à l'aide de la console CloudWatch

Les métriques sont d'abord regroupées par espace de noms de service, puis par les différentes combinaisons de dimension au sein de chaque espace de noms.

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Sous All metrics (Toutes les métriques), choisissez l'espace de noms de métrique ClientVPN.
4. Pour afficher les métriques, sélectionnez la dimension de métrique par point de terminaison.

Pour afficher les métriques à l'aide de la AWS CLI

À l'invite d'une commande, utilisez la commande suivante pour répertorier les métriques disponibles pour le Client VPN

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

Journaux CloudTrail pour AWS Client VPN

AWS Client VPN est intégré à AWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS dans Client VPN. CloudTrail capture tous les appels d'API pour Client VPN en tant qu'événements. Les appels capturés incluent les appels de la console Client VPN et les appels de code aux opérations de l'API Client VPN. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris les événements pour Client VPN. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Utilisez les informations collectées par CloudTrail pour déterminer la demande qui a été envoyée à Client VPN, l'adresse IP à l'origine de la demande, le demandeur, la date de la demande, ainsi que d'autres informations.

Pour plus d'informations sur CloudTrail, veuillez consulter le AWS CloudTrailGuide de l'utilisateur .

Informations sur Client VPN dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Lorsqu'une activité a lieu dans Client VPN, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de services AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre compte AWS, y compris les événements pour Client VPN, créez un journal de suivi. Un journal de suivi permet à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception des fichiers journaux CloudTrail de plusieurs régions et Réception des fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions Client VPN sont consignées par CloudTrail et sont documentées dans la Référence d'API Amazon EC2. À titre d'exemple, les appels vers les actions `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` et `AuthorizeClientVpnIngress` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Présentation des entrées des fichiers journaux Client VPN

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

Pour plus d'informations, consultez Journalisation des appels d'API Amazon EC2, Amazon EBS et Amazon VPC avec AWS CloudTrail dans Référence de l'API Amazon EC2.

AWS Quotas VPN pour les clients

Votre AWS compte possède les quotas suivants, anciennement appelés limites, relatifs aux points de terminaison VPN du Client. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour demander une augmentation de quota pour un quota ajustable, choisissez Yes (Oui) dans la colonne Adjustable (Ajustable). Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Quotas Client VPN

Nom	Par défaut	Ajustable
Règles d'autorisation par point de terminaison Client VPN	50	Oui
Points de terminaison Client VPN par région	5	Oui
Connexions client simultanées par point de terminaison Client VPN	Cette valeur dépend du nombre d'associations de sous-réseaux par point de terminaison. • 1 — 20 000 • 2 – 36 500 • 3 – 66 500 • 4 – 96 500 • 5 – 126 000	Oui
Nombre d'opérations simultanées par point de terminaison Client VPN †	10	Non

Nom	Par défaut	Ajustable
Entrées dans une liste de révocation de certificats clients pour les points de terminaison Client VPN	20 000	Non
Acheminements par point de terminaison Client VPN	10	Oui

† Les opérations sont les suivantes :

- Associer ou dissocier des sous-réseaux
- Créer ou supprimer des acheminements
- Créer ou supprimer des règles entrantes et sortantes
- Créer ou supprimer des groupes de sécurité

Quotas d'utilisateurs et de groupes

Lorsque vous configurez des utilisateurs et des groupes pour Active Directory ou un IdP basé sur SAML, les quotas suivants s'appliquent :

- Les utilisateurs peuvent appartenir à 200 groupes au maximum. Nous ignorons tous les groupes au-delà du 200e.
- La longueur maximale de l'ID de groupe est de 255 caractères.
- La longueur maximale de l’ID de nom est de 255 caractères. Nous tronquons les caractères au-delà du 255e.

Considérations d'ordre général

Prenez en considération les points suivants lorsque vous utilisez des points de terminaison Client VPN.

- Si vous utilisez Active Directory pour authentifier l'utilisateur, le point de terminaison VPN du Client doit appartenir au même compte que la AWS Directory Service ressource utilisée pour l'authentification Active Directory.

- Si vous utilisez l'authentification fédérée basée sur SAML pour authentifier un utilisateur, le point de terminaison VPN du Client doit appartenir au même compte que le fournisseur d'identité SAML IAM que vous créez pour définir la relation IDP à confiance.AWS Le fournisseur d'identité IAM SAML peut être partagé entre plusieurs points de terminaison VPN du Client dans le même compte. AWS

Résolution des problèmes liés AWS au VPN client

La rubrique suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer avec un point de terminaison VPN Client.

Pour plus d'informations sur le dépannage des logiciels OpenVPN utilisés par les clients pour se connecter à un VPN Client, consultez Dépannage de votre connexion VPN Client dans le AWS Client VPN Guide de l'utilisateur.

Problèmes courants

Impossible de résoudre le nom DNS du point de terminaison VPN Client

Problème

Je ne parviens pas à résoudre le nom DNS du point de terminaison VPN Client.

Cause

Le fichier de configuration du point de terminaison VPN Client inclut un paramètre appelé `remote-random-hostname`. Ce paramètre force le client à pré-insérer une chaîne aléatoire dans le nom DNS pour empêcher la mise en cache DNS. Certains clients ne reconnaissent pas ce paramètre et, par conséquent, n'ajoutent pas la chaîne aléatoire requise au nom DNS.

Solution

Ouvrez le fichier de configuration du point de terminaison VPN Client à l'aide de votre éditeur de texte préféré. Localisez la ligne qui spécifie le nom DNS du point de terminaison VPN Client et ajoutez une chaîne aléatoire au début du nom pour que le format soit *`chaîne_aléatoire.nom_DNS_affiché`*. Par Exemple:

- Nom DNS d'origine: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nom DNS modifié : `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Le trafic n'est pas réparti entre les sous-réseaux

Problème

J'essaie de répartir le trafic réseau entre deux sous-réseaux. Le trafic privé doit être acheminé par un sous-réseau privé, tandis que le trafic Internet doit l'être par un sous-réseau public. Cependant, un seul acheminement est utilisée même si j'ai ajouté les deux routes à la table de routage du point de terminaison VPN Client.

Cause

Vous pouvez associer plusieurs sous-réseaux à un point de terminaison VPN client, mais vous ne pouvez associer qu'un seul sous-réseau par zone de disponibilité. L'objectif de l'association de plusieurs sous-réseaux est de fournir une haute disponibilité et une redondance de zone de disponibilité aux clients. Toutefois, le VPN client ne vous permet pas de répartir sélectivement le trafic entre les sous-réseaux associés au point de terminaison VPN Client.

Les clients se connectent à un point de terminaison VPN Client en fonction de l'algorithme DNS round-robin (tourniquet). Cela signifie que leur trafic peut être acheminé par l'un des sous-réseaux

associés lorsqu'ils établissent une connexion. Par conséquent, les clients peuvent rencontrer des problèmes de connexion s'ils accèdent à un sous-réseau associé qui ne possède pas les entrées d'itinéraire requises.

Par exemple, supposons que vous configuriez les associations et routage de sous-réseau suivantes:

- Associations de sous-réseaux
  - Association 1 : sous-réseau A (us-east-1a)
  - Association 2 : sous-réseau B (us-east-1b)
- Routage
  - Routage 1: 10.0.0.0/16 acheminé vers le sous-réseau A
  - Routage 2: 172.31.0.0/16 acheminé vers le sous-réseau B

Dans cet exemple, les clients qui accèdent au sous-réseau A lorsqu'ils se connectent ne peuvent pas accéder à l'acheminement 2, tandis que les clients qui accèdent au sous-réseau B lorsqu'ils se connectent ne peuvent pas accéder à l'acheminement 1.

Solution

Vérifiez que le point de terminaison VPN Client a les mêmes entrées d'acheminement, avec les cibles de chaque réseau associé. Cela garantit que les clients peuvent accéder à tous les routages, quel que soit le sous-réseau via lequel leur trafic est acheminé.

Les règles d'autorisation pour les groupes Active Directory ne fonctionnent pas comme prévu

Problème

J'ai configuré des règles d'autorisation pour mes groupes Active Directory, mais elles ne fonctionnent pas comme prévu. J'ai ajouté une règle d'autorisation pour que `0.0.0.0/0` autorise le trafic pour tous les réseaux, mais le trafic continue d'échouer pour les CIDR de destination spécifiques.

Cause

Les règles d'autorisation sont indexées sur les CIDR réseau. Les règles d'autorisation doivent accorder aux groupes Active Directory l'accès à des CIDR réseau spécifiques. Les règles d'autorisation pour `0.0.0.0/0` sont traitées comme un cas particulier et sont donc évaluées en dernier, quel que soit l'ordre de création des règles d'autorisation.

Par exemple, supposons que vous créez cinq règles d'autorisation dans l'ordre suivant:

- Règle 1 : accès du groupe 1 à `10.1.0.0/16`
- Règle 2 : accès du groupe 1 à `0.0.0.0/0`
- Règle 3 : accès du groupe 2 à `0.0.0.0/0`
- Règle 4 : accès du groupe 3 à `0.0.0.0/0`
- Règle 5 : accès du groupe 2 à `172.131.0.0/16`

Dans cet exemple, les règles 2, 3 et 4 sont évaluées en dernier. Le groupe 1 n'a accès qu'à `10.1.0.0/16` et le groupe 2 n'a accès qu'à `172.131.0.0/16`. Le groupe 3 n'a pas accès à `10.1.0.0/16` ou `172.131.0.0/16`, mais il a accès à tous les autres réseaux. Si vous supprimez les règles 1 et 5, les trois groupes ont accès à tous les réseaux.

Le VPN Client utilise la correspondance du préfixe la plus longue lors de l'évaluation des règles d'autorisation. VoirPriorité d’acheminement dans leAmazon VPC Guide de l’utilisateurpour plus d'informations.

Solution

Vérifiez que vous créez des règles d'autorisation qui accordent explicitement aux groupes Active Directory l'accès à des CIDR réseau spécifiques. Si vous ajoutez une règle d'autorisation pour `0.0.0.0/0`, gardez à l'esprit qu'elle sera évaluée en dernier et que les règles d'autorisation antérieures peuvent limiter les réseaux auxquels elle accorde l'accès.

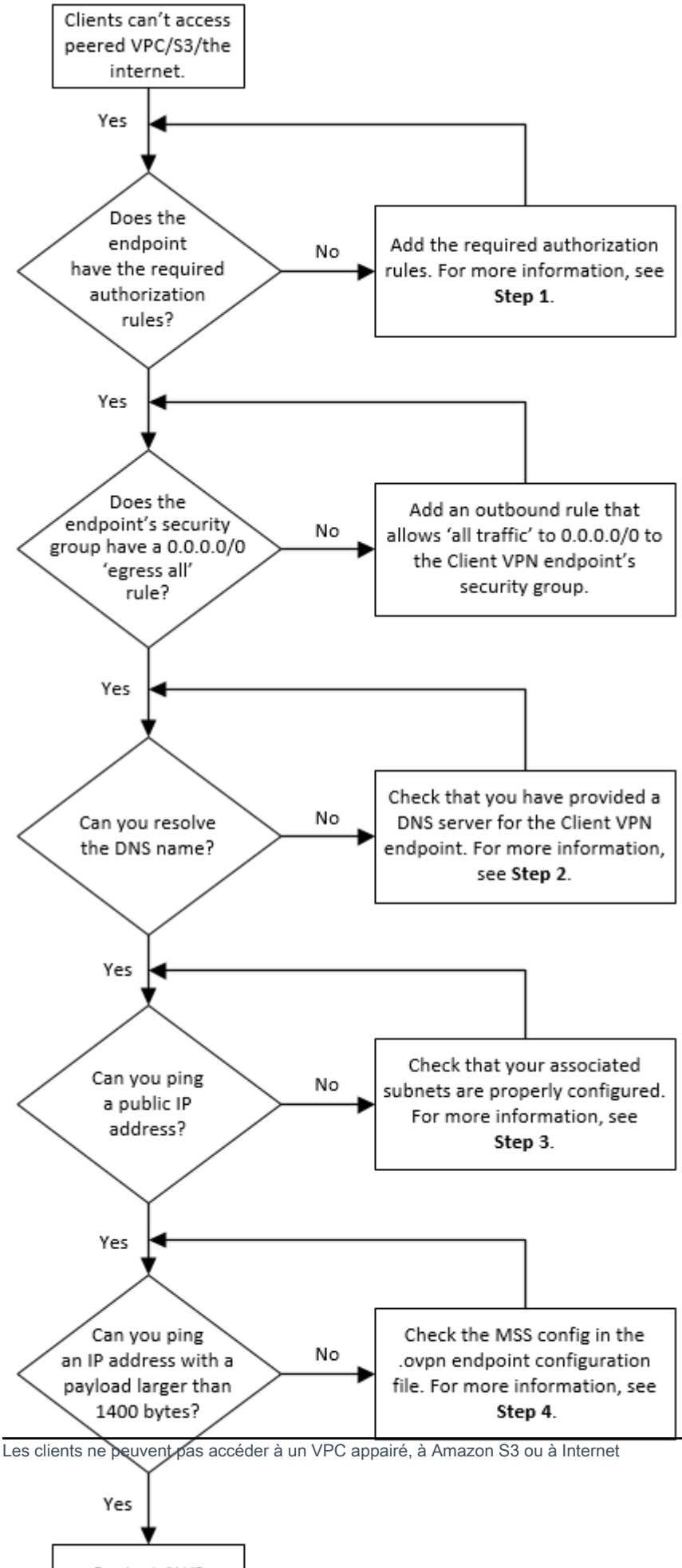
Les clients ne peuvent pas accéder à un VPC appairé, à Amazon S3 ou à Internet

Problème

J'ai correctement configuré mes routes de points de terminaison VPN Client, mais mes clients ne peuvent pas accéder à un VPC appairé, à Amazon S3 ou à Internet.

Solution

L'organigramme suivant contient les étapes permettant de diagnostiquer les problèmes de connexion à Internet, à un VPC appairé et à Amazon S3.


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. Pour accéder à Internet, ajoutez une règle d'autorisation pour `0.0.0.0/0`.

   Pour accéder à un VPC appairé, ajoutez une règle d'autorisation pour la plage CIDR IPv4 du VPC.

   Pour accéder à S3, spécifiez l'adresse IP du point de terminaison Amazon S3.
2. Vérifiez si vous êtes en mesure de résoudre le nom DNS.

   Si vous ne parvenez pas à résoudre le nom DNS, vérifiez que vous avez spécifié les serveurs DNS pour le point de terminaison VPN Client. Si vous gérez votre propre serveur DNS, spécifiez son adresse IP. Vérifiez que le serveur DNS est accessible à partir du VPC.

   Si vous n'êtes pas sûr de l'adresse IP à spécifier pour les serveurs DNS, spécifiez le résolveur DNS VPC à l'adresse IP .2 de votre VPC.
3. Pour accéder à Internet, vérifiez si vous êtes en mesure d'effectuer un ping sur une adresse IP publique ou un site Web public, par exemple, `amazon.com`. Si vous ne recevez pas de réponse, assurez-vous que la table de routage des sous-réseaux associés a une route par défaut qui cible une passerelle Internet ou une passerelle NAT. Si l'acheminement par défaut est en place, vérifiez que le sous-réseau associé ne dispose pas de règles de liste de contrôle d'accès réseau qui bloquent le trafic entrant et sortant.

   Si vous ne parvenez pas à atteindre un VPC appairé, vérifiez que la table de routage du sous-réseau associé possède une entrée de routage pour le VPC appairé.

   Si vous ne parvenez pas à atteindre Amazon S3, vérifiez que la table de routage du sous-réseau associé possède une entrée de routage pour le point de terminaison VPC de passerelle.
4. Vérifiez si vous pouvez exécuter une commande ping sur une adresse IP publique avec une charge utile supérieure à 1 400 octets. Utilisez l'une des commandes suivantes :

   - Windows

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

   - Linux

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

Si vous ne pouvez pas à exécuter une commande ping sur une adresse IP avec une charge utile supérieure à 1400 octets, ouvrez le fichier de configuration `.ovpn` du point de terminaison VPN Client à l'aide de votre éditeur de texte préféré et ajouter ce qui suit.

```
mssfix 1328
```

L'accès à un VPC appairé, à Amazon S3 ou à Internet est intermittent

Problème

J'ai des problèmes de connexion intermittents lors de la connexion à un VPC appairé, à Amazon S3 ou à Internet, mais l'accès aux sous-réseaux associés n'est pas affecté. Je dois me déconnecter et me reconnecter afin de résoudre les problèmes de connexion.

Cause

Les clients se connectent à un point de terminaison VPN Client en fonction de l'algorithme DNS round-robin (tourniquet). Cela signifie que leur trafic peut être acheminé par l'un des sous-réseaux associés lorsqu'ils établissent une connexion. Par conséquent, les clients peuvent rencontrer des problèmes de connexion s'ils accèdent à un sous-réseau associé qui ne possède pas les entrées d'itinéraire requises.

Solution

Vérifiez que le point de terminaison VPN Client a les mêmes entrées d'acheminement, avec les cibles de chaque réseau associé. Cela garantit que les clients ont accès à toutes les routes, quel que soit le sous-réseau associé via lequel leur trafic est acheminé.

Par exemple, supposons que votre point de terminaison VPN Client a trois sous-réseaux associés (sous-réseaux A, B et C) et que vous souhaitez activer l'accès Internet pour vos clients. Pour y arriver, vous devez ajouter trois routes `0.0.0.0/0`, chacune ciblant chaque sous-réseau associé:

- Acheminement 1 : `0.0.0.0/0` pour le sous-réseau A
- Acheminement 2 : `0.0.0.0/0` pour le sous-réseau B
- Acheminement 3 : `0.0.0.0/0` pour le sous-réseau C

Le logiciel client renvoie une erreur TLS

Problème

Je pouvais connecter mes clients au VPN Client avec succès, mais désormais le client OpenVPN renvoie l'une des erreurs suivantes lorsqu'il essaie de se connecter :

```
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.
```

Cause possible 1

Si vous utilisez l'authentification mutuelle et que vous avez importé une liste de révocation de certificat client, la liste de révocation de certificat client a peut-être expiré. Au cours de la phase d'authentification, le point de terminaison VPN Client vérifie le certificat client par rapport à la liste de révocation de certificats client que vous avez importée. Si la liste de révocation de certificats client a expiré, vous ne pouvez pas vous connecter au point de terminaison VPN Client.

Solution 1

Vérifiez la date d'expiration de votre liste de révocation de certificat client à l'aide de l'outil OpenSSL.

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

La sortie affiche la date et l'heure d'expiration. Si la liste de révocation de certificats client a expiré, vous devez en créer une nouvelle et l'importer dans le point de terminaison VPN Client. Pour de plus amples informations, veuillez consulter Listes de révocation des certificats de client.

Cause possible 2

Le certificat de serveur utilisé pour le point de terminaison VPN du client a expiré.

Solution 2

Vérifiez l'état de votre certificat de serveur dans la AWS Certificate Manager console ou à l'aide de la AWS CLI. Si le certificat de serveur a expiré, créez un nouveau certificat et téléchargez-le sur ACM. Pour obtenir une présentation détaillée des étapes requises pour générer les certificats et les clés

de serveur et client à l'aide de l'utilitaire Easy RSA OpenVPN et les importer dans ACM, consultez Authentification mutuelle.

Il peut aussi exister un problème avec le logiciel OpenVPN que le client utilise pour se connecter au Client VPN. Pour plus d'informations sur le dépannage des logiciels OpenVPN, consultez Dépannage de votre connexion VPN Client) dans le AWS Client VPN Guide de l'utilisateur.

Le logiciel client renvoie des erreurs de nom d'utilisateur et de mot de passe (authentification Active Directory)

Problème

J'utilise l'authentification Active Directory pour mon point de terminaison VPN Client et je pouvais connecter mes clients au Client VPN avec succès. Mais désormais, les clients obtiennent des erreurs de nom d'utilisateur et de mot de passe non valides.

Causes possibles :

Si vous utilisez l'authentification Active Directory et si vous avez activé l'authentification multi-facteur (MFA) après avoir distribué le fichier de configuration client, le fichier ne contient pas les informations nécessaires pour inviter les utilisateurs à saisir leur code MFA. Les utilisateurs sont invités à entrer leur nom d'utilisateur et leur mot de passe uniquement, et l'authentification échoue.

Solution

Téléchargez un nouveau fichier de configuration client et distribuez-le à vos clients. Vérifiez que le fichier contient la ligne suivante :

```
static-challenge "Enter MFA code " 1
```

Pour plus d’informations, veuillez consulter . Exporter et configurer le fichier de configuration du client. Testez la configuration MFA pour votre Active Directory sans utiliser le point de terminaison VPN Client pour vérifier que le MFA fonctionne comme prévu.

Le logiciel client renvoie des erreurs de nom d'utilisateur et de mot de passe (authentification fédérée)

Problème

J'essaie de vous connecter avec un nom d'utilisateur et un mot de passe avec une authentification fédérée et le message d'erreur suivant s'affiche : « Les informations d'identification reçues sont incorrectes. Contactez votre administrateur informatique. »

Cause

Cette erreur peut être due au fait qu'au moins un attribut n'est pas inclus dans la réponse SAML de l'IdP.

Solution

Assurez-vous qu'au moins un attribut est inclus dans la réponse SAML de l'IdP. Pour plus d'informations, consultez Ressources de configuration d'un IdP basé sur SAML.

Les clients ne peuvent pas se connecter (authentification mutuelle)

Problème

J'utilise l'authentification mutuelle pour mon point de terminaison VPN Client. Les clients obtiennent des erreurs d'échec de négociation de clé TLS et des erreurs de délai d'expiration.

Causes possibles :

Le fichier de configuration fourni aux clients ne contient pas le certificat client et la clé privée du client, ou le certificat et la clé sont incorrects.

Solution

Assurez-vous que le fichier de configuration contient le certificat client et la clé corrects. Si nécessaire, corrigez le fichier de configuration et redistribuez-le à vos clients. Pour de plus amples informations, veuillez consulter Exporter et configurer le fichier de configuration du client.

Le client renvoie des informations d'identification dont la taille dépasse l'erreur maximale (authentification fédérée)

Problème

J'utilise l'authentification fédérée pour mon point de terminaison VPN Client. Lorsque les clients saisissent leur nom d'utilisateur et leur mot de passe dans la fenêtre du navigateur du fournisseur

d'identité (IdP) basé sur SAML, ils obtiennent une erreur indiquant que les informations d'identification dépassent la taille maximale prise en charge.

Cause

La réponse SAML renvoyée par l'IdP dépasse la taille maximale prise en charge. Pour de plus amples informations, veuillez consulter Les exigences et les observations relatives à l'authentification fédérée basée sur SAML.

Solution

Essayez de réduire le nombre de groupes auxquels l'utilisateur appartient dans l'IdP, puis essayez de vous connecter à nouveau.

Le client n'ouvre pas le navigateur (authentification fédérée)

Problème

J'utilise l'authentification fédérée pour mon point de terminaison VPN Client. Lorsque les clients essaient de se connecter au point de terminaison, le logiciel client n'ouvre pas de fenêtre de navigateur et affiche à la place une fenêtre contextuelle de nom d'utilisateur et de mot de passe.

Cause

Le fichier de configuration fourni aux clients ne contient pas l'indicateur `auth-federate`.

Solution

Exportez le dernier fichier de configuration, importez-le sur le client AWS fourni et réessayez de vous connecter.

Le client ne renvoie aucune erreur de ports disponibles (authentification fédérée)

Problème

J'utilise l'authentification fédérée pour mon point de terminaison VPN Client. Lorsque des clients essaient de se connecter au point de terminaison, le logiciel client renvoie l'erreur suivante :

```
The authentication flow could not be initiated. There are no available ports.
```

Cause

Le client AWS fourni nécessite l'utilisation du port TCP 35001 pour terminer l'authentification. Pour de plus amples informations, veuillez consulter Les exigences et les observations relatives à l'authentification fédérée basée sur SAML.

Solution

Vérifiez que le périphérique du client ne bloque pas le port TCP 35001 ou ne l'utilise pas pour un autre processus.

Connexion VPN interrompue en raison d'une incompatibilité d'adresse IP

Problème

La connexion VPN est interrompue et le logiciel client renvoie le message d'erreur suivant : `"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."`

Cause

Le client AWS fourni nécessite que l'adresse IP à laquelle il est connecté corresponde à l'adresse IP du serveur VPN qui soutient le point de terminaison VPN du Client. Pour de plus amples informations, veuillez consulter Règles et bonnes pratiques de AWS Client VPN.

Solution

Vérifiez qu'il n'existe aucun proxy DNS entre le client AWS fourni et le point de terminaison VPN du Client.

Le routage du trafic vers le réseau local ne fonctionne pas comme prévu

Problème

La tentative d'acheminer le trafic vers le réseau local (LAN) ne fonctionne pas comme prévu lorsque les plages d'adresses IP du réseau local ne se situent pas dans les plages d'adresses IP privées standard suivantes : `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, ou `169.254.0.0/16`.

Cause

S'il est détecté que la plage d'adresses LAN du client se situe en dehors des plages standard ci-dessus, le point de terminaison du VPN client transmet automatiquement la directive OpenVPN « redirect-gateway block-local » au client, forçant ainsi tout le trafic LAN à entrer dans le VPN. Pour de plus amples informations, veuillez consulter Règles et bonnes pratiques de AWS Client VPN.

Solution

Si vous avez besoin d'un accès au réseau local pendant les connexions VPN, il est conseillé d'utiliser les plages d'adresses classiques répertoriées ci-dessus pour votre réseau local.

Vérifier la limite de bande passante pour un point de terminaison VPN Client

Problème

J'ai besoin de vérifier la limite de bande passante pour un point de terminaison VPN Client.

Cause

Le débit dépend de plusieurs facteurs, tels que la capacité de votre connexion depuis votre emplacement et la latence réseau entre votre application de bureau VPN Client sur votre ordinateur et le point de terminaison d'un VPC. Il existe également une limite de bande passante de 10 Mbits/s par connexion utilisateur.

Solution

Exécutez les commandes suivantes pour vérifier la bande passante.

```
sudo iperf3 -s -V
```

Sur le client :

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Historique du document pour le Guide de l'utilisateur Client VPN

Le tableau suivant décrit les mises à jour du Guide de l'administrateur AWS Client VPN.

Modification	Description	Date
Exemples de règles d'autorisation	Ajout d'exemples de scénario pour les règles d'autorisation.	15 septembre 2022
Durée maximale de session VPN	Vous pouvez configurer une durée maximale de session VPN plus courte pour répondre aux exigences de sécurité et de conformité.	20 janvier 2022
Bannière de connexion client	Vous pouvez activer une bannière texte sur les applications de bureau Client VPN fournies par AWS lorsqu'une session VPN est établie pour répondre aux besoins réglementaires et de conformité.	20 janvier 2022
Client Connect Handler	Vous pouvez activer Client Connect Handler pour votre point de terminaison Client VPN afin d'exécuter une logique personnalisée autorisant de nouvelles connexions.	4 novembre 2020
Portail en libre-service	Vous pouvez activer un portail en libre-service sur votre point	29 octobre 2020

	de terminaison Client VPN pour vos clients.	
Accès client à client	Vous pouvez permettre aux clients qui se connectent à un point de terminaison Client VPN de se connecter entre eux.	29 septembre 2020
Authentification fédérée basée sur SAML 2.0	Vous pouvez authentifier les utilisateurs Client VPN à l'aide de l'authentification fédérée basée sur SAML 2.0.	19 mai 2020
Spécifier les groupes de sécurité lors de la création	Vous pouvez spécifier un VPC et des groupes de sécurité lorsque vous créez votre point de terminaison AWS Client VPN.	5 mars 2020
Ports VPN configurables	Vous pouvez spécifier un numéro de port VPN pris en charge pour votre point de terminaison AWS Client VPN.	16 janvier 2020
Prise en charge de l'authentification MFA (Multi-Factor Authentication)	Votre point de terminaison AWS Client VPN prend en charge l'authentification MFA si celle-ci est activée pour votre Active Directory.	30 septembre 2019
Prise en charge des tunnels partagés	Vous pouvez activer le tunnel partagé sur votre point de terminaison AWS Client VPN.	24 juillet 2019
Première version	Cette version présente AWS Client VPN.	18 décembre 2018

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.