



Guide de l'utilisateur

# AWS VPN client



# AWS VPN client: Guide de l'utilisateur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

---

# Table of Contents

Qu'est-ce que AWS Client VPN ? .....	1
Composants du VPN client .....	1
Ressources supplémentaires pour configurer le Client VPN .....	1
Commencez avec Client VPN .....	2
Conditions préalables à l'utilisation du Client VPN .....	2
Étape 1 : Obtenir une application cliente VPN .....	3
Étape 2 : Obtenir le fichier de configuration du point de terminaison Client VPN .....	3
Étape 3 : Connexion au réseau VPN .....	4
Télécharger Client VPN .....	4
Connect à l'aide d'un client AWS fourni .....	6
Sécurité .....	6
Support pour les connexions simultanées .....	6
Directives OpenVPN .....	7
Windows .....	9
Exigences .....	9
Connect à l'aide du client .....	10
Compatibilité avec la sécurité des terminaux .....	11
Notes de mise à jour .....	13
macOS .....	29
Exigences .....	29
Connect à l'aide du client .....	30
Notes de mise à jour .....	31
Linux .....	41
Conditions requises pour se connecter au Client VPN avec un AWS client fourni pour	
Linux .....	41
Installez le client .....	42
Connect à l'aide du client .....	43
Notes de mise à jour .....	44
Se connecter à l'aide d'un client OpenVPN .....	53
Windows .....	54
Établissez une connexion VPN à l'aide d'un certificat sous Windows .....	55
macOS .....	56
Établissez une connexion VPN sur macOS .....	57
Linux .....	58

Établissez une connexion VPN sous Linux .....	58
Connexions VPN du client sur Android et iOS .....	59
Résolution des problèmes .....	61
Résolution des problèmes liés aux points de terminaison Client VPN pour les administrateurs ...	61
Envoyer les journaux de diagnostic à AWS Support dans le AWS client fourni .....	61
Envoyer des journaux de diagnostic .....	62
Résolution des problèmes liés à Windows .....	63
AWS journaux d'événements client fournis .....	63
Le client ne parvient pas à se connecter .....	64
Le client ne peut pas se connecter avec le message de journal « aucun TAP-Windows adaptateur » .....	65
Le client est bloqué à l'état de reconnexion .....	65
Le processus de connexion VPN se ferme de façon inattendue .....	66
Échec du lancement de l'application .....	66
Le client ne parvient pas à créer de profil .....	66
Le VPN se déconnecte avec un message contextuel .....	67
Un plantage du client se produit sur les ordinateurs Dell qui utilisent Windows 10 ou 11 .....	68
OpenVPN GUI .....	69
Client de connexion OpenVPN .....	70
Impossible de résoudre le DNS .....	70
Alias PKI manquant .....	71
Résolution des problèmes liés à macOS .....	71
AWS journaux d'événements client fournis .....	71
Le client ne parvient pas à se connecter .....	72
Le client est bloqué à l'état de reconnexion .....	73
Le client ne parvient pas à créer de profil .....	74
L'outil d'assistance est requis (erreur) .....	74
Tunnelblick .....	75
Algorithme de chiffrement « AES-256-GCM » introuvable .....	75
La connexion cesse de répondre et se réinitialise .....	76
EKU, Extended key usage (Utilisation étendue des clés) .....	76
Certificat expiré .....	77
OpenVPN .....	77
Impossible de résoudre le DNS .....	78
Résolution des problèmes liés à Linux .....	78
AWS journaux d'événements client fournis .....	63

---

Les requêtes DNS sont dirigées vers un serveur de noms par défaut .....	79
OpenVPN (ligne de commande) .....	80
OpenVPN via Network Manager (interface utilisateur graphique) .....	82
Problèmes courants .....	82
Échec de la négociation de clé TLS .....	83
Historique du document .....	84
.....	xcvii

# 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 aux AWS ressources et aux ressources de votre réseau local.

Ce guide fournit les étapes à suivre pour établir une connexion VPN à un point de terminaison Client VPN à l'aide d'une application cliente sur votre périphérique.

## Composants du VPN client

Les éléments clés de l'utilisation du AWS Client VPN sont les suivants.

- Point de terminaison VPN client : l'administrateur de votre VPN client crée et configure un point de terminaison VPN client dans AWS. Votre administrateur contrôle les ressources et les réseaux auxquels vous pouvez accéder lorsque vous établissez une connexion VPN.
- Application cliente VPN : application logicielle que vous utilisez pour vous connecter au point de terminaison Client VPN et établir une connexion VPN sécurisée.
- Fichier de configuration du point de terminaison Client VPN : fichier de configuration fourni par votre administrateur Client VPN. Le fichier contient des informations sur le point de terminaison VPN du Client et les certificats requis pour établir une connexion VPN. Vous chargez ce fichier dans l'application cliente VPN choisie. Le client AWS fourni vous permet de vous connecter à cinq sessions simultanées, chaque session ayant son propre fichier de configuration fourni par l'administrateur VPN du Client. Pour plus d'informations sur les sessions simultanées, consultez [Support pour les connexions simultanées](#).

## Ressources supplémentaires pour configurer le Client VPN

Si vous êtes administrateur d'un client VPN, consultez le [guide de l'AWS Client VPN administrateur](#) pour plus d'informations sur la création et la configuration d'un point de terminaison VPN client.

# Commencez avec AWS Client VPN

Avant que vous puissiez établir une session VPN, votre administrateur Client VPN doit créer et configurer un point de terminaison Client VPN. Votre administrateur contrôle les ressources et les réseaux auxquels vous pouvez accéder lorsque vous établissez une session VPN. Vous pouvez utiliser une application cliente VPN pour vous connecter à un point de terminaison Client VPN et établir une connexion VPN sécurisée.

Si vous êtes un administrateur qui doit créer un point de terminaison Client VPN, consultez le [Guide de l'administrateur AWS Client VPN](#).

## Rubriques

- [Conditions préalables à l'utilisation du Client VPN](#)
- [Étape 1 : Obtenir une application cliente VPN](#)
- [Étape 2 : Obtenir le fichier de configuration du point de terminaison Client VPN](#)
- [Étape 3 : Connexion au réseau VPN](#)
- [Téléchargez le AWS Client VPN depuis le portail en libre-service](#)

## Conditions préalables à l'utilisation du Client VPN

Pour établir une connexion VPN, vous devez disposer des éléments suivants :

- Un accès à Internet
- Un appareil pris en charge
- Une version compatible de [Windows](#), [macOS](#) ou [Linux](#).
- Pour les points de terminaison Client VPN qui utilisent l'authentification fédérée basée sur SAML (authentification unique), l'un des navigateurs suivants :
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

## Étape 1 : Obtenir une application cliente VPN

Vous pouvez vous connecter à un point de terminaison Client VPN et établir une connexion VPN à l'aide du client fourni par AWS ou d'une autre application cliente OpenVPN.

Vous pouvez télécharger l'application Client VPN selon l'une des deux méthodes suivantes, selon que l'administrateur a créé ou non le fichier de configuration du point de terminaison pour l'application :

- Si votre administrateur n'a pas configuré les fichiers de configuration du point de terminaison, téléchargez et installez le client depuis le [téléchargement du AWS Client VPN](#). Après avoir téléchargé et installé l'application, accédez [the section called “Étape 2 : Obtenir le fichier de configuration du point de terminaison Client VPN”](#) au fichier de configuration du point de terminaison auprès de votre administrateur. Si vous vous connectez à plusieurs profils, vous aurez besoin d'un fichier de configuration pour chaque profil.
- Si votre administrateur a déjà préconfiguré le fichier de configuration du point de terminaison, vous pouvez télécharger l'application Client VPN, ainsi que le fichier de configuration, depuis le portail en libre-service. Pour connaître les étapes de téléchargement du client et du fichier de configuration depuis le portail en libre-service, reportez-vous [the section called “Télécharger Client VPN”](#) à. Après avoir téléchargé et installé l'application et le fichier, rendez-vous sur [the section called “Étape 3 : Connexion au réseau VPN”](#).

Vous pouvez également télécharger et installer une application cliente OpenVPN sur l'appareil à partir duquel vous avez l'intention d'établir la connexion VPN.

## Étape 2 : Obtenir le fichier de configuration du point de terminaison Client VPN

Vous pouvez obtenir le fichier de configuration du point de terminaison Client VPN auprès de votre administrateur. Le fichier de configuration inclut les informations sur le point de terminaison Client VPN et les certificats requis pour établir une connexion VPN.

Sinon, si l'administrateur de votre VPN client a configuré un portail en libre-service pour le point de terminaison du client VPN, vous pouvez télécharger vous-même la dernière version du client AWS fourni et la dernière version du fichier de configuration du point de terminaison du client VPN. Pour de plus amples informations, veuillez consulter [Téléchargez le AWS Client VPN depuis le portail en libre-service](#).

## Étape 3 : Connexion au réseau VPN

Importez le fichier de configuration du point de terminaison du client VPN sur le client AWS fourni ou sur votre application cliente OpenVPN et connectez-vous au VPN. Pour connaître les étapes de connexion à un VPN, notamment l'importation d'un ou de plusieurs fichiers de configuration de point de terminaison pour un client AWS fourni, consultez les rubriques suivantes :

- [Connectez-vous à un AWS Client VPN point de terminaison à l'aide d'un client AWS fourni](#)
- [Connect à un AWS Client VPN point de terminaison utilisant un client OpenVPN](#)

Pour les points de terminaison Client VPN qui utilisent l'authentification Active Directory, vous serez invité à entrer votre nom d'utilisateur et votre mot de passe. Si l'authentification MFA (Multi-Factor Authentication) a été activée pour le répertoire, vous serez également invité à entrer votre code MFA.

Pour les points de terminaison VPN du Client qui utilisent l'authentification fédérée basée sur le protocole SAML (authentification unique), le client AWS fourni ouvre une fenêtre de navigateur sur votre ordinateur. Vous serez invité à saisir vos informations d'identification d'entreprise avant de pouvoir vous connecter au point de terminaison Client VPN.

## Téléchargez le AWS Client VPN depuis le portail en libre-service

Le portail en libre-service est une page Web qui vous permet de télécharger la dernière version du client AWS fourni et les dernières versions des fichiers de configuration des points de terminaison du Client VPN. Si l'administrateur du point de terminaison de votre Client VPN a préconfiguré un ou plusieurs fichiers de configuration pour le client Client VPN, vous pouvez télécharger et installer cette application VPN client ainsi que ces fichiers de configuration depuis ce portail.

### Note

Si vous êtes administrateur et souhaitez configurer le portail en libre-service, consultez la section [Points de terminaison VPN du Client](#) dans le Guide de l'AWS Client VPN administrateur.

Avant de commencer, vous devez disposer de l'identifiant de chaque point de terminaison du client VPN que vous souhaitez télécharger. L'administrateur du point de terminaison du VPN client peut vous fournir l'identifiant ou peut vous donner l'URL d'un portail en libre-service qui inclut

cet identifiant. Pour les connexions à plusieurs terminaux, vous aurez besoin de l'ID du point de terminaison pour chaque profil auquel vous souhaitez vous connecter.

Pour accéder au portail en libre-service

1. Accédez au portail en libre-service à l'adresse <https://self-service.clientvpn.amazonaws.com/>, ou utilisez l'URL qui vous a été fournie par votre administrateur.
2. Si nécessaire, entrez l'ID du point de terminaison Client VPN, par exemple, `cvpn-endpoint-0123456abcd123456`. Choisissez Suivant.
3. Entrez votre nom d'utilisateur et votre mot de passe, puis choisissez Sign In (Se connecter). Il s'agit du même nom d'utilisateur et mot de passe que vous utilisez pour vous connecter au point de terminaison Client VPN.
4. Dans le portail en libre-service, vous pouvez effectuer les opérations suivantes :
  - Téléchargez la dernière version du fichier de configuration client pour le point de terminaison Client VPN. Si vous souhaitez vous connecter à plusieurs points de terminaison, vous devez télécharger le fichier de configuration pour chaque point de terminaison.
  - Téléchargez la dernière version du client AWS fourni pour votre plateforme.
5. Répétez ces étapes pour chaque fichier de configuration du point de terminaison pour lequel vous souhaitez créer un profil de connexion.

# Connectez-vous à un AWS Client VPN point de terminaison à l'aide d'un client AWS fourni

Vous pouvez vous connecter à un point de terminaison VPN client à l'aide du client AWS fourni, qui est pris en charge sous Windows, macOS et Ubuntu. Le client AWS fourni prend également en charge jusqu'à cinq connexions simultanées ainsi que les directives OpenVPN.

## Rubriques

- [Support pour les connexions simultanées](#)
- [Directives OpenVPN](#)

## Sécurité

La sécurité est la priorité absolue du client AWS fourni. Nous publions régulièrement des correctifs pour améliorer le niveau de sécurité de l'application. Le client fourni par AWS inclut plusieurs fonctionnalités de sécurité uniques par rapport aux autres clients OpenVPN, notamment l'authentification SAML, l'application des itinéraires clients et la surveillance des paramètres des appareils.

Bien que le client AWS fourni soit conçu pour atténuer les menaces provenant d'un environnement réseau mal configuré ou compromis, il n'est pas responsable de la modification de l'environnement ou de l'élimination des menaces externes à leur source. Le client AWS fourni compte sur les clients pour maintenir un environnement sécurisé et bien configuré. Cela inclut notamment les éléments suivants :

- Empêcher les modifications non autorisées ou les abus par les utilisateurs locaux
- Restreindre les privilèges administratifs aux utilisateurs de confiance
- Maintenance des correctifs up-to-date de sécurité

## Support pour les connexions simultanées à l'aide d'un client AWS fourni

Le client AWS fourni permet de se connecter à plusieurs sessions simultanées. Cela est utile si vous avez besoin d'accéder à des ressources dans plusieurs AWS environnements et que vous disposez de différents points de terminaison pour ces ressources. Par exemple, vous pouvez avoir

besoin d'accéder à une base de données dans un environnement sur un point de terminaison différent du point de terminaison auquel vous êtes actuellement connecté, mais vous ne souhaitez pas déconnecter la connexion actuelle. Pour permettre au client que vous avez AWS fourni de se connecter aux sessions en cours, téléchargez le fichier de configuration créé par votre administrateur pour chaque point de terminaison, puis créez un profil de connexion pour chaque fichier. À l'aide du client AWS fourni, vous pouvez ensuite vous connecter à plusieurs sessions sans vous déconnecter d'une session actuellement ouverte. Ceci n'est pris en charge que pour les clients AWS fournis. Pour connaître les étapes de connexion à des sessions simultanées, consultez les rubriques suivantes :

- [Connect à l'aide du client AWS fourni pour Windows](#)
- [Connect à l'aide du client AWS fourni pour macOS](#)
- [Connect à l'aide du client AWS fourni pour Linux](#)

Lorsque vous vous connectez à plusieurs points de terminaison, le Client VPN met en œuvre des contrôles pour s'assurer qu'il n'y a aucun conflit avec d'autres connexions de point de terminaison ouvertes, par exemple si deux sessions ont des blocs CIDR ou des politiques de routage contradictoires, ou si vous êtes déjà connecté via une connexion tunnel complète. Si le contrôle détecte des conflits, aucune connexion ne sera établie tant que vous n'aurez pas choisi une autre connexion qui n'est pas en conflit avec la connexion ouverte ou que vous ne vous êtes pas déconnecté de la session ouverte à l'origine du conflit.

Les connexions DNS simultanées sont autorisées. Le serveur DNS de l'une des connexions compatibles DNS sera appliqué. Selon le serveur DNS, il se peut que vous soyez invité à vous authentifier lors de cette reconnexion.

#### Note

Le nombre maximum de sessions simultanées autorisées est de cinq.

## Directives OpenVPN

Le client AWS fourni prend en charge les directives OpenVPN suivantes. Pour plus d'informations sur ces directives, consultez la documentation sur le site Web d'[OpenVPN](#).

- auth-federate
- auth-nocache

- `auth-retry`
- `auth-user-pass`
- `block-outside-dns`
- `ca`
- `cert`
- `cipher`
- `client`
- `connect-retry`
- `connect-retry-max`
- `cryptoapicert`
- `dev`
- `dev-type`
- `bb`
- `dhcp-option`
- `ifconfig-ipv6`
- `inactive`
- `keepalive`
- `clé`
- `mssfix`
- `nobind`
- `persist-key`
- `persist-tun`
- `ping`
- `sortie ping`
- `ping-restart`
- `proto`
- `pull`
- `pull-filter`
- `rcvbuf`
- `remote`

- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- acheminement
- route-ipv6
- server-poll-timeout
- static-challenge
- tap-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

## AWS Client VPN pour Windows

Ces sections décrivent comment établir une connexion VPN à l'aide du client AWS fourni pour les systèmes Windows x64 et Windows Arm64. Vous pouvez télécharger et installer le client depuis la page de [téléchargement de AWS Client VPN](#). Le client AWS fourni ne prend pas en charge les mises à jour automatiques.

### Exigences

Le client AWS fourni prend en charge les systèmes Windows x64 et Arm64. Les éléments suivants sont requis pour chaque système d'exploitation :

#### Systèmes d'exploitation Windows Arm64

- Windows 11 (système d'exploitation 64 bits, processeur Arm64)
- .NET Framework 4.8.1 ou supérieur

#### Note

Cette application inclut des processus d'arrière-plan qui utilisent l'émulation Arm64. Ceci est entièrement pris en charge et activé par défaut sur les appareils Windows 11 Arm64,

garantissant un fonctionnement fluide sans aucune configuration supplémentaire requise. Pour plus d'informations, consultez [Comment fonctionne l'émulation sur Arm](#).

## Systèmes d'exploitation Windows x64

- Windows 11 (système d'exploitation 64 bits, processeur x64)
- .NET Framework 4.7.2 ou version ultérieure

### Note

Pour les systèmes d'exploitation Windows x64 et Arm64, points de terminaison VPN client qui utilisent l'authentification SAML-based fédérée (authentification unique), le client réserve les ports TCP 8096-8115 sur votre ordinateur.

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

## Rubriques

- [Se connecter à AWS Client VPN avec un AWS client fourni pour Windows](#)
- [Compatibilité des logiciels de sécurité des terminaux](#)
- [AWS Client VPN pour les notes de mise à jour de Windows](#)


## Se connecter à AWS Client VPN avec un AWS client fourni pour Windows

Avant de commencer, prenez connaissance des [prérequis](#). Le client AWS fourni est également appelé client AWS VPN dans les étapes suivantes.

Pour vous connecter à l'aide du AWS client fourni pour les systèmes Windows x64 ou Windows Arm64-based :

1. Ouvrez l'application AWS VPN Client.
2. Choisissez File (Fichier), Manage Profiles (Gérer les profils).

3. Choisissez Add Profile (Ajouter un profil).
4. Pour Profile name (Nom du profil), entrez un nom pour le profil.
5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN et sélectionnez-le, puis choisissez Add Profile (Ajouter un profil).
6. Si vous souhaitez créer plusieurs connexions, répétez les étapes Ajouter un profil pour chaque fichier de configuration que vous souhaitez ajouter. Vous pouvez ajouter autant de profils que vous le souhaitez, mais vous ne pouvez avoir que cinq connexions ouvertes au maximum.
7. Dans la fenêtre du client AWS VPN, choisissez le profil auquel vous souhaitez vous connecter, puis sélectionnez Connect. Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe. Répétez cette étape pour chaque connexion de profil que vous souhaitez établir, en connectant jusqu'à cinq points de terminaison simultanés.

 Note

Si un profil auquel vous vous connectez entre en conflit avec une session actuellement ouverte, vous ne pourrez pas établir la connexion. Choisissez une nouvelle connexion ou déconnectez-vous de la session à l'origine du conflit.

8. Pour consulter les statistiques d'une connexion, choisissez Connexion dans la fenêtre du client AWS VPN, choisissez Afficher les détails, puis choisissez la connexion dont vous souhaitez consulter les détails.
9. Pour déconnecter une connexion, choisissez-en une dans la fenêtre du client AWS VPN, puis choisissez Déconnecter. Si plusieurs connexions sont ouvertes, vous devez fermer chaque connexion individuellement. Vous pouvez également choisir l'icône du client dans la barre des tâches Windows, puis choisir Disconnect (Déconnexion).

## Compatibilité des logiciels de sécurité des terminaux

Les produits de sécurité des terminaux d'entreprise tels que les pare-feux basés sur l'hôte, les agents EDR (Endpoint Detection and Response) et les logiciels antivirus peuvent parfois interférer avec les connexions VPN AWS du Client. Si vous rencontrez des problèmes de connectivité lors de l'utilisation du client AWS fourni pour Windows, vous devrez peut-être configurer des exclusions dans votre logiciel de sécurité des terminaux.

## AWS Chemins exécutables du Client VPN

Le client AWS fourni pour Windows installe les exécutables clés suivants. Vous pouvez avoir besoin de ces chemins pour configurer les règles de pare-feu, les listes d'applications autorisées ou les politiques de sécurité des terminaux.

### Application cliente VPN

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

### Processus OpenVPN

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

Il s'agit du processus de base qui établit et maintient la connexion au tunnel VPN.

### Service Windows

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

## Exigences réseau

Le client AWS fourni a besoin d'un accès réseau sortant au point de terminaison VPN du Client pour établir une connexion VPN. Assurez-vous que votre pare-feu ou votre logiciel de sécurité des terminaux autorise le trafic sortant du `acvc-openvpn.exe` processus vers le port et le protocole configurés sur le point de terminaison de votre Client VPN.

## Configuration des exclusions de sécurité des terminaux

Si votre produit de sécurité des terminaux interfère avec la connectivité client AWS fournie, passez en revue les catégories d'exclusion suivantes avec votre administrateur de sécurité :

### Process-based exclusions

Ajoutez les exécutables répertoriés dans la liste [the section called "AWS Chemins exécutables du Client VPN"](#) des processus autorisés ou exclus de votre produit de sécurité des terminaux.

### Network-based exclusions

Autorisez le trafic sortant du `acvc-openvpn.exe` processus vers le port et le protocole du point de terminaison de votre Client VPN.

## Path-based exclusions

Excluez le répertoire d'installation du client AWS fourni de l'analyse en temps réel ou de l'analyse comportementale :

```
C:\Program Files\Amazon\AWS VPN Client\
```

### Important

Les instructions de configuration prescriptives pour des produits tiers spécifiques de sécurité des terminaux ne sont pas incluses dans la AWS documentation en raison de la variabilité entre les versions et les configurations des produits. Consultez la documentation de votre fournisseur de solutions de sécurité des terminaux pour obtenir des instructions détaillées sur la configuration des exclusions pour votre produit spécifique.

## AWS Client VPN pour les notes de mise à jour de Windows

Le tableau suivant contient les notes de mise à jour et les liens de téléchargement pour les versions actuelles et précédentes de AWS Client VPN pour les systèmes Windows x64 et Windows ARM64.

### Note

Nous continuons à fournir des correctifs d'utilisabilité et de sécurité à chaque version. Nous vous recommandons vivement d'utiliser la dernière version pour chaque plateforme. Les versions précédentes peuvent être affectées par des problèmes de and/or sécurité liés à l'utilisabilité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement et SHA256
5.3.4 (x64 et Arm64)	<ul style="list-style-type: none"><li>• Correctifs de bogues mineurs et améliorations</li><li>• Niveau de sécurité amélioré</li></ul>	27 mars 2026	<ul style="list-style-type: none"><li>• <a href="#">Téléchargez Windows x64 version 5.3.4</a></li></ul>

Version	Modifications	Date	Lien de téléchargement et SHA256
			<p>sha256 : 81a5c5101 624c5f74d e8afdc81 6f03ea8ff 9e8c6a5ea a8890a957 79a94dbe41</p> <ul style="list-style-type: none"><li>• <a href="#">Téléchargez Windows Arm64 version 5.3.4</a></li></ul> <p>sha256 : 3410282eb b024e6481 2a63668b3 0117657d4 70ed4c51f 05e96fc81 2b8871587d</p>

Version	Modifications	Date	Lien de téléchargement et SHA256
5.3.3 (x64 et Arm64)	<ul style="list-style-type: none"><li>Défaillances de connexion corrigées dans la version 5.3.2</li></ul>	28 février 2026	<ul style="list-style-type: none"><li><a href="#">Téléchargez Windows x64 version 5.3.3</a>  sha256 : bbaebb977 b270add64 97c941505 fed5913b5 8056e980e 372170733 7dc051ac86</li><li><a href="#">Téléchargez Windows Arm64 version 5.3.3</a>  sha256 : c30b6d012 1a5070643 fdbebc27e 7f9569d57 4a5698631 480becb5c b96cac9fde</li></ul>

Version	Modifications	Date	Lien de téléchargement et SHA256
5.3.2 (x64 et Arm64)	<ul style="list-style-type: none"><li>• Correctifs de bogues mineurs et améliorations</li><li>• Posture de sécurité améliorée.</li></ul>	17 février 2026	<ul style="list-style-type: none"><li>• <a href="#">Téléchargez Windows x64 version 5.3.2</a>  sha256 : dd1e4fb67 18dddbf13 a5aee5421 75761bf8e d854290c5 76a488b98 173a0ccf92</li><li>• <a href="#">Téléchargez Windows Arm64 version 5.3.2</a>  sha256 : d2d18d91c a9ef53cc5 57434db18 ef5d0002e 7825a998f 2d739eac4 43b034af00</li></ul>

Version	Modifications	Date	Lien de téléchargement et SHA256
5.3.1 (x64 et Arm64)	Correctifs de bogues mineurs et améliorations	30 septembre 2025	<ul style="list-style-type: none"><li>• <a href="#">Téléchargez Windows x64 version 5.3.1</a>  sha256 : b71ddbc78 230630963 acf3ebba7 afeb6e525 99843091f f589aed6a fce4c9eb06</li><li>• <a href="#">Téléchargez Windows Arm64 version 5.3.1</a>  sha256 : e691bdb0b dcb55b3da 36f4fb2e5 198f20f18 78dc22a00 bf55bc660 999698500b</li></ul>

Version	Modifications	Date	Lien de téléchargement et SHA256
5.3.0 (Arm64)	<p>Nouveau AWS Client VPN support pour les systèmes d'exploitation Windows ARM64.</p> <p>Cette version inclut toutes les mises à jour de la version 5.3.0 de Windows (x64).</p>	26 août 2025	<p><a href="#">Téléchargez Windows Arm64 version 5.3.0</a></p> <p>sha256 : 3f1be6b48 7af8307da fbb0f7737 cd597cf71 dc64dcd31 775aeefbf 91d04b8dce</p>
5.3.0	<ul style="list-style-type: none"><li>• Améliorations mineures.</li><li>• Ajout de la prise en charge IPv6 des connexions</li></ul>	14 août 2025	<p><a href="#">Téléchargez Windows x64 version 5.3.0</a></p> <p>sha256 : e3cf1aff6 e14d79aa4 4378229a3 a0602a9e9 c2a0c6d0d 055df9014 40b6d1454a</p>

Version	Modifications	Date	Lien de téléchargement et SHA256
5.2.2	Posture de sécurité améliorée.	2 juin 2025	<a href="#">Télécharger la version 5.2.2</a>  sha256 : f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	<ul style="list-style-type: none"><li>• Ajout du support pour le ping-exit drapeau OpenVPN.</li><li>• Mise à jour de la bibliothèque OpenSSL.</li><li>• Correctifs de bogues mineurs et améliorations</li></ul>	21 avril 2025	N'est plus pris en charge.
5.2.0	<ul style="list-style-type: none"><li>• Améliorations mineures.</li><li>• Ajout de la prise en charge de l'application de l'itinéraire client.</li></ul>	8 avril 2025	N'est plus pris en charge.
5.1.0	<ul style="list-style-type: none"><li>• Correction d'un problème en raison duquel AWS Client VPN la version 5.0.x se reconnectait automatiquement au VPN après un délai d'inactivité.</li><li>• Correctifs de bogues mineurs et améliorations</li></ul>	17 mars 2025	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement et SHA256
5.0.2	<ul style="list-style-type: none"> <li>• Correction d'un problème de DNS pour les connexions simultanées.</li> <li>• Correction de problèmes sporadiques lors de l'installation de nouveaux adaptateurs TAP.</li> </ul>	24 février 2025	N'est plus pris en charge.
5.0.1	Correction d'un problème qui provoquait des erreurs de connexion VPN sporadiques sur le client Windows version 5.0.0.	30 janvier 2025	N'est plus pris en charge.
5.0.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge des connexions simultanées.</li> <li>• Mise à jour de la version du pilote TAP.</li> <li>• Mise à jour de l'interface utilisateur graphique.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	21 janvier 2025	N'est plus pris en charge.
4.1.0	Correctifs de bogues mineurs et améliorations	12 novembre 2024	N'est plus pris en charge.
4.0.0	Améliorations mineures.	25 septembre 2024	<a href="#">Télécharger la version 4.0.0</a>  sha256 : 6532f9113 85ec8fac1 494d0847c 8f90a999b 3bd738084 4e2ea4318 e9db4a2ebc

Version	Modifications	Date	Lien de téléchargement et SHA256
3.14.2	Ajout du support pour le mssfix drapeau OpenVPN.	4 septembre 2024	<a href="#">Télécharger la version 3.14.2</a>  sha256 : c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Correctifs de bogues mineurs et améliorations	22 août 2024	<a href="#">Télécharger la version 3.14.1</a>  sha256 : f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3,14,0	<ul style="list-style-type: none"> <li>Ajout du support pour le tap-sleep drapeau OpenVPN.</li> <li>Mise à jour des bibliothèques OpenVPN et OpenSSL.</li> </ul>	12 août 2024	<a href="#">Télécharger la version 3.14.0</a>  sha256 : 812fb2f6d 263288c66 4d598f6bd 70e3f601d 11dcb89e6 3b281b0a9 6b96354516

Version	Modifications	Date	Lien de téléchargement et SHA256
3,13,0	Mise à jour des bibliothèques OpenVPN et OpenSSL.	29 juillet 2024	<a href="#">Télécharger la version 3.13.0</a>  sha256 : c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12.1	Correction d'un problème qui empêchait le client Windows version 3.12.0 d'établir une connexion VPN pour certains utilisateurs.	18 juillet 2024	<a href="#">Télécharger la version 3.12.1</a>  sha256 : 5ed34aee6 c03aa281e 625acdbed 272896c67 046364a9e 5846ca697 e05dbfec08
3.12.0	<ul style="list-style-type: none"> <li>• Reconnectez-vous automatiquement lorsque la portée du réseau local change.</li> <li>• Suppression du focus automatique sur les applications lors de la connexion à des points de terminaison SAML.</li> </ul>	21 mai 2024	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
3.11.2	Résolution d'un problème d'authentification SAML avec les navigateurs basés sur Chromium depuis la version 123.	11 avril 2024	<a href="#">Télécharger la version 3.11.2</a>  sha256 : 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc
3.11.1	<ul style="list-style-type: none"> <li>• Correction d'une action de dépassement de la mémoire tampon qui pouvait potentiellement permettre à un acteur local d'exécuter des commandes arbitraires avec des autorisations élevées.</li> <li>• Posture de sécurité améliorée.</li> </ul>	16 février 2024	<a href="#">Télécharger la version 3.11.1</a>  sha256 : fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	<ul style="list-style-type: none"> <li>• Correction d'un problème de connectivité causé par Windows VMs.</li> <li>• Problèmes de connectivité résolus pour certaines configurations de réseau local.</li> <li>• Accessibilité améliorée.</li> </ul>	6 décembre 2023	<a href="#">Télécharger la version 3.11.0</a>  sha256 : 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version	Modifications	Date	Lien de téléchargement et SHA256
3.10.0	<ul style="list-style-type: none"> <li>• Correction d'un problème de connectivité lorsqu'il NAT64 est activé sur le réseau client.</li> <li>• Correction d'un problème de connectivité lorsque les adaptateurs réseau Hyper-V sont installés sur l'ordinateur client.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	24 août 2023	<a href="#">Télécharger la version 3.10.0</a>  sha256 : d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	Posture de sécurité améliorée.	3 août 2023	<a href="#">Télécharger la version 3.9.0</a>  sha256 : de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.7.0	Annulation des modifications apportées à la version 3.6.0.	15 juillet 2023	N'est plus pris en charge
3.6.0	Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.5.0	Correctifs de bogues mineurs et améliorations	3 avril 2023	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
3.4.0	Annulation des modifications apportées à la version 3.3.0.	28 mars 2023	N'est plus pris en charge
3.3.0	Correctifs de bogues mineurs et améliorations	17 mars 2023	N'est plus pris en charge
3.2.0	<ul style="list-style-type: none"><li>• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ».</li><li>• Détection automatique de la disponibilité des versions mises à jour du client.</li><li>• Ajout de la possibilité d'installer automatiquement les nouvelles versions du client lorsqu'elles sont disponibles.</li></ul>	23 janvier 2023	N'est plus pris en charge
3.1.0	Posture de sécurité améliorée.	23 mai 2022	N'est plus pris en charge
3.0.0	<ul style="list-style-type: none"><li>• Ajout de la prise en charge de Windows 11.</li><li>• Correction de la dénomination du pilote Windows TAP qui affectait d'autres noms de pilotes.</li><li>• Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée.</li><li>• Correction de l'affichage du texte de la bannière pour des textes plus longs.</li><li>• Posture de sécurité améliorée.</li></ul>	3 mars 2022	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
2.0.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie.</li> <li>• Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	20 janvier 2022	N'est plus pris en charge
1.3.7	<ul style="list-style-type: none"> <li>• Correction d'une tentative de connexion d'authentification fédérée dans certains cas.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	08 novembre 2021	N'est plus pris en charge
1.3.6	<ul style="list-style-type: none"> <li>• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, . server-poll-timeout</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	20 septembre 2021	N'est plus pris en charge
1.3.5	Correctif pour supprimer les fichiers journaux volumineux des fenêtres.	16 août 2021	N'est plus pris en charge
1.3.4	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de l'indicateur OpenVPN : dhcp-option.</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	4 août 2021	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.3.3	<ul style="list-style-type: none"> <li>• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route.</li> <li>• Résolution d'un problème qui bloquait l'application lors de la déconnexion ou de la sortie.</li> <li>• Correction d'un problème avec les noms d'utilisateur Active Directory avec barre oblique inverse.</li> <li>• Correction d'un blocage d'application lors de la manipulation de la liste de profil en dehors de l'application</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	1er juillet 2021	N'est plus pris en charge
1.3.2	<ul style="list-style-type: none"> <li>• Ajoutez la prévention des IPv6 fuites, lorsqu'elle est configurée.</li> <li>• Correction d'un incident potentiel lorsque vous utilisez l'option Afficher les détails sous Connexion.</li> </ul>	12 mai 2021	N'est plus pris en charge
1.3.1	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de plusieurs certificats clients avec le même sujet. Les certificats expirés seront ignorés.</li> <li>• Correction de la conservation des journaux locaux pour réduire l'utilisation du disque.</li> <li>• Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'.</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	5 avril 2021	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.3.0	Ajout de fonctionnalités de support, telles que le signalement d'erreurs, l'envoi de journaux de diagnostic et l'analytique.	8 mars 2021	N'est plus pris en charge
1.2.7	<ul style="list-style-type: none"> <li>Ajout de la prise en charge de la directive OpenVPN cryptoapicert.</li> <li>Correction des routes périmées entre connexions.</li> <li>Correctifs de bogue mineurs et améliorations.</li> </ul>	25 février 2021	N'est plus pris en charge
1.2.6	Correctifs de bogue mineurs et améliorations.	26 octobre 2020	N'est plus pris en charge
1.2.5	<ul style="list-style-type: none"> <li>Ajout de la prise en charge des commentaires dans la configuration OpenVPN.</li> <li>Ajout d'un message d'erreur pour les erreurs de liaison TLS.</li> </ul>	8 octobre 2020	N'est plus pris en charge
1.2.4	Correctifs de bogue mineurs et améliorations.	1 septembre 2020	N'est plus pris en charge
1.2.3	Annulez les changements dans la version 1.2.2.	20 août 2020	N'est plus pris en charge
1.2.1	Correctifs de bogue mineurs et améliorations.	1er juillet 2020	N'est plus pris en charge
1.2.0	<ul style="list-style-type: none"> <li>Ajout de la prise en charge de <a href="#">l'authentification fédérée basée sur SAML 2.0</a>.</li> <li>Prise en charge obsolète de la plate-forme Windows 7.</li> </ul>	19 mai 2020	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.1.1	Correctifs de bogue mineurs et améliorations.	21 avril 2020	N'est plus pris en charge
1.1.0	<ul style="list-style-type: none"><li>• Ajout de la prise en charge de la fonctionnalité écho « static-challenge » d'OpenVPN pour masquer ou afficher le texte affiché dans l'interface utilisateur.</li><li>• Correctifs de bogue mineurs et améliorations.</li></ul>	9 mars 2020	N'est plus pris en charge
1.0.0	Version initiale.	4 février 2020	N'est plus pris en charge

## AWS Client VPN pour macOS

Ces sections décrivent comment établir une connexion VPN à l'aide du client AWS fourni pour macOS. Vous pouvez télécharger et installer le client depuis la page de [téléchargement de AWS Client VPN](#). Le client AWS fourni ne prend pas en charge les mises à jour automatiques.

### Exigences

Pour utiliser le client AWS fourni pour macOS, les éléments suivants sont requis :

- macOS Sonoma (14.0), Sequoia (15.0) ou Tahoe (26.0)
- x86\_64 ou ARM64 compatible avec le processeur.
- Pour le VPN client, les points de terminaison qui utilisent l'authentification fédérée basée sur SAML (authentification unique), le client réserve les ports TCP 8096-8115 sur votre ordinateur.

### Rubriques

- [Se connecter à AWS Client VPN avec un AWS client fourni pour macOS](#)
- [AWS Client VPN notes de mise à jour pour macOS](#)

## Se connecter à AWS Client VPN avec un AWS client fourni pour macOS

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

De même, prenez connaissance des [prérequis](#). Le client AWS fourni est également appelé client AWS VPN dans les étapes suivantes.

Pour vous connecter à l'aide du AWS client fourni pour macOS

1. Ouvrez l'application AWS VPN Client.
2. Choisissez File (Fichier), Manage Profiles (Gérer les profils).
3. Choisissez Add Profile (Ajouter un profil).
4. Pour Profile name (Nom du profil), entrez un nom pour le profil.
5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN et sélectionnez-le, puis choisissez Add Profile (Ajouter un profil).
6. Si vous souhaitez créer plusieurs connexions, répétez les étapes Ajouter un profil pour chaque fichier de configuration que vous souhaitez ajouter. Vous pouvez ajouter autant de profils que vous le souhaitez, mais vous ne pouvez avoir que cinq connexions ouvertes au maximum.
7. Dans la fenêtre du client AWS VPN, choisissez le profil auquel vous souhaitez vous connecter, puis sélectionnez Connect. Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe. Répétez cette étape pour chaque connexion de profil que vous souhaitez établir, en connectant jusqu'à cinq points de terminaison simultanés.

### Note

Si un profil auquel vous vous connectez entre en conflit avec une session actuellement ouverte, vous ne pourrez pas établir la connexion. Choisissez une nouvelle connexion ou déconnectez-vous de la session à l'origine du conflit.

8. Pour consulter les statistiques d'une connexion, choisissez Connexion dans la fenêtre du client AWS VPN, choisissez Afficher les détails, puis choisissez la connexion dont vous souhaitez consulter les détails.

- Pour déconnecter une connexion, choisissez-en une dans la fenêtre du client AWS VPN, puis choisissez Déconnecter. Si plusieurs connexions sont ouvertes, vous devez fermer chaque connexion individuellement.

## AWS Client VPN notes de mise à jour pour macOS

Le tableau suivant contient les notes de publication et les liens de téléchargement des versions actuelles et précédentes de AWS Client VPN pour macOS.

### Note

Nous continuons à fournir des correctifs d'utilisabilité et de sécurité à chaque version. Nous vous recommandons vivement d'utiliser la dernière version pour chaque plateforme. Les versions précédentes peuvent être affectées par des problèmes de and/or sécurité liés à l'utilisabilité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement
5.3.5	<ul style="list-style-type: none"> <li>• Correctifs de bogues mineurs et améliorations</li> <li>• Niveau de sécurité amélioré</li> <li>• Mise à niveau automatique activée vers le client ARM64 natif pour les utilisateurs de ARM-based Mac dans les futures mises à jour, éliminant ainsi le besoin de migration manuelle depuis le Intel-based client exécuté sous la couche de traduction Rosetta</li> </ul>	14 mai 2026	<ul style="list-style-type: none"> <li>• <a href="#">Téléchargez la version 5.3.5 de macOS ARM64</a> sha256 : 048c9011b7cea43720cb92d7c2fe064c8d853b391ee499408736cba5d9111652</li> <li>• <a href="#">Téléchargez la version 5.3.5 de macOS x64</a> sha256 : 64a84f529a09b2ee9756dd8f5e193b9624b3239bcd76d9f20411a72d1f93887c</li> </ul>

Version	Modifications	Date	Lien de téléchargement
5.3.4	<ul style="list-style-type: none"> <li>• Suppression de l'exigence de couche de compatibilité Intel (Rosetta) sur les machines ARM</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	17 février 2026	N'est plus pris en charge.
5.3.3	<ul style="list-style-type: none"> <li>• Correctifs de bogues mineurs et améliorations</li> <li>• Posture de sécurité améliorée.</li> </ul>	26 décembre 2025	N'est plus pris en charge.
5.3.2	<ul style="list-style-type: none"> <li>• Ajout du support natif pour l'architecture Apple Silicon et d'un nouveau programme d'installation de macOS ARM64.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	27 octobre 2025	N'est plus pris en charge.
5.3.1	<ul style="list-style-type: none"> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	9 septembre 2025	N'est plus pris en charge.
5.3.0	<ul style="list-style-type: none"> <li>• Améliorations mineures.</li> <li>• Ajout du support pour les connexions IPv6.</li> </ul>	14 août 2025	N'est plus pris en charge.
5.2.1	<ul style="list-style-type: none"> <li>• Ajout du support pour le drapeau OpenVPN ping-exit.</li> <li>• Mise à jour de la bibliothèque OpenSSL.</li> <li>• Posture de sécurité améliorée.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	18 juin 2025	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
5.2.0	<ul style="list-style-type: none"> <li>• Améliorations mineures.</li> <li>• Ajout de la prise en charge de l'application de l'itinéraire client.</li> </ul>	8 avril 2025	N'est plus pris en charge.
5.1.0	<ul style="list-style-type: none"> <li>• Correction d'un problème en raison duquel AWS Client VPN la version 5.0.x se reconnectait automatiquement au VPN après un délai d'inactivité.</li> <li>• Correction d'un problème qui AWS Client VPN empêchait d'établir une connexion VPN pour les fichiers de configuration comportant des fins de Windows-style ligne.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	17 mars 2025	N'est plus pris en charge.
5.0.3	Correctifs de bogues mineurs et améliorations	6 mars 2025	N'est plus pris en charge.
5.0.2	Correction d'un problème qui provoquait des erreurs sporadiques lors du choix de Connect.	17 février 2025	N'est plus pris en charge.
5.0.1	Correction d'un problème qui empêchait la version 5.0.0 du client d'établir une connexion VPN pour les noms de profil contenant des espaces.	22 janvier 2025	N'est plus pris en charge.
5.0.0	<ul style="list-style-type: none"> <li>• Ajout du support pour les connexions simultanées.</li> <li>• Mise à jour de l'interface utilisateur graphique.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	21 janvier 2025	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
4.1.0	Correctifs de bogues mineurs et améliorations	12 novembre 2024	N'est plus pris en charge.
4.0.0	Améliorations mineures.	25 septembre 2024	N'est plus pris en charge.
3.12.1	Ajout du support pour le mssfix drapeau OpenVPN.	4 septembre 2024	N'est plus pris en charge.
3.12.0	<ul style="list-style-type: none"> <li>Ajout du support pour le tap-sleep drapeau OpenVPN.</li> <li>Mise à jour des bibliothèques OpenVPN et OpenSSL.</li> </ul>	12 août 2024	N'est plus pris en charge.
3.11.0	<ul style="list-style-type: none"> <li>Mise à jour des bibliothèques OpenVPN et OpenSSL.</li> </ul>	29 juillet 2024	N'est plus pris en charge.
3.10.0	<ul style="list-style-type: none"> <li>Reconnectez-vous automatiquement lorsque la portée du réseau local change.</li> <li>Correction d'un problème de restauration du DNS lors du changement de réseau.</li> <li>Suppression du focus automatique sur les applications lors de la connexion à des points de terminaison SAML.</li> </ul>	21 mai 2024	N'est plus pris en charge.
3.9.2	<ul style="list-style-type: none"> <li>Résolution d'un problème d'authentification SAML avec Chromium-based les navigateurs depuis la version 123.</li> <li>Ajout du support pour macOS Sonoma. Déconseillez la prise en charge de macOS Big Sur.</li> <li>Posture de sécurité améliorée.</li> </ul>	11 avril 2024	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
3.9.1	<ul style="list-style-type: none"> <li>• Correction d'une action de dépassement de la mémoire tampon qui pouvait potentiellement permettre à un acteur local d'exécuter des commandes arbitraires avec des autorisations élevées.</li> <li>• Barre de progression du téléchargement des mises à jour de l'application fixe.</li> <li>• Posture de sécurité améliorée.</li> </ul>	16 février 2024	N'est plus pris en charge.
3.9.0	<ul style="list-style-type: none"> <li>• Problèmes de connectivité résolus pour certaines configurations de réseau local.</li> <li>• Accessibilité améliorée.</li> </ul>	6 décembre 20	N'est plus pris en charge.
3.8.0	<ul style="list-style-type: none"> <li>• Correction d'un problème de connectivité lorsque NAT64 est activé sur le réseau client.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	24 août 2023	N'est plus pris en charge.
3.7.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	3 août 2023	N'est plus pris en charge.
3.6.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	15 juillet 2023	N'est plus pris en charge.
3.5.0	<ul style="list-style-type: none"> <li>• Annulation des modifications apportées à la version 3.4.0.</li> </ul>	15 juillet 2023	N'est plus pris en charge.
3.4.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	14 juillet 2023	N'est plus pris en charge.
3.3.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de macOS Ventura (13.0).</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	27 avril 2023	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
3.2.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ».</li> <li>• Détection automatique de la disponibilité des versions mises à jour du client.</li> <li>• Ajout de la possibilité d'installer automatiquement les nouvelles versions du client lorsqu'elles sont disponibles.</li> </ul>	23 janvier 2023	N'est plus pris en charge.
3.1.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge pour macOS Monterey.</li> <li>• Correction d'un problème de détection du type de lecteur.</li> <li>• Posture de sécurité améliorée.</li> </ul>	23 mai 2022	N'est plus pris en charge.
3.0.0	<ul style="list-style-type: none"> <li>• Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée.</li> <li>• Correction de l'affichage du texte de la bannière pour des textes plus longs.</li> <li>• Posture de sécurité améliorée.</li> </ul>	3 mars 2022	N'est plus pris en charge.
2.0.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie.</li> <li>• Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	20 janvier 2022	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.4.0	<ul style="list-style-type: none"> <li>• Ajout de la surveillance du serveur DNS pendant la connexion. Les paramètres seront reconfigurés s'ils ne correspondent pas aux paramètres VPN.</li> <li>• Correction d'une tentative de connexion d'authentification fédérée dans certains cas.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	9 novembre 20	N'est plus pris en charge.
1.3.5	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge des indicateurs OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	20 septembre 2	N'est plus pris en charge.
1.3.4	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de l'indicateur OpenVPN : dhcp-option.</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	4 août 2021	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.3.3	<ul style="list-style-type: none"><li>• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route.</li><li>• Correction d'un problème avec les noms de fichiers de configuration comportant des espaces ou des caractères Unicode.</li><li>• Résolution d'un problème qui bloquait l'application lors de la déconnexion ou de la sortie.</li><li>• Correction d'un problème avec les noms d'utilisateur Active Directory avec barre oblique inverse.</li><li>• Correction d'un blocage d'application lors de la manipulation de la liste de profil en dehors de l'application</li><li>• Correctifs de bogue mineurs et améliorations.</li></ul>	1er juillet 2021	N'est plus pris en charge.
1.3.2	<ul style="list-style-type: none"><li>• Ajouter la prévention des fuites IPv6, lorsqu'il est configuré.</li><li>• Correction d'un incident potentiel lorsque vous utilisez l'option Afficher les détails sous Connexion.</li><li>• Ajouter la rotation du journal du démon.</li></ul>	12 mai 2021	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.3.1	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de macOS Big Sur (10.16).</li> <li>• Correction d'un problème qui supprimait les paramètres DNS configurés par d'autres applications.</li> <li>• Correction d'un problème lors de l'utilisation d'un certificat non valide pour l'authentification mutuelle, provoquant des problèmes de connectivité.</li> <li>• Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'.</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	5 avril 2021	N'est plus pris en charge.
1.3.0	Ajout de fonctionnalités de support, telles que le signalement d'erreurs, l'envoi de journaux de diagnostic et l'analytique.	8 mars 2021	N'est plus pris en charge.
1.2.5	Correctifs de bogue mineurs et améliorations.	25 février 2021	N'est plus pris en charge.
1.2.4	Correctifs de bogue mineurs et améliorations.	26 octobre 202	N'est plus pris en charge.
1.2.3	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge des commentaires dans la configuration OpenVPN.</li> <li>• Ajout d'un message d'erreur pour les erreurs de liaison TLS.</li> <li>• Correction d'un bug de désinstallation affectant certains utilisateurs.</li> </ul>	8 octobre 2020	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.2.2	Correctifs de bogues mineurs et améliorations.	12 août 2020	N'est plus pris en charge.
1.2.1	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de la désinstallation de l'application.</li> <li>• Correctifs de bogues mineurs et améliorations.</li> </ul>	1er juillet 2020	N'est plus pris en charge.
1.2.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de <a href="#">l'authentification fédérée basée sur SAML 2.0</a>.</li> <li>• Ajout de la prise en charge de macOS Catalina (10.15).</li> </ul>	19 mai 2020	N'est plus pris en charge.
1.1.2	Correctifs de bogues mineurs et améliorations.	21 avril 2020	N'est plus pris en charge.
1.1.1	<ul style="list-style-type: none"> <li>• Correction d'un problème de non-résolution DNS.</li> <li>• Correction d'un problème de panne d'application causé par des connexions plus longues.</li> <li>• Correction d'un problème d'authentification MFA.</li> </ul>	2 avril 2020	N'est plus pris en charge.
1.1.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de la configuration DNS macOS.</li> <li>• Ajout de la prise en charge de la fonctionnalité écho « static-challenge » d'OpenVPN pour masquer ou afficher le texte affiché dans l'interface utilisateur.</li> <li>• Correctifs de bogues mineurs et améliorations.</li> </ul>	9 mars 2020	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.0.0	Version initiale.	4 février 2020	N'est plus pris en charge.

## AWS Client VPN pour Linux

Ces sections décrivent l'installation du client AWS fourni pour Linux, puis l'établissement d'une connexion VPN à l'aide du client AWS fourni. Le client AWS fourni pour Linux ne prend pas en charge les mises à jour automatiques. Pour les dernières mises à jour et téléchargements, consultez [lethe section called “Notes de mise à jour”](#).

### Conditions requises pour se connecter au Client VPN avec un AWS client fourni pour Linux

Pour utiliser le client AWS fourni pour Linux, les éléments suivants sont requis :

- Ubuntu 22.04 LTS (AMD64), Ubuntu 24.04 LTS (AMD64 uniquement) ou Ubuntu 26.04 LTS (AMD64 uniquement)

Pour les points de terminaison VPN du Client qui utilisent l'authentification SAML-based fédérée (authentification unique), le client réserve les ports TCP 8096-8115 sur votre ordinateur.

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

#### Rubriques

- [Installez le logiciel fourni AWS Client VPN pour Linux](#)
- [Connectez-vous au AWS Client VPN pour Linux](#)
- [AWS Client VPN notes de mise à jour pour Linux](#)

## Installez le logiciel fourni AWS Client VPN pour Linux

Plusieurs méthodes peuvent être utilisées pour installer le client AWS fourni pour Linux. Utilisez l'une des méthodes fournies par les options suivantes. Avant de commencer, prenez connaissance des [prérequis](#).

### Option 1 : Installation via le référentiel de packages

1. Ajoutez la clé publique du client AWS VPN à votre système d'exploitation Ubuntu.

```
wget -q0- https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/awsvpnclient_public_key.asc
```

2. Utilisez la commande suivante pour ajouter le référentiel à votre système d'exploitation Ubuntu (version 22.04 et ultérieure) :

```
echo "deb [arch=amd64] https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/ubuntu main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

3. Utilisez la commande suivante pour mettre à jour les référentiels sur votre système.

```
sudo apt-get update
```

4. Utilisez la commande suivante pour installer le client AWS fourni pour Linux.

```
sudo apt-get install awsvpnclient
```

### Option 2 : installation à l'aide du fichier de package .deb

1. Téléchargez le fichier .deb à partir de [Téléchargement de AWS Client VPN](#) ou à l'aide de la commande suivante.

```
curl https://d20adtpz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o awsvpnclient_amd64.deb
```

2. Installez le client AWS fourni pour Linux à l'aide de l'outil dpkg.

```
sudo dpkg -i awsvpnclient_amd64.deb
```

## Option 3 -- Installation du paquet .deb à l'aide de la Logithèque Ubuntu

1. Téléchargez le fichier de package .deb à partir de [Téléchargement de AWS Client VPN](#).
2. Après avoir téléchargé le fichier de package .deb, utilisez la Logithèque Ubuntu pour installer le package. Suivez la procédure d'installation à partir d'un paquet .deb autonome à l'aide du Logithèque Ubuntu, comme décrit dans le [Wiki Ubuntu](#).

## Connectez-vous au AWS Client VPN pour Linux

Le client AWS fourni est également appelé client AWS VPN dans les étapes suivantes.

Pour vous connecter à l'aide du AWS client fourni pour Linux

1. Ouvrez l'application AWS VPN Client.
2. Choisissez File (Fichier), Manage Profiles (Gérer les profils).
3. Choisissez Add Profile (Ajouter un profil).
4. Pour Profile name (Nom du profil), entrez un nom pour le profil.
5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN. Choisissez Open.
6. Choisissez Add Profile (Ajouter un profil).
7. Si vous souhaitez créer plusieurs connexions, répétez les étapes Ajouter un profil pour chaque fichier de configuration que vous souhaitez ajouter. Vous pouvez ajouter autant de profils que vous le souhaitez, mais vous ne pouvez avoir que cinq connexions ouvertes au maximum.
8. Dans la fenêtre du client AWS VPN, choisissez le profil auquel vous souhaitez vous connecter, puis sélectionnez Connect. Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe. Répétez cette étape pour chaque connexion de profil que vous souhaitez établir, en connectant jusqu'à cinq points de terminaison simultanés.

### Note

Si un profil auquel vous vous connectez entre en conflit avec une session actuellement ouverte, vous ne pourrez pas établir la connexion. Choisissez une nouvelle connexion ou déconnectez-vous de la session à l'origine du conflit.

9. Pour consulter les statistiques d'une connexion, choisissez Connexion dans la fenêtre du client AWS VPN, choisissez Afficher les détails, puis choisissez la connexion dont vous souhaitez consulter les détails.
10. Pour déconnecter une connexion, choisissez-en une dans la fenêtre du client AWS VPN, puis choisissez Déconnecter. Si plusieurs connexions sont ouvertes, vous devez fermer chaque connexion individuellement.

## AWS Client VPN notes de mise à jour pour Linux

Le tableau suivant contient les notes de publication et les liens de téléchargement pour les versions actuelles et précédentes de AWS Client VPN for Linux.

### Note

Nous continuons à fournir des correctifs d'utilisabilité et de sécurité à chaque version. Nous vous recommandons vivement d'utiliser la dernière version pour chaque plateforme. Les versions précédentes peuvent être affectées par des problèmes de and/or sécurité liés à l'utilisabilité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement
5.3.3	<ul style="list-style-type: none"> <li>• Correctifs de bogues mineurs et améliorations</li> <li>• Niveau de sécurité amélioré</li> </ul>	18 mai 2026	<a href="#">Télécharger la version 5.3.3</a>  sha256 : d0096c934 b36122c24 5d8c2243d 4146cdac6 7125c7421 c4e1e6ad4 30eb3adfcf
5.3.2	<ul style="list-style-type: none"> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	17 décembre 2025	<a href="#">Télécharger la version 5.3.2</a>

Version	Modifications	Date	Lien de téléchargement
	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>		sha256 : 89e4b9f2c 9f7def371 67f5f137f4ff9c6c52 46fd6e0a7 244b70c19 6a17683569
5.3.1	<ul style="list-style-type: none"> <li>• Améliorations mineures.</li> </ul>	25 septembre 2025	<a href="#">Télécharger la version 5.3.1</a>  sha256 : 4a426cc22 6382748d6 83a494634 0447dab87 ec4258397 7d9488ee4 5d11cdcec0
5.3.0	<ul style="list-style-type: none"> <li>• Améliorations mineures.</li> <li>• Ajout du support pour les connexions IPv6.</li> </ul>	14 août 2025	<a href="#">Télécharger la version 5.3.0</a>  sha256 : 31edb55f1 2dcd68a7a 4ca9b6233 ddbeebcd3 7e01f8765 5a520cc7e 7542bbfcb4

Version	Modifications	Date	Lien de téléchargement
5.2.0	<ul style="list-style-type: none"> <li>Améliorations mineures.</li> <li>Ajout de la prise en charge de l'application de l'itinéraire client.</li> </ul>	8 avril 2025	<a href="#">Télécharger la version 5.2.0</a>  sha256 : ef7189f08 5db30ef0c 521adcdfe c892075cb 005c8e001 4fdbcc590 218509891f
5.1.0	<ul style="list-style-type: none"> <li>Correction d'un problème en raison duquel AWS Client VPN la version 5.0.x se reconnectait automatiquement au VPN après un délai d'inactivité.</li> <li>Correctifs de bogues mineurs et améliorations</li> </ul>	17 mars 2025	<a href="#">Télécharger la version 5.1.0</a>  sha256 : 14f26c05b 11b0cc484 b08a8f8d2 0739de3d8 15c268db3 bba9ac70c 0e766b70ba
5.0.0	<ul style="list-style-type: none"> <li>Ajout de la prise en charge de plusieurs connexions simultanées.</li> <li>Mise à jour de l'interface utilisateur graphique.</li> <li>Correctifs de bogues mineurs et améliorations</li> </ul>	21 janvier 2025	<a href="#">Télécharger la version 5.0.0</a>  sha256 : 645126b56 98cb550e9 dc822e58e d899a5730 d2e204f28 f4023ec67 1915fdda0c

Version	Modifications	Date	Lien de téléchargement
4.1.0	<ul style="list-style-type: none"><li>• Ajout du support pour Ubuntu 22.04 et 24.04.</li><li>• Correctifs de bogue.</li></ul>	12 novembre 2024	<a href="#">Télécharger la version 4.1.0</a>  sha256 : 334d00222 458fbfe9d ade16c99f e97e9ebcb d51fff017 d0d6b1d1b 764e7af472
4.0.0	Améliorations mineures.	25 septembre 2024	<a href="#">Télécharger la version 4.0.0</a>  sha256 : c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Ajout du support pour le mssfix drapeau OpenVPN.	4 septembre 2024	<a href="#">Télécharger la version 3.15.1</a>  sha256 : ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2

Version	Modifications	Date	Lien de téléchargement
3,15,0	<ul style="list-style-type: none"><li>Ajout du support pour le tap-sleep drapeau OpenVPN.</li><li>Mise à jour des bibliothèques OpenVPN et OpenSSL.</li></ul>	12 août 2024	<a href="#">Télécharger la version 3.15.0</a>  sha256 : 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012
3,14,0	<ul style="list-style-type: none"><li>Mise à jour des bibliothèques OpenVPN et OpenSSL.</li></ul>	29 juillet 2024	<a href="#">Télécharger la version 3.14.0</a>  sha256 : bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3,13,0	<ul style="list-style-type: none"><li>Reconnectez-vous automatiquement lorsque la portée du réseau local change.</li></ul>	21 mai 2024	<a href="#">Télécharger la version 3.13.0</a>  sha256 : e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1

Version	Modifications	Date	Lien de téléchargement
3.12.2	<ul style="list-style-type: none"><li>Résolution d'un problème d'authentification SAML avec Chromium-based les navigateurs depuis la version 123.</li></ul>	11 avril 2024	<a href="#">Télécharger la version 3.12.2</a>  sha256 : f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	<ul style="list-style-type: none"><li>Correction d'une action de dépassement de la mémoire tampon qui pouvait potentiellement permettre à un acteur local d'exécuter des commandes arbitraires avec des autorisations élevées.</li><li>Posture de sécurité améliorée.</li></ul>	16 février 2024	<a href="#">Télécharger la version 3.12.1</a>  sha256 : 547c4ffd3 e35c54db8 e0b792aed 9de1510f6 f31a6009e 55b8af4f0 c2f5cf31d0
3.12.0	<ul style="list-style-type: none"><li>Problèmes de connectivité résolus pour certaines configurations de réseau local.</li></ul>	19 décembre 2023	<a href="#">Télécharger la version 3.12.0</a>  sha256 : 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1

Version	Modifications	Date	Lien de téléchargement
3.11.0	<ul style="list-style-type: none"> <li>Restauration pour « Problèmes de connectivité résolus pour certaines configurations de réseau local ».</li> <li>Accessibilité améliorée.</li> </ul>	6 décembre 2023	<a href="#">Télécharger la version 3.11.0</a>  sha256 : 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	<ul style="list-style-type: none"> <li>Problèmes de connectivité résolus pour certaines configurations de réseau local.</li> <li>Accessibilité améliorée.</li> </ul>	6 décembre 2023	<a href="#">Télécharger la version 3.10.0</a>  sha256 : e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	<ul style="list-style-type: none"> <li>Correction d'un problème de connectivité lorsque NAT64 est activé sur le réseau client.</li> <li>Correctifs de bogues mineurs et améliorations</li> </ul>	24 août 2023	<a href="#">Télécharger la version 3.9.0</a>  sha256 : 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454

Version	Modifications	Date	Lien de téléchargement
3.8.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	3 août 2023	<a href="#">Télécharger la version 3.8.0</a>  sha256 : 5fe479236 cc0a1940b a37fe168e 551096f8d ae4c68d45 560a164e4 1edea3e5bd
3.7.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	15 juillet 2023	N'est plus pris en charge
3.6.0	<ul style="list-style-type: none"> <li>• Annulation des modifications apportées à la version 3.5.0.</li> </ul>	15 juillet 2023	N'est plus pris en charge
3.5.0	<ul style="list-style-type: none"> <li>• Posture de sécurité améliorée.</li> </ul>	14 juillet 2023	N'est plus pris en charge
3.4.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ».</li> </ul>	14 février 2023	N'est plus pris en charge
3.1.0	<ul style="list-style-type: none"> <li>• Correction d'un problème de détection du type de lecteur.</li> <li>• Posture de sécurité améliorée.</li> </ul>	23 mai 2022	N'est plus pris en charge
3.0.0	<ul style="list-style-type: none"> <li>• Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée.</li> <li>• Correction de l'affichage du texte de la bannière pour des séquences de caractères plus longues et spécifiques.</li> <li>• Posture de sécurité améliorée.</li> </ul>	3 mars 2022	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
2.0.0	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie.</li> <li>• Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	20 janvier 2022	N'est plus pris en charge.
1.0.3	<ul style="list-style-type: none"> <li>• Correction d'une tentative de connexion d'authentification fédérée dans certains cas.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	08 novembre 2021	N'est plus pris en charge.
1.0.2	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge des indicateurs OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.</li> <li>• Correctifs de bogues mineurs et améliorations</li> </ul>	28 septembre 2021	N'est plus pris en charge.
1.0.1	<ul style="list-style-type: none"> <li>• Option activée pour quitter la barre d'application Ubuntu.</li> <li>• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route.</li> <li>• Correctifs de bogue mineurs et améliorations.</li> </ul>	4 août 2021	N'est plus pris en charge.
1.0.0	Version initiale.	11 juin 2021	N'est plus pris en charge.

# Connect à un AWS Client VPN point de terminaison utilisant un client OpenVPN

Vous pouvez établir une connexion à un point de terminaison VPN client à l'aide d'applications clientes Open VPN courantes. Client VPN est pris en charge sur les systèmes d'exploitation suivants :

- Windows

Utilisez un certificat et une clé privée provenant du Windows Certificate Store. Une fois que vous avez généré le certificat et la clé, vous pouvez établir une connexion AWS client à l'aide de l'application client OpenVPN GUI ou du client OpenVPN GUI Connect. Pour connaître les étapes de création du certificat et de la clé, consultez [Établissez une connexion VPN à l'aide d'un certificat sous Windows](#).

- macOS

Établissez une connexion VPN à l'aide d'un fichier de configuration pour Mac OS-based Tunnelblick ou pour Client VPN AWS . Pour de plus amples informations, veuillez consulter [Établissez une connexion VPN sur macOS](#).

- Linux

Établissez une connexion VPN sous Linux à l'aide de l'interface OpenVPN - Network Manager ou de l'application OpenVPN. Pour utiliser l'interface OpenVPN - Network Manager, vous devez d'abord installer le module de gestion réseau s'il n'est pas déjà installé. Pour de plus amples informations, veuillez consulter [Établissez une connexion VPN sous Linux](#).

- Android et iOS

Établissez une connexion VPN à l'aide de l'application cliente OpenVPN sur un appareil Android ou iOS. Pour de plus amples informations, veuillez consulter [Connexions VPN du client sur Android et iOS](#).

## Important

Si le point de terminaison VPN du Client a été configuré pour utiliser l'[authentification SAML-based fédérée](#), vous ne pouvez pas utiliser le client OpenVPN-based VPN pour vous connecter à un point de terminaison VPN du Client. Cela inclut toutes les ARM-based

architectures. Si vous utilisez un appareil doté d'un processeur ARM (tel qu'un Mac Apple Silicon ou un appareil ARM-based Windows), vous devez utiliser des points de terminaison SAML-based VPN avec le client AWS fourni plutôt que des clients OpenVPN.

## Applications clientes

- [Connect à un AWS Client VPN point de terminaison utilisant une application cliente Windows](#)
- [Connect à un AWS Client VPN point de terminaison utilisant une application cliente macOS](#)
- [Connect à un AWS Client VPN point de terminaison utilisant une application cliente OpenVPN](#)
- [AWS Client VPN connexions sur les applications Android et iOS](#)

## Connect à un AWS Client VPN point de terminaison utilisant une application cliente Windows

Ces sections décrivent comment établir une connexion VPN à l'aide de clients Windows-based VPN.

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

Pour plus d'informations sur le dépannage, consultez [Résolution des problèmes AWS Connexions VPN entre Windows-based clients et clients](#).

### Important

Si le point de terminaison VPN du Client a été configuré pour utiliser l'[authentification SAML-based fédérée](#), vous ne pouvez pas utiliser le client OpenVPN-based VPN pour vous connecter à un point de terminaison VPN du Client. Cela inclut toutes les ARM-based architectures. Si vous utilisez un appareil doté d'un processeur ARM (tel qu'un Mac Apple Silicon ou un appareil ARM-based Windows), vous devez utiliser des points de terminaison SAML-based VPN avec le client AWS fourni plutôt que des clients OpenVPN.

## Tâches

- [Utilisez un certificat et établissez un AWS Connexion VPN du client sous Windows](#)

## Utilisez un certificat et établissez un AWS Connexion VPN du client sous Windows

Vous pouvez configurer le client OpenVPN pour qu'il utilise un certificat et une clé privée du magasin de certificats système de Windows. Cette option est pratique si vous utilisez une carte à puce pour votre connexion Client VPN. Pour plus d'informations sur l'option `cryptoapicert` du client OpenVPN, consultez le [Manuel de référence d'OpenVPN](#) sur le site Web d'OpenVPN.

### Note

Le certificat doit être stocké sur l'ordinateur local.

Pour utiliser un certificat et établir une connexion

1. Créez un fichier `.pfx` contenant le certificat client et la clé privée.
2. Importez le fichier `.pfx` dans votre magasin de certificats personnel, sur votre ordinateur local. Pour plus d'informations, consultez [How to: View certificates with the MMC snap-in](#) (Procédure : afficher les certificats avec le composant logiciel enfichable MMC) sur le site Web de Microsoft.
3. Vérifiez que votre compte dispose des autorisations nécessaires pour lire le certificat de l'ordinateur local. Vous pouvez utiliser Microsoft Management Console pour modifier les autorisations. Pour plus d'informations, consultez la section [Droits pour consulter le magasin de certificats informatiques local](#) sur le site Web de Microsoft.
4. Mettez à jour le fichier de configuration OpenVPN et spécifiez le certificat en utilisant son objet ou son empreinte.

Voici un exemple de spécification du certificat à l'aide d'un objet.

```
cryptoapicert "SUBJ:Jane Doe"
```

Voici un exemple de spécification du certificat à l'aide d'une empreinte. Microsoft Management Console permet de trouver l'empreinte. Pour plus d'informations, consultez [Comment : récupérer l'empreinte numérique d'un certificat sur le site Web](#) de Microsoft.

```
cryptoapicert "THUMB:a5 42 00 42 01"
```

5. Une fois la configuration terminée, utilisez OpenVPN pour établir une connexion VPN en effectuant l'une des opérations suivantes :
  - Utilisez l'application client OpenVPN GUI
    1. Démarrez l'application cliente OpenVPN.
    2. Dans la barre des tâches de Windows, choisissez les Show/Hide icônes. Right-click OpenVPN GUI, puis choisissez Importer un fichier.
    3. Dans la boîte de dialogue Open (Ouvrir), sélectionnez le fichier de configuration que vous avez reçu de votre administrateur Client VPN et choisissez Open (Ouvrir).
    4. Dans la barre des tâches de Windows, choisissez les Show/Hide icônes. Right-click OpenVPN GUI, puis choisissez Connect.
  - Utilisez le client OpenVPN GUI Connect
    1. Lancez l'application OpenVPN et choisissez Importer, À partir d'un fichier local... .
    2. Accédez au fichier de configuration que vous avez reçu de votre administrateur VPN et choisissez Open (Ouvrir).

## Connect à un AWS Client VPN point de terminaison utilisant une application cliente macOS

Ces sections décrivent comment établir une connexion VPN à l'aide du client OS-based VPN Mac, Tunnelblick ou Client VPN AWS .

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

Pour plus d'informations sur le dépannage, consultez [Résolution des problèmes AWS Connexions VPN clientes avec des clients macOS](#).

**⚠ Important**

Si le point de terminaison VPN du Client a été configuré pour utiliser l'[authentification SAML-based fédérée](#), vous ne pouvez pas utiliser le client OpenVPN-based VPN pour vous connecter à un point de terminaison VPN du Client. Cela inclut toutes les ARM-based architectures. Si vous utilisez un appareil doté d'un processeur ARM (tel qu'un Mac Apple Silicon ou un appareil ARM-based Windows), vous devez utiliser des points de terminaison SAML-based VPN avec le client AWS fourni plutôt que des clients OpenVPN.

## Rubriques

- [Établissez un AWS Client VPN connexion sur macOS](#)

## Établissez un AWS Client VPN connexion sur macOS

Vous pouvez établir une connexion VPN à l'aide de l'application cliente Tunnelblick sur un ordinateur macOS.

**📘 Note**

Pour plus d'informations sur l'application cliente Tunnelblick pour macOS, consultez la [documentation Tunnelblick](#) sur le site web Tunnelblick.

Pour établir une connexion VPN à l'aide de Tunnelblick

1. Démarrez l'application cliente Tunnelblick et choisissez I have configuration files (Je dispose des fichiers de configuration).
2. Faites glisser le fichier de configuration que vous avez reçu de votre administrateur VPN vers le panneau Configurations.
3. Sélectionnez le fichier de configuration dans le volet Configurations et choisissez Connect (Se connecter).

Pour établir une connexion VPN à l'aide de AWS Client VPN.

1. Démarrez l'application OpenVPN et choisissez Import (Importer), From local file... (Depuis le fichier local).

2. Accédez au fichier de configuration que vous avez reçu de votre administrateur VPN et choisissez Open (Ouvrir).

## Connect à un AWS Client VPN point de terminaison utilisant une application cliente OpenVPN

Ces sections décrivent comment établir une connexion VPN à l'aide d'OpenVPN - Network Manager ou d'OpenVPN.

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

Pour plus d'informations sur le dépannage, consultez [Résolution des problèmes AWS Connexions VPN entre Linux-based clients et clients](#).

### Important

Si le point de terminaison VPN du Client a été configuré pour utiliser l'[authentification SAML-based fédérée](#), vous ne pouvez pas utiliser le client OpenVPN-based VPN pour vous connecter à un point de terminaison VPN du Client. Cela inclut toutes les ARM-based architectures. Si vous utilisez un appareil doté d'un processeur ARM (tel qu'un Mac Apple Silicon ou un appareil ARM-based Windows), vous devez utiliser des points de terminaison SAML-based VPN avec le client AWS fourni plutôt que des clients OpenVPN.

### Rubriques

- [Établissez un AWS Client VPN connexion sous Linux](#)

## Établissez un AWS Client VPN connexion sous Linux

Établissez une connexion VPN à l'aide de l'interface graphique Network Manager sur un ordinateur Ubuntu ou de l'application OpenVPN.

## Pour établir une connexion VPN à l'aide d'OpenVPN - Network Manager

1. Installez le module Network Manager à l'aide de la commande suivante.

```
sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
```

2. Accédez à Settings (Paramètres), Network (Réseau).
3. Choisissez le symbole plus (+) en regard de VPN, puis choisissez Import from file... (Importer à partir du fichier).
4. Accédez au fichier de configuration que vous avez reçu de votre administrateur VPN et choisissez Open (Ouvrir).
5. Dans la fenêtre Ajouter un VPN choisissez Ajouter.
6. Démarrez la connexion en activant le bouton en regard du profil VPN que vous avez ajouté.

## Pour établir une connexion VPN à l'aide d'OpenVPN

1. Installez OpenVPN à l'aide de la commande suivante.

```
sudo apt-get install openvpn
```

2. Démarrez la connexion en chargeant le fichier de configuration que vous avez reçu de votre administrateur VPN.


```
sudo openvpn --config /path/to/config/file
```

## AWS Client VPN connexions sur les applications Android et iOS

### Important

Si le point de terminaison VPN du Client a été configuré pour utiliser l'[authentification SAML-based fédérée](#), vous ne pouvez pas utiliser le client OpenVPN-based VPN pour vous connecter à un point de terminaison VPN du Client. Cela inclut toutes les ARM-based architectures. Si vous utilisez un appareil doté d'un processeur ARM (tel qu'un Mac Apple Silicon ou un appareil ARM-based Windows), vous devez utiliser des points de terminaison SAML-based VPN avec le client AWS fourni plutôt que des clients OpenVPN.

Les informations suivantes montrent comment établir une connexion VPN à l'aide de l'application cliente OpenVPN sur un appareil mobile iOS ou Android. Les étapes sont identiques pour Android et iOS.

 Note

Pour plus d'informations sur le téléchargement et l'utilisation de l'application cliente OpenVPN pour iOS ou Android, consultez le guide de l'[utilisateur d'OpenVPN Connect](#) sur le site Web d'OpenVPN.

Avant de commencer, assurez-vous que votre administrateur Client VPN a [créé un point de terminaison Client VPN](#) et vous a fourni le [fichier de configuration du point de terminaison Client VPN](#). Si vous souhaitez vous connecter à plusieurs profils simultanément, vous aurez besoin d'un fichier de configuration pour chaque profil.

Pour établir la connexion, démarrez l'application cliente OpenVPN, puis importez le fichier que vous avez reçu de votre administrateur Client VPN.

# Résolution des problèmes AWS Connexions VPN du client

Utilisez les rubriques suivantes pour résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation d'une application cliente pour vous connecter à un point de terminaison Client VPN.

## Rubriques

- [Résolution des problèmes liés aux points de terminaison Client VPN pour les administrateurs](#)
- [Envoyer les journaux de diagnostic à AWS Support dans le AWS client fourni](#)
- [Résolution des problèmes AWS Connexions VPN entre Windows-based clients et clients](#)
- [Résolution des problèmes AWS Connexions VPN clientes avec des clients macOS](#)
- [Résolution des problèmes AWS Connexions VPN entre Linux-based clients et clients](#)
- [Dépannage courant AWS Problèmes liés au VPN du client](#)

## Résolution des problèmes liés aux points de terminaison Client VPN pour les administrateurs

Vous pouvez effectuer certaines étapes de ce guide. D'autres étapes doivent être effectuées par votre administrateur Client VPN sur le point de terminaison Client VPN lui-même. Les sections suivantes vous permettent de savoir quand vous devez contacter votre administrateur.

Pour plus d'informations sur la résolution des problèmes liés au point de terminaison Client VPN, consultez [Résolution des problèmes liés à Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Envoyer les journaux de diagnostic à AWS Support dans le AWS client fourni

Si vous rencontrez des problèmes avec le client AWS fourni et que vous devez le contacter AWS Support pour aider à résoudre le problème, le client AWS fourni a la possibilité d'envoyer les journaux de diagnostic à AWS Support. Cette option est disponible sur les applications clientes Windows, macOS et Linux.

Avant d'envoyer les fichiers, vous devez accepter d'autoriser l'accès AWS Support à vos journaux de diagnostic. Une fois que vous avez donné votre accord, nous vous fournissons un numéro de

référence que vous pouvez communiquer AWS Support afin qu'ils puissent accéder immédiatement aux fichiers.

## Envoyer des journaux de diagnostic

Le client AWS fourni est également appelé client AWS VPN dans les étapes suivantes.

Pour envoyer des journaux de diagnostic à l'aide du AWS client fourni pour Windows

1. Ouvrez l'application AWS VPN Client.
2. Choisissez Help (Aide), Send Diagnostic Logs (Envoyer des journaux de diagnostic).
3. Dans la fenêtre Send Diagnostic Logs (Envoyer des journaux de diagnostic, choisissez Yes (Oui).
4. Dans la fenêtre Send Diagnostic Logs (Envoyer des journaux de diagnostic), effectuez l'une des opérations suivantes :
  - Pour copier le numéro de référence dans le Presse-papier, choisissez Yes (Oui), puis OK.
  - Pour suivre manuellement le numéro de référence, choisissez No (Non).

Lorsque vous les contacterez AWS Support, vous devrez leur fournir le numéro de référence.

Pour envoyer des journaux de diagnostic à l'aide du AWS client fourni pour macOS

1. Ouvrez l'application AWS VPN Client.
2. Choisissez Help (Aide), Send Diagnostic Logs (Envoyer des journaux de diagnostic).
3. Dans la fenêtre Send Diagnostic Logs (Envoyer des journaux de diagnostic, choisissez Yes (Oui).
4. Notez le numéro de référence affiché dans la fenêtre de confirmation, puis choisissez OK .

Lorsque vous les contacterez AWS Support, vous devrez leur fournir le numéro de référence.

Pour envoyer des journaux de diagnostic à l'aide du AWS client fourni pour Ubuntu

1. Ouvrez l'application AWS VPN Client.
2. Choisissez Help (Aide), Send Diagnostic Logs (Envoyer des journaux de diagnostic).

3. Dans la fenêtre Send Diagnostic Logs (Envoyer des journaux de diagnostic), choisissez Send (Envoyer).
4. Notez le numéro de référence affiché dans la fenêtre de confirmation. Vous avez le choix de copier les informations dans votre presse-papiers.

Lorsque vous les contacterez AWS Support, vous devrez leur fournir le numéro de référence.

## Résolution des problèmes AWS Connexions VPN entre Windows-based clients et clients

Les sections suivantes contiennent des informations sur les problèmes que vous pouvez rencontrer lorsque vous utilisez des Windows-based clients pour vous connecter à un point de terminaison VPN client.

### AWS journaux d'événements client fournis

Le client AWS fourni crée des journaux d'événements et les stocke à l'emplacement suivant sur votre ordinateur.

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

Les types de journaux suivants sont disponibles :

- Journaux d'application : contiennent des informations sur l'application. Le préfixe « aws\_vpn\_client\_ » est ajouté au nom de ces journaux.
- Journaux OpenVPN : contiennent des informations sur les processus OpenVPN. Le préfixe « ovpn\_aws\_vpn\_client\_ » est ajouté au nom de ces journaux.

Le client AWS fourni utilise le service Windows pour effectuer des opérations root. Les journaux de service Windows sont stockés à l'emplacement suivant sur votre ordinateur.

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

### Résolution des problèmes liés aux rubriques

- [Le client ne parvient pas à se connecter](#)
- [Le client ne peut pas se connecter avec le message de journal « aucun TAP-Windows adaptateur »](#)

- [Le client est bloqué à l'état de reconnexion](#)
- [Le processus de connexion VPN se ferme de façon inattendue](#)
- [Échec du lancement de l'application](#)
- [Le client ne parvient pas à créer de profil](#)
- [Le VPN se déconnecte avec un message contextuel](#)
- [Un plantage du client se produit sur les ordinateurs Dell qui utilisent Windows 10 ou 11](#)
- [OpenVPN GUI](#)
- [Client de connexion OpenVPN](#)
- [Impossible de résoudre le DNS](#)
- [Alias PKI manquant](#)

## Le client ne parvient pas à se connecter

### Problème

Le client AWS fourni ne peut pas se connecter au point de terminaison VPN du Client.

### Cause

L'origine du problème peut être l'une des causes suivantes :

- Un autre processus OpenVPN est déjà en cours d'exécution sur votre ordinateur, ce qui empêche le client de se connecter.
- Votre fichier de configuration (.ovpn) n'est pas valide.

### Solution

Vérifiez si d'autres applications OpenVPN sont en cours d'exécution sur votre ordinateur. Si une connexion est en cours d'exécution, arrêtez ou quittez ces processus et essayez de vous connecter à nouveau au point de terminaison Client VPN. Vérifiez les erreurs dans les journaux OpenVPN et demandez à votre administrateur Client VPN de vérifier les informations suivantes :

- Que le fichier de configuration contient la clé et le certificat client appropriés. Pour plus d'informations, consultez [Exporter la configuration du client](#) dans le Guide de l'administrateur AWS Client VPN .

- Que la liste de révocation de certificats est toujours valide. Pour plus d'informations, consultez [Les clients ne parviennent pas à se connecter à un point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Le client ne peut pas se connecter avec le message de journal « aucun TAP-Windows adaptateur »

### Problème

Le client AWS fourni ne peut pas se connecter au point de terminaison VPN du Client et le message d'erreur suivant apparaît dans les journaux de l'application : « Il n'y a aucun TAP-Windows adaptateur sur ce système. Vous devriez pouvoir créer un TAP-Windows adaptateur en cliquant sur Démarrer - > Tous les programmes -> TAP-Windows -> Utilitaires -> Ajouter un nouvel adaptateur Ethernet TAP-Windows virtuel ».

### Solution

Vous pouvez résoudre ce problème en prenant une ou plusieurs des mesures suivantes :

- Redémarrez l' TAP-Windows adaptateur.
- Réinstallez le TAP-Windows pilote.
- Créez un nouvel TAP-Windows adaptateur.

## Le client est bloqué à l'état de reconnexion

### Problème

Le client AWS fourni essaie de se connecter au point de terminaison VPN du Client, mais il est bloqué dans un état de reconnexion.

### Cause

L'origine du problème peut être l'une des causes suivantes :

- Votre ordinateur n'est pas connecté à Internet.
- Le nom d'hôte DNS n'est pas résolu en adresse IP.
- Un processus OpenVPN tente indéfiniment de se connecter au point de terminaison.

## Solution

Vérifiez que votre ordinateur est connecté à Internet. Demandez à votre administrateur Client VPN de vérifier que la directive `remote` du fichier de configuration est résolue en une adresse IP valide. Vous pouvez également déconnecter la session VPN en choisissant Déconnecter dans la fenêtre du client AWS VPN, puis réessayer de vous connecter.

## Le processus de connexion VPN se ferme de façon inattendue

### Problème

Lors de la connexion à un point de terminaison Client VPN, le client se ferme de façon inattendue.

### Cause

TAP-Windows n'est pas installé sur votre ordinateur. Ce logiciel est nécessaire pour exécuter le client.

### Solution

Réexécutez le programme d'installation du client AWS fourni pour installer toutes les dépendances requises.

## Échec du lancement de l'application

### Problème

Sous Windows 7, le client AWS fourni ne démarre pas lorsque vous essayez de l'ouvrir.

### Cause

.NET Framework version 4.7.2 ou supérieure n'est pas installé sur votre ordinateur. Il est nécessaire pour exécuter le client.

### Solution

Réexécutez le programme d'installation du client AWS fourni pour installer toutes les dépendances requises.

## Le client ne parvient pas à créer de profil

### Problème

Vous recevez le message d'erreur suivant lorsque vous essayez de créer un profil à l'aide du client fourni par AWS .

```
The config should have either cert and key or auth-user-pass specified.
```

## Cause

Si le point de terminaison Client VPN utilise l'authentification mutuelle, le fichier de configuration (.ovpn) ne contient pas le certificat et la clé client.

## Solution

Assurez-vous que votre administrateur Client VPN ajoute le certificat et la clé client au fichier de configuration. Pour plus d'informations, consultez [Exporter la configuration du client](#) dans le Guide de l'administrateur AWS Client VPN .

# Le VPN se déconnecte avec un message contextuel

## Problème

Le VPN se déconnecte avec un message contextuel indiquant : « La connexion VPN est interrompue car l'espace d'adressage du réseau local auquel votre appareil est connecté a changé. Veuillez établir une nouvelle connexion VPN. »

## Cause

TAP-Windows l'adaptateur ne contient pas la description requise.

## Solution

Si le Description champ ci-dessous ne correspond pas, retirez d'abord l' TAP-Windows adaptateur, puis réexécutez le programme d'installation client AWS fourni pour installer toutes les dépendances requises.

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

```
Description . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

## Un plantage du client se produit sur les ordinateurs Dell qui utilisent Windows 10 ou 11

### Problème

Sur certains ordinateurs Dell (de bureau et portables) qui utilisent Windows 10 ou 11, un plantage peut se produire lorsque vous parcourez votre système de fichiers pour importer un fichier de configuration VPN. Si ce problème se produit, vous verrez des messages tels que les suivants dans les journaux du client AWS fourni :

```
System.AccessViolationException: Attempted to read or write protected memory. This is
often an indication that other memory is corrupt.
  at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
Int32 flags, IntPtr& db)
  at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
  at System.Data.SQLite.SQLiteConnection.Open()
  at
STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
newConnection)
  at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
targetSettings)
  at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

### Cause

Le système Dell Backup and Recovery sous Windows 10 et 11 peut provoquer des conflits avec le client AWS fourni, en particulier avec les trois DLL suivantes :

- DBRShellExtension.dll
- DBROverlayIconBackupped.dll
- DBROverlayIconNotBackupped.dll

### Solution

Pour éviter ce problème, assurez-vous d'abord que votre client est à jour avec la dernière version du client AWS fourni. Allez sur la page de [téléchargement d'AWS Client VPN](#) et si une version plus récente est disponible, passez à la dernière version.

En outre, effectuez l'une des opérations suivantes :

- Si vous utilisez l'application Dell Backup and Recovery, assurez-vous qu'elle est à jour. Une [publication du forum Dell](#) indique que ce problème est résolu dans les versions plus récentes de l'application.
- Si vous n'utilisez pas l'application Dell Backup and Recovery, certaines mesures devront tout de même être prises si vous rencontrez ce problème. Si vous ne souhaitez pas mettre l'application à niveau, vous pouvez, comme alternative, supprimer ou renommer les fichiers DLL. Toutefois, notez que cela empêchera l'application Dell Backup and Recovery de fonctionner.

Supprimer ou renommer les fichiers DLL

1. Allez dans l'Explorateur Windows et naviguez jusqu'à l'emplacement où Dell Backup and Recovery est installé. Il est généralement installé à l'emplacement suivant, mais vous devrez peut-être effectuer une recherche pour le trouver.

```
C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
```

2. Supprimez manuellement les fichiers DLL suivants du répertoire d'installation ou renommez-les. L'une ou l'autre de ces actions les empêchera d'être chargés.
  - DBRShellExtension.dll
  - DBROverlayIconBackupped.dll
  - DBROverlayIconNotBackupped.dll

Vous pouvez renommer les fichiers en ajoutant « .bak » à la fin du nom du fichier, par exemple. DBROverlayIconBackupped.dll.bak

## OpenVPN GUI

Les informations de résolution des problèmes suivantes ont été testées sur les versions 11.10.0.0 et 11.11.0.0 du logiciel OpenVPN GUI sur Windows 10 Famille (64 bits) et Windows Server 2016 (64 bits).

Le fichier de configuration est stocké à l'emplacement suivant sur votre ordinateur.

```
C:\Users\User\OpenVPN\config
```

Les journaux de connexion sont stockés à l'emplacement suivant sur votre ordinateur.

```
C:\Users\User\OpenVPN\log
```

## Client de connexion OpenVPN

Les informations de résolution des problèmes suivantes ont été testées sur les versions 2.6.0.100 et 2.7.1.101 du logiciel OpenVPN Connect Client sur Windows 10 Famille (64 bits) et Windows Server 2016 (64 bits).

Le fichier de configuration est stocké à l'emplacement suivant sur votre ordinateur.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

Les journaux de connexion sont stockés à l'emplacement suivant sur votre ordinateur.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

## Impossible de résoudre le DNS

### Problème

La connexion échoue avec l'erreur suivante.

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-east-1.amazonaws.com/)' for UDP session: No such host is known.
```

### Cause

Le nom DNS ne peut pas être résolu. Le client doit ajouter une chaîne aléatoire au début du nom DNS pour empêcher la mise en cache DNS ; cependant, certains clients ne le font pas.

### Solution

Consultez la solution pour [Impossible de résoudre le nom DNS du point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Alias PKI manquant

### Problème

Une connexion à un point de terminaison Client VPN qui n'utilise pas l'authentification mutuelle échoue avec l'erreur suivante.

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

### Cause

Le logiciel OpenVPN Connect Client rencontre un problème connu où il tente de s'authentifier à l'aide de l'authentification mutuelle. Si le fichier de configuration ne contient pas de clé ni de certificat client, l'authentification échoue.

### Solution

Spécifiez une clé et un certificat client aléatoires dans le fichier de configuration Client VPN et importez la nouvelle configuration dans le logiciel OpenVPN Connect Client. Vous pouvez également utiliser un autre client, tel que le client OpenVPN GUI (v11.12.0.0) ou le client Viscosity (v.1.7.14).

## Résolution des problèmes AWS Connexions VPN clientes avec des clients macOS

Les sections suivantes contiennent des informations sur la journalisation et les problèmes que vous pourriez rencontrer lors de l'utilisation de clients macOS. Veillez à exécuter la dernière version de ces clients.

### AWS journaux d'événements client fournis

Le client AWS fourni crée des journaux d'événements et les stocke à l'emplacement suivant sur votre ordinateur.

```
/Users/username/.config/AWSVPNClient/logs
```

Les types de journaux suivants sont disponibles :

- Journaux d'application : contiennent des informations sur l'application. Le préfixe « `aws_vpn_client_` » est ajouté au nom de ces journaux.
- Journaux OpenVPN : contiennent des informations sur les processus OpenVPN. Le préfixe « `ovpn_aws_vpn_client_` » est ajouté au nom de ces journaux.

Le client AWS fourni utilise le démon client pour effectuer des opérations root. Les journaux du démon sont stockés dans les emplacements suivants sur votre ordinateur.

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

Le client AWS fourni stocke les fichiers de configuration à l'emplacement suivant sur votre ordinateur.

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

Résolution des problèmes liés aux rubriques

- [Le client ne parvient pas à se connecter](#)
- [Le client est bloqué à l'état de reconnexion](#)
- [Le client ne parvient pas à créer de profil](#)
- [L'outil d'assistance est requis \(erreur\)](#)
- [Tunnelblick](#)
- [Algorithme de chiffrement « AES-256-GCM » introuvable](#)
- [La connexion cesse de répondre et se réinitialise](#)
- [EKU, Extended key usage \(Utilisation étendue des clés\)](#)
- [Certificat expiré](#)
- [OpenVPN](#)
- [Impossible de résoudre le DNS](#)

## Le client ne parvient pas à se connecter

Problème

Le client AWS fourni ne peut pas se connecter au point de terminaison VPN du Client.

## Cause

L'origine du problème peut être l'une des causes suivantes :

- Un autre processus OpenVPN est déjà en cours d'exécution sur votre ordinateur, ce qui empêche le client de se connecter.
- Votre fichier de configuration (.ovpn) n'est pas valide.

## Solution

Vérifiez si d'autres applications OpenVPN sont en cours d'exécution sur votre ordinateur. Si une connexion est en cours d'exécution, arrêtez ou quittez ces processus et essayez de vous connecter à nouveau au point de terminaison Client VPN. Vérifiez les erreurs dans les journaux OpenVPN et demandez à votre administrateur Client VPN de vérifier les informations suivantes :

- Que le fichier de configuration contient la clé et le certificat client appropriés. Pour plus d'informations, consultez [Exporter la configuration du client](#) dans le Guide de l'administrateur AWS Client VPN .
- Que la liste de révocation de certificats est toujours valide. Pour plus d'informations, consultez [Les clients ne parviennent pas à se connecter à un point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Le client est bloqué à l'état de reconnexion

### Problème

Le client AWS fourni essaie de se connecter au point de terminaison VPN du Client, mais il est bloqué dans un état de reconnexion.

### Cause

L'origine du problème peut être l'une des causes suivantes :

- Votre ordinateur n'est pas connecté à Internet.
- Le nom d'hôte DNS n'est pas résolu en adresse IP.
- Un processus OpenVPN tente indéfiniment de se connecter au point de terminaison.

## Solution

Vérifiez que votre ordinateur est connecté à Internet. Demandez à votre administrateur Client VPN de vérifier que la directive `remote` du fichier de configuration est résolue en une adresse IP valide. Vous pouvez également déconnecter la session VPN en choisissant `Déconnecter` dans la fenêtre du client AWS VPN, puis réessayer de vous connecter.

## Le client ne parvient pas à créer de profil

### Problème

Vous recevez le message d'erreur suivant lorsque vous essayez de créer un profil à l'aide du client fourni par AWS .

```
The config should have either cert and key or auth-user-pass specified.
```

### Cause

Si le point de terminaison Client VPN utilise l'authentification mutuelle, le fichier de configuration (.ovpn) ne contient pas le certificat et la clé client.

### Solution

Assurez-vous que votre administrateur Client VPN ajoute le certificat et la clé client au fichier de configuration. Pour plus d'informations, consultez [Exporter la configuration du client](#) dans le Guide de l'administrateur AWS Client VPN .

## L'outil d'assistance est requis (erreur)

### Problème

L'erreur suivante s'affiche lorsque vous essayez de connecter le VPN.

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

### Solution

Consultez l'article suivant sur AWS Re:Post. [Client VPN AWS - Erreur liée à l'outil d'assistance requise](#)

## Tunnelblick

Les informations de résolution des problèmes suivantes ont été testées sur la version 3.7.8 (build 5180) du logiciel Tunnelblick sur macOS High Sierra 10.13.6.

Le fichier de configuration pour les configurations privées est stocké à l'emplacement suivant sur votre ordinateur.

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

Le fichier de configuration pour les configurations partagées est stocké à l'emplacement suivant sur votre ordinateur.

```
/Library/Application Support/Tunnelblick/Shared
```

Les journaux de connexion sont stockés à l'emplacement suivant sur votre ordinateur.

```
/Library/Application Support/Tunnelblick/Logs
```

Pour augmenter le niveau de détail du journal, ouvrez l'application Tunnelblick, choisissez Settings (Paramètres), et ajustez la valeur de VPN log level (Niveau de journal VPN).

## Algorithme de chiffrement « AES-256-GCM » introuvable

### Problème

La connexion échoue et renvoie l'erreur suivante dans les journaux.

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

### Cause

L'application utilise une version d'OpenVPN qui ne supporte pas les algorithmes de chiffrement. AES-256-GCM

### Solution

Choisissez une version OpenVPN compatible en procédant comme suit :

1. Ouvrez l'application Tunnelblick.

2. Cliquez sur Paramètres.
3. Pour OpenVPN version (Version OpenVPN), choisissez 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - La version OpenSSL est v1.0.2q).

## La connexion cesse de répondre et se réinitialise

### Problème

La connexion échoue et renvoie l'erreur suivante dans les journaux.

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
  Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

### Cause

Le certificat client a été révoqué. La connexion cesse de répondre après la tentative d'authentification et est finalement réinitialisée côté serveur.

### Solution

Demandez un nouveau fichier de configuration à votre administrateur Client VPN.

## EKU, Extended key usage (Utilisation étendue des clés)

### Problème

La connexion échoue et renvoie l'erreur suivante dans les journaux.

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
```

```
VERIFY KU OK
Validating certificate extended key usage
++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

## Cause

L'authentification du serveur a réussi. Toutefois, l'authentification du client échoue car le champ EKU (Extended Key Usage) du certificat client est activé pour l'authentification du serveur.

## Solution

Assurez-vous d'utiliser le certificat et la clé client appropriés. Si nécessaire, vérifiez auprès de votre administrateur Client VPN. Cette erreur peut se produire si vous utilisez le certificat de serveur et non le certificat client pour vous connecter au point de terminaison Client VPN.

## Certificat expiré

### Problème

L'authentification du serveur réussit, mais l'authentification du client échoue avec l'erreur suivante.

```
WARNING: "Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
process restarting"
```

### Cause

Le certificat de client a expiré.

### Solution

Demandez un nouveau certificat client à votre administrateur Client VPN.

## OpenVPN

Les informations de résolution des problèmes suivantes ont été testées sur la version 2.7.1.100 du logiciel OpenVPN Connect Client sur macOS High Sierra 10.13.6.

Le fichier de configuration est stocké à l'emplacement suivant sur votre ordinateur.

```
/Library/Application Support/OpenVPN/profile
```

Les journaux de connexion sont stockés à l'emplacement suivant sur votre ordinateur.

```
Library/Application Support/OpenVPN/log/connection_name.log
```

## Impossible de résoudre le DNS

### Problème

La connexion échoue avec l'erreur suivante.

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-  
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found  
(authoritative)  
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...  
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]  
Mon Jul 15 13:07:18 2019 DISCONNECTED  
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

### Cause

OpenVPN Connect ne parvient pas à résoudre le nom DNS de Client VPN.

### Solution

Consultez la solution pour [Impossible de résoudre le nom DNS du point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Résolution des problèmes AWS Connexions VPN entre Linux-based clients et clients

Les sections suivantes contiennent des informations sur la journalisation et sur les problèmes que vous pouvez rencontrer lors de l'utilisation de Linux-based clients. Veillez à exécuter la dernière version de ces clients.

### Rubriques

- [AWS journaux d'événements client fournis](#)

- [Les requêtes DNS sont dirigées vers un serveur de noms par défaut](#)
- [OpenVPN \(ligne de commande\)](#)
- [OpenVPN via Network Manager \(interface utilisateur graphique\)](#)

## AWS journaux d'événements client fournis

Le client AWS fourni stocke les fichiers journaux et les fichiers de configuration à l'emplacement suivant sur votre système :

```
/home/username/.config/AWSVPNClient/
```

Le processus démon client AWS fourni stocke les fichiers journaux à l'emplacement suivant sur votre système :

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

Par exemple, vous pouvez consulter les fichiers journaux suivants pour détecter les erreurs dans les up/down scripts DNS à l'origine de l'échec de la connexion :

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

## Les requêtes DNS sont dirigées vers un serveur de noms par défaut

### Problème

Dans certaines circonstances, après l'établissement d'une connexion VPN, les requêtes DNS sont toujours dirigées vers le serveur de noms système par défaut, et non pas vers les serveurs de noms configurés pour le point de terminaison ClientVPN.

### Cause

Le client interagit avec `systemd-resolved`, un service disponible sur les systèmes Linux, qui sert d'élément central de la gestion DNS. Il permet de configurer les serveurs DNS qui sont poussés à partir du point de terminaison ClientVPN. Le problème se produit parce que `systemd-resolved` ne définit pas la priorité la plus élevée pour les serveurs DNS fournis par le point de terminaison ClientVPN. Au lieu de cela, il ajoute les serveurs à la liste existante des serveurs DNS qui sont

configurés sur le système local. Par conséquent, les serveurs DNS d'origine peuvent toujours avoir la priorité la plus élevée et être, par conséquent, utilisés pour résoudre les requêtes DNS.

## Solution

1. Ajoutez la directive suivante dans la première ligne du fichier de configuration OpenVPN pour vous assurer que toutes les requêtes DNS sont envoyées dans le tunnel VPN.

```
dhcp-option DOMAIN-ROUTE .
```

2. Utilisez le résolveur de stub fourni par systemd-resolved. Pour ce faire, établissez le lien symbolique `/etc/resolv.conf` sur `/run/systemd/resolve/stub-resolv.conf` en exécutant la commande suivante sur le système.

```
sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
```

3. (Facultatif) Si vous ne souhaitez pas que systemd-resolved mandate les requêtes DNS par proxy mais préférez que les requêtes soient envoyées directement aux serveurs de noms DNS réels, établissez le lien symbolique `/etc/resolv.conf` sur `/run/systemd/resolve/resolv.conf` à la place.

```
sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

Cette procédure est utile pour contourner la configuration systemd-resolved, par exemple pour la mise en cache des réponses DNS, la configuration DNS interface par interface, l'application DNSSEC, etc. Cette option est particulièrement utile si vous avez besoin de remplacer un enregistrement DNS public par un enregistrement privé alors que vous êtes connecté à un VPN. Par exemple, vous pouvez avoir un résolveur DNS privé dans votre VPC privé avec un enregistrement pour `www.example.com`, qui se résout en une adresse IP privée. Cette option pourrait être utilisée pour remplacer l'enregistrement public de `www.example.com`, qui se résout en une adresse IP publique.

## OpenVPN (ligne de commande)

### Problème

La connexion ne fonctionne pas correctement, car la résolution DNS ne fonctionne pas.

### Cause

Le serveur DNS n'est pas configuré sur le point de terminaison Client VPN, ou il n'est pas respecté par le logiciel client.

## Solution

Suivez les étapes suivantes pour vérifier que le serveur DNS est configuré et qu'il fonctionne correctement.

1. Assurez-vous qu'une entrée de serveur DNS est présente dans les journaux. Dans l'exemple suivant, le serveur DNS 192.168.0.2 (configuré dans le point de terminaison Client VPN) est renvoyé dans la dernière ligne.

```
Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
  'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
10.0.0.98 255.255.255.224,peer-id 0
```

Si aucun serveur DNS n'est spécifié, demandez à votre administrateur Client VPN de modifier le point de terminaison Client VPN et assurez-vous qu'un serveur DNS (par exemple, le serveur DNS VPC) a été spécifié pour le point de terminaison Client VPN. Pour plus d'informations, consultez [Points de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

2. Assurez-vous que le package `resolvconf` est installé en exécutant la commande suivante.

```
sudo apt list resolvconf
```

La sortie doit renvoyer les informations suivantes.

```
Listing... Done
resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
```

Si le package n'est pas installé, installez-le à l'aide de la commande suivante.

```
sudo apt install resolvconf
```

3. Ouvrez le fichier de configuration Client VPN (le fichier `.ovpn`) dans un éditeur de texte et ajoutez les lignes suivantes.

```
script-security 2
```

```
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

Consultez les journaux pour vérifier que le script `resolvconf` a été appelé. Les journaux doivent contenir une ligne similaire à la ligne suivante.

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

## OpenVPN via Network Manager (interface utilisateur graphique)

### Problème

Lors de l'utilisation du client Network Manager OpenVPN, la connexion échoue avec l'erreur suivante.

```
Apr 15 17:11:07 OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Sep 5 2018
Apr 15 17:11:07 library versions: OpenSSL 1.1.0g 2 Nov 2017, LZ0 2.08
Apr 15 17:11:07 RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07 RESOLVE: Cannot resolve host
Apr 15 17:11:07 Could not determine IPv4/IPv6 protocol
```

### Cause

L'indicateur `remote-random-hostname` n'est pas respecté et le client ne peut pas se connecter à l'aide du package `network-manager-gnome`.

### Solution

Consultez la solution pour [Impossible de résoudre le nom DNS du point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

## Dépannage courant AWS Problèmes liés au VPN du client

Voici les problèmes courants que vous pouvez rencontrer lorsque vous utilisez un client pour vous connecter à un point de terminaison Client VPN.

# Échec de la négociation de clé TLS

## Problème

La négociation TLS échoue avec l'erreur suivante.

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

## Cause

L'origine du problème peut être l'une des causes suivantes :

- Les règles de pare-feu bloquent le trafic UDP ou TCP.
- Vous utilisez une mauvaise clé et un mauvais certificat client dans votre fichier de configuration (.ovpn).
- La liste de révocation des certificats client a expiré.

## Solution

Vérifiez que les règles de pare-feu de votre ordinateur ne bloquent pas le trafic TCP ou UDP entrant ou sortant sur les ports 443 ou 1194. Demandez à votre administrateur Client VPN de vérifier les informations suivantes :

- Que les règles de pare-feu du point de terminaison Client VPN ne bloquent pas le trafic TCP ou UDP sur les ports 443 ou 1194.
- Que le fichier de configuration contient la clé et le certificat client appropriés. Pour plus d'informations, consultez [Exporter la configuration du client](#) dans le Guide de l'administrateur AWS Client VPN .
- Que la liste de révocation de certificats est toujours valide. Pour plus d'informations, consultez [Les clients ne parviennent pas à se connecter à un point de terminaison Client VPN](#) dans le Guide de l'administrateur AWS Client VPN .

# Historique du document

Le tableau suivant décrit les mises à jour du Guide de l'utilisateur du AWS Client VPN.

Modification	Description	Date
<a href="#">AWS sortie du client fourni (5.3.3) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	18 mai 2026
<a href="#">AWS client fourni (5.3.5) pour macOS ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 mai 2026
<a href="#">AWS client fourni (5.3.4) pour Windows ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	26 mars 2026
<a href="#">AWS client fourni (5.3.3) pour Windows ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	28 février 2026
<a href="#">AWS client fourni (5.3.4) pour macOS ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 février 2026
<a href="#">AWS client fourni (5.3.2) pour Windows ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 février 2026
<a href="#">AWS client fourni (5.3.3) pour macOS ARM64 et x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	26 décembre 2025
<a href="#">AWS sortie du client fourni (5.3.2) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 décembre 2025

<a href="#">AWS client fourni (5.3.2) pour macOS x64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	27 octobre 2025
<a href="#">AWS client fourni (5.3.2) pour les systèmes macOS ARM64 publié</a>	Support désormais ajouté pour les systèmes ARM64-based d'exploitation macOS. Cela inclut le téléchargement de AWS Client VPN la nouvelle version 5.3.2 spécifiquement pour les systèmes macOS ARM64. Consultez la section <a href="#">Configuration requise pour le Client VPN pour macOS</a> pour plus de détails et <a href="#">AWS Client VPN les notes de version pour macOS</a> pour le lien de téléchargement.	27 octobre 2025
<a href="#">AWS client fourni (5.3.1) pour Windows x64 et Arm64 publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	30 septembre 2025
<a href="#">AWS le client fourni pour macOS supporte désormais Tahoe (26.0)</a>	Voir les exigences pour plus de détails.	25 septembre 2025
<a href="#">AWS sortie du client fourni (5.3.1) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2025
<a href="#">AWS sortie du client fourni (5.3.1) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	9 septembre 2025

<a href="#">AWS client fourni (5.3.0) pour les systèmes Windows Arm64 publié</a>	Support est désormais ajouté pour les systèmes Arm64-bas ed d'exploitation Windows. Cela inclut le téléchargement de AWS Client VPN la nouvelle version 5.3.0 spécifiquement pour les systèmes Windows Arm64. Consultez les <a href="#">exigences du Client VPN pour Windows</a> pour plus de détails et les <a href="#">notes de version AWS Client VPN pour Windows</a> pour le lien de téléchargement.	26 août 2025
<a href="#">AWS sortie du client fourni (5.3.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 août 2025
<a href="#">AWS sortie du client fourni (5.3.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 août 2025
<a href="#">AWS sortie du client fourni (5.3.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 août 2025
<a href="#">AWS sortie du client fourni (5.2.1) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	18 juin 2025
<a href="#">AWS sortie du client fourni (5.2.2) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	2 juin 2025
<a href="#">AWS sortie du client fourni (5.2.1) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 avril 2025

<a href="#">AWS sortie du client fourni (5.2.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
<a href="#">AWS sortie du client fourni (5.2.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
<a href="#">AWS sortie du client fourni (5.2.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
<a href="#">AWS sortie du client fourni (5.1.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025
<a href="#">AWS sortie du client fourni (5.1.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025
<a href="#">AWS sortie du client fourni (5.1.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025
<a href="#">Suppression du support pour macOS Monterey et ajout du support pour macOS Sonoma (14.0)</a>	Consultez la section <a href="#">Configuration requise pour le Client VPN pour macOS</a> pour plus de détails.	12 mars 2025
<a href="#">Suppression du support pour Ubuntu 18.0.4 (LTS) et Ubuntu 20.04 LTS (AMD64 uniquement)</a>	Consultez la section <a href="#">Configuration requise pour le Client VPN pour Linux</a> pour plus de détails.	12 mars 2025
<a href="#">AWS sortie du client fourni (5.0.3) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	6 mars 2025

<a href="#">AWS sortie du client fourni (5.0.2) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	24 février 2025
<a href="#">AWS sortie du client fourni (5.0.2) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 février 2025
<a href="#">AWS sortie du client fourni (5.0.1) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	30 janvier 2025
<a href="#">AWS sortie du client fourni (5.0.1) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	22 janvier 2025
<a href="#">Le client AWS fourni prend désormais en charge jusqu'à cinq connexions simultanées</a>	Consultez <a href="#">Support pour les connexions simultanées à l'aide d'un client AWS fourni</a> pour plus de détails.	21 janvier 2025
<a href="#">AWS sortie du client fourni (5.0.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 janvier 2025
<a href="#">AWS client fourni (5.0.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 janvier 2025
<a href="#">AWS sortie du client fourni (5.0.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
<a href="#">AWS sortie du client fourni (4.1.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024

<a href="#">AWS sortie du client fourni (4.1.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
<a href="#">AWS sortie du client fourni (4.1.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
<a href="#">AWS sortie du client fourni (4.0.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
<a href="#">AWS client fourni (4.0.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
<a href="#">AWS Le client fourni (4.0.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
<a href="#">AWS Le client fourni (3.15.1) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024
<a href="#">AWS sortie du client fourni (3.14.2) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024
<a href="#">AWS sortie du client fourni (3.12.1) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024
<a href="#">AWS sortie du client fourni (3.14.1) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	22 août 2024
<a href="#">AWS Le client fourni (3.15.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024

<a href="#">AWS sortie du client fourni (3.14.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024
<a href="#">AWS sortie du client fourni (3.12.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024
<a href="#">AWS Le client fourni (3.14.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
<a href="#">AWS client fourni (3.13.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
<a href="#">AWS sortie du client fourni (3.11.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
<a href="#">AWS sortie du client fourni (3.12.1) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	18 juillet 2024
<a href="#">AWS Le client fourni (3.13.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
<a href="#">AWS client fourni (3.12.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
<a href="#">AWS sortie du client fourni (3.10.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
<a href="#">AWS sortie du client fourni (3.9.2) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024

---

<a href="#">AWS Le client fourni (3.12.2) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024
<a href="#">AWS sortie du client fourni (3.11.2) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024
<a href="#">AWS sortie du client fourni (3.9.1) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
<a href="#">AWS Le client fourni (3.12.1) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
<a href="#">AWS sortie du client fourni (3.11.1) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
<a href="#">AWS Le client fourni (3.12.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	19 décembre 2023
<a href="#">AWS sortie du client fourni (3.9.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
<a href="#">AWS client fourni (3.11.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
<a href="#">AWS Le client fourni (3.11.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
<a href="#">AWS Le client fourni (3.10.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023

<a href="#">AWS sortie du client fourni (3.9.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
<a href="#">AWS sortie du client fourni (3.8.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
<a href="#">AWS client fourni (3.10.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
<a href="#">AWS sortie du client fourni (3.9.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023
<a href="#">AWS sortie du client fourni (3.8.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023
<a href="#">AWS sortie du client fourni (3.7.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023
<a href="#">AWS sortie du client fourni (3.8.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
<a href="#">AWS sortie du client fourni (3.7.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
<a href="#">AWS sortie du client fourni (3.7.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
<a href="#">AWS sortie du client fourni (3.6.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023

<a href="#">AWS sortie du client fourni (3.6.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
<a href="#">AWS sortie du client fourni (3.5.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
<a href="#">AWS sortie du client fourni (3.6.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
<a href="#">AWS sortie du client fourni (3.5.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
<a href="#">AWS sortie du client fourni (3.4.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
<a href="#">AWS sortie du client fourni (3.3.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	27 avril 2023
<a href="#">AWS sortie du client fourni (3.5.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 avril 2023
<a href="#">AWS sortie du client fourni (3.4.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	28 mars 2023
<a href="#">AWS sortie du client fourni (3.3.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2023
<a href="#">AWS sortie du client fourni (3.4.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	14 février 2023

<a href="#">AWS sortie du client fourni (3.2.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
<a href="#">AWS client fourni (3.2.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
<a href="#">AWS sortie du client fourni (3.1.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
<a href="#">AWS sortie du client fourni (3.1.0) pour Windows</a>	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
<a href="#">AWS sortie du client fourni (3.1.0) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
<a href="#">AWS sortie du client fourni (3.0.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
<a href="#">AWS client fourni (3.0.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
<a href="#">AWS Le client fourni (3.0.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
<a href="#">AWS sortie du client fourni (2.0.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
<a href="#">AWS client fourni (2.0.0) pour Windows publié</a>	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022

<a href="#">AWS Le client fourni (2.0.0) pour Ubuntu est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
<a href="#">AWS sortie du client fourni (1.4.0) pour macOS</a>	Pour plus d'informations, consultez les notes de mise à jour.	9 novembre 2021
<a href="#">AWS sortie du client fourni pour Windows (1.3.7)</a>	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021
<a href="#">AWS sortie du client fourni (1.0.3) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021
<a href="#">AWS sortie du client fourni (1.0.2) pour Ubuntu</a>	Pour plus d'informations, consultez les notes de mise à jour.	28 septembre 2021
<a href="#">AWS le client fourni pour Windows (1.3.6) et macOS (1.3.5) est sorti</a>	Pour plus d'informations, consultez les notes de mise à jour.	20 septembre 2021
<a href="#">AWS client fourni pour Ubuntu 18.04 LTS et Ubuntu 20.04 LTS publié</a>	Vous pouvez utiliser le client AWS fourni sur Ubuntu 18.04 LTS et Ubuntu 20.04 LTS.	11 juin 2021
<a href="#">Support d'OpenVPN avec un certificat du magasin de certificats système de Windows</a>	Vous pouvez utiliser OpenVPN avec un certificat du magasin de certificats système de Windows.	25 février 2021
<a href="#">Self-service portail</a>	Vous pouvez accéder à un portail en libre-service pour obtenir le client et le fichier de configuration les plus récents AWS fournis.	29 octobre 2020

[AWS client fourni](#)

Vous pouvez utiliser le client AWS fourni pour vous connecter à un point de terminaison VPN client.

4 février 2020

[Première version](#)

Cette version introduit AWS le 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.