Guide de l'utilisateur

AWS Client VPN

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Client VPN: Guide de l’utilisateur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez 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
Support pour les connexions simultanées ... 6
Directives OpenVPN ... 7
Windows ... 9
Prérequis ... 9
Connect à l'aide du client ... 9
Notes de mise à jour ... 10
macOS ... 21
Prérequis ... 21
Connect à l'aide du client ... 22
Notes de mise à jour ... 23
Linux ... 35
Conditions requises pour se connecter au Client VPN avec un client AWS fourni pour Linux ... 35
Installez le client ... 36
Connect à l'aide du client ... 37
Notes de mise à jour ... 38
Se connecter à l'aide d'un client OpenVPN ... 46
Windows ... 47
Établissez une connexion VPN à l'aide d'un certificat sous Windows ... 48
Connexions VPN du client sur Android et iOS ... 49
macOS ... 50
Établissez une connexion VPN sur macOS ... 51
Linux ... 51
Établissez une connexion VPN sous Linux ... 52

Résolution des problèmes ... 54
Résolution des problèmes liés aux points de terminaison Client VPN pour les administrateurs ... 54
Envoyer les journaux de diagnostic AWS Support au client AWS fourni ... 54
Envoyer des journaux de diagnostic ... 55
Résolution des problèmes liés à Windows ... 56
AWS journaux d'événements client fournis ... 56
Le client ne parvient pas à se connecter ... 57
Le client ne peut pas se connecter et reçoit le message de journal « aucun adaptateur TAP-Windows » ... 58
Le client est bloqué à l'état de reconnexion ... 58
Le processus de connexion VPN se ferme de façon inattendue ... 59
Échec du lancement de l'application ... 59
Le client ne parvient pas à créer de profil ... 60
Le VPN se déconnecte avec un message contextuel ... 60
Un crash du client se produit sur PCs Dell sous Windows 10 ou 11 ... 61
OpenVPN GUI ... 62
Client de connexion OpenVPN ... 63
Impossible de résoudre le DNS ... 63
Alias PKI manquant ... 64
Résolution des problèmes liés à macOS ... 64
AWS journaux d'événements client fournis ... 64
Le client ne parvient pas à se connecter ... 65
Le client est bloqué à l'état de reconnexion ... 66
Le client ne parvient pas à créer de profil ... 67
L'outil d'assistance est requis (erreur) ... 67
Tunnelblick ... 68
Algorithme de chiffrement AES-256-GCM introuvable ... 68
La connexion cesse de répondre et se réinitialise ... 69
EKU, Extended key usage (Utilisation étendue des clés) ... 69
Certificat expiré ... 70
OpenVPN ... 70
Impossible de résoudre le DNS ... 71
Résolution des problèmes liés à Linux ... 71
AWS journaux d'événements client fournis ... 56
Les requêtes DNS sont dirigées vers un serveur de noms par défaut ... 72
OpenVPN (ligne de commande) ... 73

OpenVPN via Network Manager (interface utilisateur graphique) 75
Problèmes courants 75
Échec de la négociation de clé TLS 76
Historique du document 77
..... lxxxvii

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, consultezSupport 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 surthe 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
- Connectez-vous à un AWS Client VPN terminal à l'aide d'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 exempl, `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 de 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

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 situé sur un point de terminaison différent de celui 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
- 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 Windows. 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.

Prérequis

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

- Windows 10 ou Windows 11 (système d'exploitation 64 bits, processeur x64)
- .NET Framework 4.7.2 ou version ultérieure

Pour les points de terminaison VPN du Client qui utilisent l'authentification fédérée basée sur le protocole SAML (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 l'aide d'un client AWS fourni pour Windows
- AWS Client VPN pour les notes de mise à jour de Windows

Se connecter à AWS Client VPN l'aide d'un client AWS fourni pour Windows

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

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

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 AWS VPN Client, 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).

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 Windows.

> **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
5.2.2	Posture de sécurité améliorée.	2 juin 2025	Télécharger la version 5.2.2 sha256 : f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	• Ajout du support pour le `ping-exit` drapeau OpenVPN. • Mise à jour de la bibliothèque OpenSSL. • Correctifs de bogues mineurs et améliorations	21 avril 2025	N'est plus pris en charge.
5.2.0	• Améliorations mineures. • Ajout de la prise en charge de l'application de l'itinéraire client.	8 avril 2025	N'est plus pris en charge.
5.1.0	• 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. • Correctifs de bogues mineurs et améliorations	17 mars 2025	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement et SHA256
5.0.2	• Correction d'un problème de DNS pour les connexions simultanées. • Correction de problèmes sporadiques lors de l'installation de nouveaux adaptateurs TAP.	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	• Ajout de la prise en charge des connexions simultanées. • Mise à jour de la version du pilote TAP. • Mise à jour de l'interface utilisateur graphique. • Correctifs de bogues mineurs et améliorations	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	Télécharger la version 4.0.0 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	Télécharger la version 3.14.2 sha256 : c171639d7e07e5fd48998cf76f74e6e49e5cbe3356c6264a67b4a9bf473b5f5d
3.14.1	Correctifs de bogues mineurs et améliorations	22 août 2024	Télécharger la version 3.14.1 sha256 : f743a7b4bc82daa4b803c2994390529997bb57a4bb54d1f5195ab28827283335
3,14,0	• Ajout du support pour le `tap-sleep` drapeau OpenVPN. • Mise à jour des bibliothèques OpenVPN et OpenSSL.	12 août 2024	Télécharger la version 3.14.0 sha256 : 812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516

Version	Modifications	Date	Lien de téléchargement et SHA256
3,13,0	Mise à jour des bibliothèques OpenVPN et OpenSSL.	29 juillet 2024	Télécharger la version 3.13.0 sha256 : c9cc896e81a7441184 0951e349ed9384507 c53337fb703c5ec64d 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	Télécharger la version 3.12.1 sha256 : 5ed34aee6c03aa281e 625acdbed272896c67 046364a9e5846ca697 e05dbfec08
3.12.0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change. • Suppression du focus automatique sur les applications lors de la connexion à des points de terminaison SAML.	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	Télécharger la version 3.11.2 sha256 : 8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc
3.11.1	• 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. • Posture de sécurité améliorée.	16 février 2024	Télécharger la version 3.11.1 sha256 : fb67b60aa837019795 8a11ea6f57d5bc0512279560b52a857ae34cb321eaefd0
3.11.0	• Correction d'un problème de connectivité causé par Windows VMs. • Problèmes de connectivité résolus pour certaines configurations de réseau local. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.11.0 sha256 : 9b6b7def99d76c59a97b067b6a73bdc6ee1c6b89a2063286f542e96b32df5ae9

Version	Modifications	Date	Lien de téléchargement et SHA256
3.10.0	• Correction d'un problème de connectivité lorsqu'il NAT64 est activé sur le réseau client. • Correction d'un problème de connectivité lorsque les adaptateurs réseau Hyper-V sont installés sur l'ordinateur client. • Correctifs de bogues mineurs et améliorations	24 août 2023	Télécharger la version 3.10.0 sha256 : d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.9.0 sha256 : de9a3800ea23491555 40bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
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	• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ». • Détection automatique de la disponibilité des versions mises à jour du client. • Ajout de la possibilité d'installer automatiquement les nouvelles versions du client lorsqu'elles sont disponibles.	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	• Ajout de la prise en charge de Windows 11. • Correction de la dénomination du pilote Windows TAP qui affectait d'autres noms de pilotes. • Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée. • Correction de l'affichage du texte de la bannière pour des textes plus longs. • Posture de sécurité améliorée.	3 mars 2022	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
2.0.0	• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie. • Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho • Correctifs de bogues mineurs et améliorations	20 janvier 2022	N'est plus pris en charge
1.3.7	• Correction d'une tentative de connexion d'authentification fédérée dans certains cas. • Correctifs de bogues mineurs et améliorations	08 novembre 2021	N'est plus pris en charge
1.3.6	• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Correctifs de bogues mineurs et améliorations	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	• Ajout de la prise en charge de l'indicateur OpenVPN : dhcp-option. • Correctifs de bogue mineurs et améliorations.	4 août 2021	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.3.3	• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route. • Résolution d'un problème qui bloquait l'application lors de la déconnexion ou de la sortie. • Correction d'un problème avec les noms d'utilisateur Active Directory avec barre oblique inverse. • Correction d'un blocage d'application lors de la manipulation de la liste de profil en dehors de l'application • Correctifs de bogue mineurs et améliorations.	1er juillet 2021	N'est plus pris en charge
1.3.2	• Ajoutez la prévention des IPv6 fuites, lorsqu'elle est configurée. • Correction d'un incident potentiel lorsque vous utilisez l'option Afficher les détails sous Connexion.	12 mai 2021	N'est plus pris en charge
1.3.1	• Ajout de la prise en charge de plusieurs certificats clients avec le même sujet. Les certificats expirés seront ignorés. • Correction de la conservation des journaux locaux pour réduire l'utilisation du disque. • Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'. • Correctifs de bogue mineurs et améliorations.	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	• Ajout de la prise en charge de la directive OpenVPN cryptoapicert. • Correction des routes périmées entre connexions. • Correctifs de bogue mineurs et améliorations.	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	• Ajout de la prise en charge des commentaires dans la configuration OpenVPN. • Ajout d'un message d'erreur pour les erreurs de liaison TLS.	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	• Ajout de la prise en charge de l'authentification fédérée basée sur SAML 2.0. • Prise en charge obsolète de la plate-forme Windows 7.	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	• 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. • Correctifs de bogue mineurs et améliorations.	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.

Prérequis

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

- macOS Ventura (13.0), Sonoma (14.0) ou Sequoia (15.0).
- Compatibilité avec un processeur x86_64.
- Pour les points de terminaison VPN du Client qui utilisent l'authentification fédérée basée sur le protocole SAML (authentification unique), le client réserve les ports TCP 8096-8115 sur votre ordinateur.

> **Note**
>
> Si vous utilisez un Mac équipé d'un processeur Apple Silicon, vous devez installer Rosetta 2 pour exécuter le logiciel client. Pour plus de détails, consultez À propos de l'environnement de traduction Rosetta sur le site Web d'Apple.

Rubriques

- Connectez-vous à l' AWS Client VPN aide d'un client AWS fourni pour macOS
- AWS Client VPN notes de mise à jour pour macOS

Connectez-vous à l' AWS Client VPN aide d'un client AWS 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 le AWS VPN client dans les étapes suivantes.

Pour vous connecter à l'aide du client AWS 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 AWS VPN Client, 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.

AWS Client VPN notes de mise à jour pour macOS

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 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
5.2.1	• Ajout du support pour le drapeau OpenVPN ping-exit. • Mise à jour de la bibliothèque OpenSSL.	18 juin 2025	Télécharger la version 5.2.1

Version	Modifications	Date	Lien de téléchargement
	• Posture de sécurité améliorée. • Correctifs de bogues mineurs et améliorations		sha256 : 906f77fbca3334fbdcd1145dd6f2725beab82a30b9b51eafd1a25c3fe7d669eb
5.2.0	• Améliorations mineures. • Ajout de la prise en charge de l'application de l'itinéraire client.	8 avril 2025	Télécharger la version 5.2.0 sha256 : f062e971a84e98d8a61caced3d7f6be322c28dab02ec81194c0f9a3e62bd8249
5.1.0	• 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. • Correction d'un problème qui AWS Client VPN empêchait d'établir une connexion VPN pour les fichiers de configuration avec des fins de ligne de type Windows. • Correctifs de bogues mineurs et améliorations	17 mars 2025	Télécharger la version 5.1.0 sha256 : ef7ff34ae85a29f90212514568c93849ef6e67f30b2c83ae1494d307f7650e10

Version	Modifications	Date	Lien de téléchargement
5.0.3	Correctifs de bogues mineurs et améliorations	6 mars 2025	Télécharger la version 5.0.3 sha256 : 8ce0f91ce81c322cead3ed27948ddeda4d5a61f5ed5a6115ab8e18f5d8963f6b
5.0.2	Correction d'un problème qui provoquait des erreurs sporadiques lors du choix de Connect.	17 février 2025	Télécharger la version 5.0.2 sha256 : e8128774608147e65b14f992a4b5a6d753646424fe3b68fab231810addac1f7c
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	Télécharger la version 5.0.1 sha256 : 7d9de8c89154c9a99bfd56b196600a9a09eb6a952cb10a7b16d01bdbadb0e57a

Version	Modifications	Date	Lien de téléchargement
5.0.0	• Ajout de la prise en charge des connexions simultanées. • Mise à jour de l'interface utilisateur graphique. • Correctifs de bogues mineurs et améliorations	21 janvier 2025	Télécharger la version 5.0.0 sha256 : e9c95ecdd6d582e72e1af0b05d03fe678f96b8b1028b5f569f962902943ecf02
4.1.0	Correctifs de bogues mineurs et améliorations	12 novembre 2024	Télécharger la version 4.1.0 sha256 : afe1ec8a6d7e2e1d618a6507f44a8c41db744fb55f94573e318d75bc5e96cd269
4.0.0	Améliorations mineures.	25 septembre 2024	Télécharger la version 4.0.0 sha256 : ad574475a80b614499c97ae75612ef1ff905bb4aa1b5f7109420e80bf95aefcbd

Version	Modifications	Date	Lien de téléchargement
3.12.1	Ajout du support pour le `mssfix` drapeau OpenVPN.	4 septembre 2024	Télécharger la version 3.12.1 sha256 : a5c31d3e0 e8bf89376 82805c9ff f76ca9205 875e009e9 49ad1b053 2f449cee47
3.12.0	• Ajout du support pour le `tap-sleep` drapeau OpenVPN. • Mise à jour des bibliothèques OpenVPN et OpenSSL.	12 août 2024	Télécharger la version 3.12.0 sha256 : 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• Mise à jour des bibliothèques OpenVPN et OpenSSL.	29 juillet 2024	Télécharger la version 3.11.0 sha256 : 44b5e6f84 788bf45dd b77871d74 3e09007e1 597555850 6221b8cae a81732848f

Version	Modifications	Date	Lien de téléchargement
3.10.0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change. • Correction d'un problème de restauration du DNS lors du changement de réseau. • Suppression du focus automatique sur les applications lors de la connexion à des points de terminaison SAML.	21 mai 2024	Télécharger la version 3.10.0 sha256 : 28bf26fa134b01ff12703cf59ffa4adba7c44ceb793dce4addd4404e84287dd
3.9.2	• Résolution d'un problème d'authentification SAML avec les navigateurs basés sur Chromium depuis la version 123. • Ajout du support pour macOS Sonoma. Déconseillez la prise en charge de macOS Big Sur. • Posture de sécurité améliorée.	11 avril 2024	Télécharger la version 3.9.2 sha256 : 374467d991e8953b5032e5b985cda80a0ea27fb5d5f23cf16c556a1568b0d480
3.9.1	• 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. • Barre de progression du téléchargement des mises à jour de l'application fixe. • Posture de sécurité améliorée.	16 février 2024	Télécharger la version 3.9.1 sha256 : 9bba4b27a635e75038703e2cf4cd814aa75306179fac8e500e2c7af4e899e971

Version	Modifications	Date	Lien de téléchargement
3.9.0	• Problèmes de connectivité résolus pour certaines configurations de réseau local. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.9.0 sha256 : f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• Correction d'un problème de connectivité lorsqu'il NAT64 est activé sur le réseau client. • Correctifs de bogues mineurs et améliorations	24 août 2023	Télécharger la version 3.8.0 sha256 : d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.7.0 sha256 : 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a

Version	Modifications	Date	Lien de téléchargement
3.6.0	• Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.5.0	• Annulation des modifications apportées à la version 3.4.0.	15 juillet 2023	N'est plus pris en charge
3.4.0	• Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.3.0	• Ajout de la prise en charge de macOS Ventura (13.0). • Correctifs de bogues mineurs et améliorations	27 avril 2023	N'est plus pris en charge
3.2.0	• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ». • Détection automatique de la disponibilité des versions mises à jour du client. • Ajout de la possibilité d'installer automatiquement les nouvelles versions du client lorsqu'elles sont disponibles.	23 janvier 2023	N'est plus pris en charge
3.1.0	• Ajout de la prise en charge pour macOS Monterey. • Correction d'un problème de détection du type de lecteur. • Posture de sécurité améliorée.	23 mai 2022	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement
3.0.0	• Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée. • Correction de l'affichage du texte de la bannière pour des textes plus longs. • Posture de sécurité améliorée.	3 mars 2022	N'est plus pris en charge.
2.0.0	• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie. • Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho • Correctifs de bogues mineurs et améliorations	20 janvier 2022	N'est plus pris en charge.
1.4.0	• Ajout de la surveillance du serveur DNS pendant la connexion. Les paramètres seront reconfigurés s'ils ne correspondent pas aux paramètres VPN. • Correction d'une tentative de connexion d'authentification fédérée dans certains cas. • Correctifs de bogues mineurs et améliorations	9 novembre 2021	N'est plus pris en charge.
1.3.5	• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Correctifs de bogues mineurs et améliorations	20 septembre 2021	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.3.4	• Ajout de la prise en charge de l'indicateur OpenVPN : dhcp-option. • Correctifs de bogue mineurs et améliorations.	4 août 2021	N'est plus pris en charge.
1.3.3	• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route. • Correction d'un problème avec les noms de fichiers de configuration comportant des espaces ou des caractères Unicode. • Résolution d'un problème qui bloquait l'application lors de la déconnexion ou de la sortie. • Correction d'un problème avec les noms d'utilisateur Active Directory avec barre oblique inverse. • Correction d'un blocage d'application lors de la manipulation de la liste de profil en dehors de l'application • Correctifs de bogue mineurs et améliorations.	1er juillet 2021	N'est plus pris en charge.
1.3.2	• Ajoutez la prévention des IPv6 fuites, lorsqu'elle est configurée. • Correction d'un incident potentiel lorsque vous utilisez l'option Afficher les détails sous Connexion. • Ajouter la rotation du journal du démon.	12 mai 2021	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.3.1	• Ajout de la prise en charge de macOS Big Sur (10.16). • Correction d'un problème qui supprimait les paramètres DNS configurés par d'autres applications. • Correction d'un problème lors de l'utilisation d'un certificat non valide pour l'authentification mutuelle, provoquant des problèmes de connectivité. • Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'. • Correctifs de bogue mineurs et améliorations.	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 2020	N'est plus pris en charge.
1.2.3	• Ajout de la prise en charge des commentaires dans la configuration OpenVPN. • Ajout d'un message d'erreur pour les erreurs de liaison TLS. • Correction d'un bug de désinstallation affectant certains utilisateurs.	8 octobre 2020	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.2.2	Correctifs de bogue mineurs et améliorations.	12 août 2020	N'est plus pris en charge.
1.2.1	• Ajout de la prise en charge de la désinstallation de l'application. • Correctifs de bogue mineurs et améliorations.	1er juillet 2020	N'est plus pris en charge.
1.2.0	• Ajout de la prise en charge de l'authentification fédérée basée sur SAML 2.0. • Ajout de la prise en charge de macOS Catalina (10.15).	19 mai 2020	N'est plus pris en charge.
1.1.2	Correctifs de bogue mineurs et améliorations.	21 avril 2020	N'est plus pris en charge.
1.1.1	• Correction d'un problème de non-résolution DNS. • Correction d'un problème de panne d'application causé par des connexions plus longues. • Correction d'un problème d'authentification MFA.	2 avril 2020	N'est plus pris en charge.
1.1.0	• Ajout de la prise en charge de la configuration DNS macOS. • 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. • Correctifs de bogue mineurs et améliorations.	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 client AWS fourni pour Linux

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

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

Pour les points de terminaison VPN du Client qui utilisent l'authentification fédérée basée sur le protocole SAML (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 système fourni 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 -qO- https://d20adtppz83p9s.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://d20adtppz83p9s.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://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
 awsvpnclient_amd64.deb
```

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

```
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 deTéléchargement 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 système fourni AWS Client VPN pour Linux

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

Pour vous connecter à l'aide du client AWS 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 AWS VPN Client, 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 d'utilisabilité et/ou de sécurité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement
5.2.0	• Améliorations mineures. • Ajout de la prise en charge de l'application de l'itinéraire client.	8 avril 2025	Télécharger la version 5.2.0 sha256 : ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• Correction d'un problème en raison duquel AWS Client VPN la version	17 mars 2025	Télécharger la version 5.1.0

Version	Modifications	Date	Lien de téléchargement
	5.0.x se reconnectait automatiquement au VPN après un délai d'inactivité. • Correctifs de bogues mineurs et améliorations		sha256 : 14f26c05b 11b0cc484 b08a8f8d2 0739de3d8 15c268db3 bba9ac70c 0e766b70ba
5.0.0	• Ajout de la prise en charge de plusieurs connexions simultanées. • Mise à jour de l'interface utilisateur graphique. • Correctifs de bogues mineurs et améliorations	21 janvier 2025	Télécharger la version 5.0.0 sha256 : 645126b56 98cb550e9 dc822e58e d899a5730 d2e204f28 f4023ec67 1915fdda0c
4.1.0	• Ajout du support pour Ubuntu 22.04 et 24.04. • Correctifs de bogue.	12 novembre 2024	Télécharger la version 4.1.0 sha256 : 334d00222 458fbfe9d ade16c99f e97e9ebcb d51fff017 d0d6b1d1b 764e7af472

Version	Modifications	Date	Lien de téléchargement
4.0.0	Améliorations mineures.	25 septembre 2024	Télécharger la version 4.0.0 sha256 : c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Ajout du support pour le `mssfix` drapeau OpenVPN.	4 septembre 2024	Télécharger la version 3.15.1 sha256 : ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2
3,15,0	• Ajout du support pour le `tap-sleep` drapeau OpenVPN. • Mise à jour des bibliothèques OpenVPN et OpenSSL.	12 août 2024	Télécharger la version 3.15.0 sha256 : 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012

Version	Modifications	Date	Lien de téléchargement
3,14,0	• Mise à jour des bibliothèques OpenVPN et OpenSSL.	29 juillet 2024	Télécharger la version 3.14.0 sha256 : bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60
3,13,0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change.	21 mai 2024	Télécharger la version 3.13.0 sha256 : e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1
3.12.2	• Résolution d'un problème d'authentification SAML avec les navigateurs basés sur Chromium depuis la version 123.	11 avril 2024	Télécharger la version 3.12.2 sha256 : f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d

Version	Modifications	Date	Lien de téléchargement
3.12.1	• 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. • Posture de sécurité améliorée.	16 février 2024	Télécharger la version 3.12.1 sha256 : 547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• Problèmes de connectivité résolus pour certaines configurations de réseau local.	19 décembre 2023	Télécharger la version 3.12.0 sha256 : 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Restauration pour « Problèmes de connectivité résolus pour certaines configurations de réseau local ». • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.11.0 sha256 : 86c0fa1bf1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970

Version	Modifications	Date	Lien de téléchargement
3.10.0	• Problèmes de connectivité résolus pour certaines configurations de réseau local. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.10.0 sha256 : e7450b2490f3b96ab7d589a8000d838d9fd2adcdd72ae80666c4c0d900687e51
3.9.0	• Correction d'un problème de connectivité lorsqu'il NAT64 est activé sur le réseau client. • Correctifs de bogues mineurs et améliorations	24 août 2023	Télécharger la version 3.9.0 sha256 : 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454
3.8.0	• Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.8.0 sha256 : 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd

Version	Modifications	Date	Lien de téléchargement
3.7.0	• Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.6.0	• Annulation des modifications apportées à la version 3.5.0.	15 juillet 2023	N'est plus pris en charge
3.5.0	• Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.4.0	• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ».	14 février 2023	N'est plus pris en charge
3.1.0	• Correction d'un problème de détection du type de lecteur. • Posture de sécurité améliorée.	23 mai 2022	N'est plus pris en charge
3.0.0	• Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée. • Correction de l'affichage du texte de la bannière pour des séquences de caractères plus longues et spécifiques. • Posture de sécurité améliorée.	3 mars 2022	N'est plus pris en charge.
2.0.0	• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie. • Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho • Correctifs de bogues mineurs et améliorations	20 janvier 2022	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.0.3	• Correction d'une tentative de connexion d'authentification fédérée dans certains cas. • Correctifs de bogues mineurs et améliorations	08 novembre 2021	N'est plus pris en charge.
1.0.2	• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Correctifs de bogues mineurs et améliorations	28 septembre 2021	N'est plus pris en charge.
1.0.1	• Option activée pour quitter la barre d'application Ubuntu. • Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route. • Correctifs de bogue mineurs et améliorations.	4 août 2021	N'est plus pris en charge.
1.0.0	Version initiale.	11 juin 2021	N'est plus pris en charge.

Connectez-vous à un AWS Client VPN terminal à l'aide d'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, consultezÉtablissez une connexion VPN à l'aide d'un certificat sous Windows.
- 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.
- macOS

  Établissez une connexion VPN à l'aide d'un fichier de configuration pour Tunnelblick basé sur macOS 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.

> **Important**
>
> Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification fédérée basée sur SAML, vous ne pouvez pas utiliser le client VPN basé sur OpenVPN pour vous connecter à un point de terminaison Client VPN. Cela inclut toutes les architectures basées

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

Applications clientes

- Se connecter à un AWS Client VPN point de terminaison à l'aide d'une application cliente Windows
- AWS Client VPN connexions sur les applications Android et iOS
- Connectez-vous à un AWS Client VPN terminal à l'aide d'une application cliente macOS
- Connectez-vous à un AWS Client VPN terminal à l'aide d'une application cliente OpenVPN

Se connecter à un AWS Client VPN point de terminaison à l'aide d'une application cliente Windows

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

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 liés aux connexions VPN des AWS clients avec des clients Windows.

> **Important**
>
> Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification fédérée basée sur SAML, vous ne pouvez pas utiliser le client VPN basé sur OpenVPN pour vous connecter à un point de terminaison Client VPN. Cela inclut toutes les architectures basées sur ARM. Si vous utilisez un appareil équipé d'un processeur ARM (tel que des Mac Apple Silicon ou des appareils Windows basés sur ARM), vous devez utiliser des points de terminaison VPN basés sur SAML avec le AWS client fourni plutôt que des clients OpenVPN.

Tâches

- Utiliser un certificat et établir une connexion AWS Client VPN sous Windows

Utiliser un certificat et établir une connexion AWS Client VPN 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 Afficher/Masquer les icônes. Cliquez avec le bouton droit sur 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 Afficher/Masquer les icônes. Cliquez avec le bouton droit sur 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).

AWS Client VPN connexions sur les applications Android et iOS

> **Important**
>
> Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification fédérée basée sur SAML, vous ne pouvez pas utiliser le client VPN basé sur OpenVPN pour vous connecter à un point de terminaison Client VPN. Cela inclut toutes les architectures basées sur ARM. Si vous utilisez un appareil équipé d'un processeur ARM (tel que des Mac Apple Silicon ou des appareils Windows basés sur ARM), vous devez utiliser des points de terminaison VPN basés sur SAML avec le AWS client 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.

Connectez-vous à un AWS Client VPN terminal à l'aide d'une application cliente macOS

Ces sections décrivent comment établir une connexion VPN à l'aide du client VPN basé sur macOS, 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 de connexion VPN entre AWS clients et clients macOS.

> **Important**
>
> Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification fédérée basée sur SAML, vous ne pouvez pas utiliser le client VPN basé sur OpenVPN pour vous connecter à un point de terminaison Client VPN. Cela inclut toutes les architectures basées sur ARM. Si vous utilisez un appareil équipé d'un processeur ARM (tel que des Mac Apple Silicon ou des appareils Windows basés sur ARM), vous devez utiliser des points de terminaison VPN basés sur SAML avec le AWS client fourni plutôt que des clients OpenVPN.

Rubriques

- Établir une AWS Client VPN connexion sur macOS

Établir une 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 AWS du VPN du Client.

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).

Connectez-vous à un AWS Client VPN terminal à l'aide d'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 liés aux connexions VPN des AWS clients avec des clients basés sur Linux.

> **Important**
>
> Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification fédérée basée sur SAML, vous ne pouvez pas utiliser le client VPN basé sur OpenVPN pour vous connecter à un point de terminaison Client VPN. Cela inclut toutes les architectures basées sur ARM. Si vous utilisez un appareil équipé d'un processeur ARM (tel que des Mac Apple Silicon ou des appareils Windows basés sur ARM), vous devez utiliser des points de terminaison VPN basés sur SAML avec le AWS client fourni plutôt que des clients OpenVPN.

Rubriques

- Établir une AWS Client VPN connexion sous Linux

Établir une 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
```

Résolution des problèmes liés aux connexions VPN du AWS 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 AWS Support au client AWS fourni
- Résolution des problèmes liés aux connexions VPN des AWS clients avec des clients Windows
- Résolution des problèmes de connexion VPN entre AWS clients et clients macOS
- Résolution des problèmes liés aux connexions VPN des AWS clients avec des clients basés sur Linux
- Résolution des problèmes courants liés AWS au Client VPN

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 AWS Support au client AWS 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 le AWS VPN client dans les étapes suivantes.

Pour envoyer des journaux de diagnostic à l'aide du client AWS 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 client AWS 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 client AWS 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 liés aux connexions VPN des AWS clients avec des clients Windows

Les sections suivantes traitent des problèmes que vous pouvez rencontrer lors de l'utilisation de clients Windows pour vous connecter à un point de terminaison Client VPN.

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 et reçoit le message de journal « aucun adaptateur TAP-Windows »
- 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 crash du client se produit sur PCs Dell sous 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 et reçoit le message de journal « aucun adaptateur TAP-Windows »

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'existe aucun adaptateur TAP-Windows sur ce système. Pour créer un adaptateur TAP-Windows, accédez à Démarrer -> Tous les programmes -> TAP-Windows -> Utilitaires -> Ajouter un nouvel adaptateur Ethernet virtuel TAP-Windows ».

Solution

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

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

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

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

Solution

Si le `Description` champ ci-dessous ne correspond pas, supprimez d'abord l'adaptateur TAP-Windows, 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 crash du client se produit sur PCs Dell sous Windows 10 ou 11

Problème

Sur certains ordinateurs Dell PCs (ordinateurs de bureau et portables) exécutant Windows 10 ou 11, un crash 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 suivants DLLs :

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.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
   - DBROverlayIconBackuped.dll
   - DBROverlayIconNotBackuped.dll

   Vous pouvez renommer les fichiers en ajoutant « .bak » à la fin du nom du fichier, DBROverlay IconBackuped par exemple .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 de connexion VPN entre AWS clients et 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

Le message d'erreur suivant 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. Erreur relative au client VPN AWS : l'outil d'assistance est requis

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 OpenVPN qui ne prend pas en charge l'algorithme de chiffrement AES-256-GCM.

Solution

Choisissez une version OpenVPN compatible en procédant comme suit :

1. Ouvrez l'application Tunnelblick.

2. Sélectionnez 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 liés aux connexions VPN des AWS clients avec des clients basés sur Linux

Les sections suivantes traitent de la journalisation et des problèmes que vous pouvez rencontrer lors de l'utilisation de clients Linux. 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 client daemon 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
   ```

   Vous souhaiterez peut-être suivre cette procédure afin de contourner la configuration résolue par le système, par exemple pour la mise en cache des réponses DNS, la configuration DNS par interface, DNSSec l'application, 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, LZO 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 .

Résolution des problèmes courants liés AWS au Client VPN

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
AWS sortie du client fourni (5.2.1) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	18 juin 2025
AWS sortie du client fourni (5.2.2) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	2 juin 2025
AWS sortie du client fourni (5.2.1) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	21 avril 2025
AWS sortie du client fourni (5.2.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
AWS sortie du client fourni (5.2.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
AWS sortie du client fourni (5.2.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	8 avril 2025
AWS sortie du client fourni (5.1.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025
AWS sortie du client fourni (5.1.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025

AWS sortie du client fourni (5.1.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2025
Suppression du support pour macOS Monterey et ajout du support pour macOS Sonoma (14.0)	Consultez la section Configuration requise pour le Client VPN pour macOS pour plus de détails.	12 mars 2025
Suppression du support pour Ubuntu 18.0.4 (LTS) et Ubuntu 20.04 LTS (uniquement) AMD64	Consultez la section Configuration requise pour le Client VPN pour Linux pour plus de détails.	12 mars 2025
AWS sortie du client fourni (5.0.3) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	6 mars 2025
AWS sortie du client fourni (5.0.2) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	24 février 2025
AWS sortie du client fourni (5.0.2) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	17 février 2025
AWS sortie du client fourni (5.0.1) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	30 janvier 2025
AWS sortie du client fourni (5.0.1) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	22 janvier 2025
Le client AWS fourni prend désormais en charge jusqu'à cinq connexions simultanées	Consultez Support pour les connexions simultanées à l'aide d'un client AWS fourni pour plus de détails.	21 janvier 2025

AWS sortie du client fourni (5.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	21 janvier 2025
AWS client fourni (5.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	21 janvier 2025
AWS sortie du client fourni (5.0.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
AWS sortie du client fourni (4.1.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
AWS client fourni (4.1.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
AWS sortie du client fourni (4.1.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	12 novembre 2024
AWS sortie du client fourni (4.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
AWS client fourni (4.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
AWS Le client fourni (4.0.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	25 septembre 2024
AWS Le client fourni (3.15.1) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024

AWS sortie du client fourni (3.14.2) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024
AWS sortie du client fourni (3.12.1) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	4 septembre 2024
AWS client fourni (3.14.1) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	22 août 2024
AWS Le client fourni (3.15.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024
AWS sortie du client fourni (3.14.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024
AWS sortie du client fourni (3.12.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	12 août 2024
AWS Le client fourni (3.14.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
AWS sortie du client fourni (3.13.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
AWS sortie du client fourni (3.11.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	29 juillet 2024
AWS sortie du client fourni (3.12.1) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	18 juillet 2024

AWS Le client fourni (3.13.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
AWS sortie du client fourni (3.12.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
AWS sortie du client fourni (3.10.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	21 mai 2024
AWS sortie du client fourni (3.9.2) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024
AWS sortie du client fourni (3.12.2) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024
AWS sortie du client fourni (3.11.2) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	11 avril 2024
AWS sortie du client fourni (3.9.1) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
AWS Le client fourni (3.12.1) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
AWS sortie du client fourni (3.11.1) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	16 février 2024
AWS Le client fourni (3.12.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	19 décembre 2023

AWS sortie du client fourni (3.9.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
AWS client fourni (3.11.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
AWS Le client fourni (3.11.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
AWS sortie du client fourni (3.10.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
AWS sortie du client fourni (3.9.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
AWS sortie du client fourni (3.8.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
AWS client fourni (3.10.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	24 août 2023
AWS sortie du client fourni (3.9.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023
AWS sortie du client fourni (3.8.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023
AWS sortie du client fourni (3.7.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	3 août 2023

AWS sortie du client fourni (3.8.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.7.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.7.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.6.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.6.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.5.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.6.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
AWS sortie du client fourni (3.5.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
AWS sortie du client fourni (3.4.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
AWS sortie du client fourni (3.3.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	27 avril 2023

AWS sortie du client fourni (3.5.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	3 avril 2023
AWS sortie du client fourni (3.4.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	28 mars 2023
AWS sortie du client fourni (3.3.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2023
AWS sortie du client fourni (3.4.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	14 février 2023
AWS sortie du client fourni (3.2.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
AWS client fourni (3.2.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
AWS sortie du client fourni (3.1.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
AWS sortie du client fourni (3.1.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
AWS sortie du client fourni (3.1.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
AWS sortie du client fourni (3.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022

AWS client fourni (3.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
AWS Le client fourni (3.0.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
AWS sortie du client fourni (2.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS client fourni (2.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS Le client fourni (2.0.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS sortie du client fourni (1.4.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	9 novembre 2021
AWS sortie du client fourni pour Windows (1.3.7)	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021
AWS sortie du client fourni (1.0.3) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021
AWS sortie du client fourni (1.0.2) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	28 septembre 2021
AWS le client fourni pour Windows (1.3.6) et macOS (1.3.5) est sorti	Pour plus d'informations, consultez les notes de mise à jour.	20 septembre 2021

AWS client fourni pour Ubuntu 18.04 LTS et Ubuntu 20.04 LTS publié	Vous pouvez utiliser le client AWS fourni sur Ubuntu 18.04 LTS et Ubuntu 20.04 LTS.	11 juin 2021
Support d'OpenVPN avec un certificat du magasin de certificats système de Windows	Vous pouvez utiliser OpenVPN avec un certificat du magasin de certificats système de Windows.	25 février 2021
Portail en libre-service	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.