Guide de l’utilisateur

AWS Cliente VPN

AWS Cliente VPN: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS le client VPN ?

AWS VPNLe client est un VPN service géré basé sur le client qui vous permet d'accéder en toute sécurité aux AWS ressources et aux ressources de votre réseau sur site.

Ce guide décrit les étapes à suivre pour établir une VPN connexion à un point de VPN terminaison client à l'aide d'une application cliente installée sur votre appareil.

VPNComposants du client

Les éléments clés de l'utilisation du AWS client sont les suivantsVPN.

- Point de VPNterminaison client : votre VPN administrateur client crée et configure un point de VPN terminaison client dans AWS. Votre administrateur contrôle les réseaux et les ressources auxquels vous pouvez accéder lorsque vous établissez une VPN connexion.
- VPNapplication client : application logicielle que vous utilisez pour vous connecter au point de VPN terminaison client et établir une VPN connexion sécurisée.
- Fichier de configuration du point de VPN terminaison client : fichier de configuration qui vous est fourni par VPN l'administrateur de votre client. Le fichier contient des informations sur le point de VPN terminaison du client et les certificats requis pour établir une VPN connexion. Vous chargez ce fichier dans l'application VPN cliente de votre choix.

Ressources supplémentaires pour configurer le client VPN

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

Commencez avec AWS Client VPN

Avant de pouvoir établir une VPN session, votre VPN administrateur client doit créer et configurer un point de VPN terminaison client. Votre administrateur contrôle les réseaux et les ressources auxquels vous pouvez accéder lorsque vous établissez une VPN session. Vous utilisez ensuite une application VPN client pour vous connecter à un point de VPN terminaison client et établir une VPN connexion sécurisée.

Si vous êtes un administrateur qui doit créer un point de VPN terminaison client, consultez le guide de l'AWS Client VPN administrateur.

Rubriques

Conditions préalables à l'utilisation du client VPN

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

- Un accès à Internet
- Un appareil pris en charge
- Pour les VPN terminaux clients qui utilisent l'authentification fédérée SAML basée (authentification unique), l'un des navigateurs suivants :
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Étape 1 : obtenir une application VPN client

Vous pouvez vous connecter à un point de VPN terminaison client et établir une VPN connexion à l'aide du client AWS fourni ou d'une autre application client VPN basée sur Open.

Le client AWS fourni est compatible avec Windows, macOS, Ubuntu 18.04 LTS et Ubuntu LTS 20.04.

Vous pouvez télécharger l'VPNapplication client 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 le fichier de configuration du point de terminaison, téléchargez et installez le client à partir du VPNtéléchargement du AWS client. Après avoir téléchargé et installé l'application, accédez the section called "Étape 2 : obtenir le fichier de configuration du VPN point de terminaison client" au fichier de configuration du point de terminaison auprès de votre administrateur.
- Si votre administrateur a déjà préconfiguré le fichier de configuration du point de terminaison, vous pouvez télécharger l'VPNapplication client, 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, consultezthe section called "Télécharger le client VPN". Après avoir téléchargé et installé l'application et le fichier, rendez-vous surthe section called "Étape 3 : Connectez-vous au VPN".

Vous pouvez également télécharger et installer une application VPN client Open sur l'appareil à partir duquel vous souhaitez établir la VPN connexion.

Étape 2 : obtenir le fichier de configuration du VPN point de terminaison client

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

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

Étape 3 : Connectez-vous au VPN

Importez le fichier de configuration du point de VPN terminaison client vers le client AWS fourni ou vers votre application VPN client Open et connectez-vous auVPN. Pour connaître les étapes de connexion à unVPN, y compris l'importation du fichier de configuration du point de terminaison, consultez les rubriques suivantes :

- Connectez-vous à un point de VPN terminaison client à l'aide d'un client AWS fourni
- Se connecter à un point de VPN terminaison client à l'aide d'un VPN client Open

Pour les VPN terminaux clients qui utilisent l'authentification Active Directory, vous serez invité à saisir votre nom d'utilisateur et votre mot de passe. Si l'authentification multifactorielle (MFA) a été activée pour le répertoire, vous serez également invité à saisir votre MFA code.

Pour les VPN terminaux clients qui utilisent l'authentification fédérée SAML basée (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 VPN terminaison client.

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 la dernière version du fichier de configuration du point de VPN terminaison du client. Si l'administrateur de votre point de VPN terminaison client a préconfiguré le fichier de configuration pour le VPN client client, vous pouvez télécharger et installer cette VPN application client avec le fichier de configuration à partir de ce portail.

> **Note**
>
> Si vous êtes administrateur et que vous souhaitez configurer le portail en libre-service, consultez la section VPNPoints de terminaison clients dans le guide de l'AWS Client VPN administrateur.

Avant de commencer, vous devez disposer de l'ID du point de VPN terminaison client. L'administrateur de votre point de VPN terminaison client peut vous fournir l'identifiant ou vous fournir un portail en libre-service URL qui inclut cet identifiant.

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 le portail URL qui vous a été fourni par votre administrateur.
2. Si nécessaire, entrez l'ID du point de VPN terminaison client, par exemple,`cvpn-endpoint-0123456abcd123456`. Choisissez Suivant.
3. Entrez votre nom d'utilisateur et votre mot de passe, puis choisissez Sign In (Se connecter). Il s'agit du même nom d'utilisateur et du même mot de passe que ceux que vous utilisez pour vous connecter au point de VPN terminaison client.
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 VPN terminaison client.
   - Téléchargez la dernière version du client AWS fourni pour votre plateforme.

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

Vous pouvez vous connecter à un point de VPN terminaison client à l'aide du client AWS fourni. Le client AWS fourni est compatible avec Windows, macOS, Ubuntu 18.04 LTS et Ubuntu LTS 20.04.

Clients

- AWS Client VPN pour Windows
- AWS Client VPN pour macOS
- AWS Client VPN pour Linux

VPNDirectives ouvertes

Le client AWS fourni prend en charge les VPN directives Open suivantes :

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- inactive

- keepalive
- clé
- nobind
- persist-key
- persist-tun
- 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
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN pour Windows

Ces sections décrivent comment établir une VPN connexion à l'aide du client AWS fourni pour Windows. Vous pouvez télécharger et installer le client dans la section VPNTéléchargement AWS du client. 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)
- . NETFramework 4.7.2 ou supérieur

Le client réserve le TCP port 8096 sur votre ordinateur. Pour les VPN terminaux clients qui utilisent l'authentification fédérée SAML basée (authentification unique), le client réserve TCP le port 35001.

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Rubriques

- Connect to Client VPN avec un client AWS fourni pour Windows
- AWS Client VPN pour les notes de mise à jour de Windows

Connect to Client VPN avec 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. Dans Fichier de VPN configuration, accédez au fichier de configuration que vous avez reçu de l'VPNadministrateur du client, puis sélectionnez-le, puis choisissez Ajouter un profil.
6. Dans la fenêtre AWS VPN Client, assurez-vous que votre profil est sélectionné, puis sélectionnez Connect (Connexion). Si le point de VPN terminaison du client 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.
7. Pour afficher les statistiques de votre connexion, choisissez Connection (Connexion), Show Details (Afficher les détails).

8. Pour vous déconnecter, dans la fenêtre AWS VPN Client, sélectionnez Disconnect (Déconnexion). 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 d'utilisabilité et/ou de sécurité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement et SHA256
3,14,0	• Ajout du support pour le VPN drapeau `tap-sleep` ouvert. • Mise à jour des SSL bibliothèques Open VPN et Open.	12 août 2024	Télécharger la version 3.14.0 sha256 : 812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516
3,13,0	Mise à jour des SSL bibliothèques Open VPN et Open.	29 juillet 2024	Télécharger la version 3.13.0 sha256 : c9cc896e81a74411840951e349e

Version	Modifications	Date	Lien de téléchargement et SHA256
			ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12.1	Correction d'un problème qui empêchait le client Windows version 3.12.0 d'établir VPN une connexion pour certains utilisateurs.	18 juillet 2024	Télécharger la version 3.12.1 sha256 : 5ed34aee6 c03aa281e 625acdbed 272896c67 046364a9e 5846ca697 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 SAML points de terminaison.	21 mai 2024	N'est plus pris en charge
3.11.2	Résolution d'un problème SAML d'authentification avec les navigateurs basés sur Chromium depuis la version 123.	11 avril 2024	Télécharger la version 3.11.2 sha256 : 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc

Version	Modifications	Date	Lien de téléchargement et SHA256
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 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Correction d'un problème de connectivité causé par WindowsVMs. • Correction de problèmes de connectivité pour certaines LAN configurations. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.11.0 sha256 : 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9
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 : d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f

Version	Modifications	Date	Lien de téléchargement et SHA256
3.9.0	Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.9.0 sha256 : de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.7.0	Annulation des modifications apportées à la version 3.6.0.	15 juillet 2023	N'est plus pris en charge
3.6.0	Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.5.0	Correctifs de bogues mineurs et améliorations	3 avril 2023	N'est plus pris en charge
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

Version	Modifications	Date	Lien de téléchargement et SHA256
3.2.0	• Ajout du support pour le drapeau ouvert « verify-x509-name ». VPN • 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 des pilotes TAP Windows, ce qui affectait les 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
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 et SHA256
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 Open VPN flags : 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 du support pour Open VPN flag : dhcp-option. • Correctifs de bogues 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 Open VPN flags : inactive, 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 du support pour la directive ouverte VPN « route-ipv6 ». • Correctifs de bogues 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 du support pour la directive cryptoapicert Open. VPN • 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 du support pour les commentaires dans la VPN configuration Open. • Ajout d'un message d'erreur pour les erreurs de TLS poignée de main.	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'SAMLauthentification fédérée basée sur la version 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 Open VPN static challenge echo pour masquer ou afficher le texte affiché dans l'interface utilisateur. • Correctifs de bogues 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 VPN connexion à l'aide du client AWS fourni pour macOS. Vous pouvez télécharger et installer le client dans la section VPNTéléchargement AWS du client. 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 Monterey (12.0), Ventura (13.0) ou Sonoma (14.0).
- Compatibilité avec un processeur x86_64.
- Le client réserve le TCP port 8096 sur votre ordinateur.
- Pour les VPN terminaux clients qui utilisent l'authentification fédérée SAML basée (authentification unique), le client réserve TCP le port 35001.

> **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

Connect to Client VPN avec un client AWS fourni pour macOS

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

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 le fichier VPN de configuration, accédez au fichier de configuration que vous avez reçu de l'VPNadministrateur de votre client. Choisissez Open.
6. Choisissez Add Profile (Ajouter un profil).
7. Dans la fenêtre AWS VPN Client, assurez-vous que votre profil est sélectionné, puis sélectionnez Connect (Connexion). Si le point de VPN terminaison du client 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.
8. Pour afficher les statistiques de votre connexion, choisissez Connection (Connexion), Show Details (Afficher les détails).

9. Pour vous déconnecter, dans la fenêtre AWS VPN Client, sélectionnez Disconnect (Déconnexion). Vous pouvez également choisir l'icône du client dans la barre de menu, puis sélectionner Déconnecter < your-profile-name >.

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 d'utilisabilité et/ou de sécurité. Pour plus d'informations, consultez les notes de mise à jour.

Version	Modifications	Date	Lien de téléchargement
3.12.0	• Ajout du support pour le VPN drapeau `tap-sleep` ouvert. • Mise à jour des SSL bibliothèques Open VPN et Open.	12 août 2024	Télécharger la version 3.12.0 sha256 : 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• Mise à jour des SSL bibliothèques Open VPN et Open.	29 juillet 2024	Télécharger la version 3.11.0 sha256 : 44b5e6f84 788bf45dd

Version	Modifications	Date	Lien de téléchargement
			b77871d74 3e09007e1 597555850 6221b8cae a81732848f
3.10.0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change. • Correction d'un problème DNS de restauration lors du changement de réseau. • Suppression du focus automatique sur les applications lors de la connexion à des SAML points de terminaison.	21 mai 2024	Télécharger la version 3.10.0 sha256 : 28bf26fa1 34b01ff12703cf59ff fa4adba7c 44ceb793d ce4addd44 04e84287dd
3.9.2	• Résolution d'un problème SAML d'authentification 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 : 374467d99 1e8953b50 32e5b985c da80a0ea2 7fb5d5f23 cf16c556a 1568b0d480

Version	Modifications	Date	Lien de téléchargement
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
3.9.0	• Correction de problèmes de connectivité pour certaines LAN configurations. • 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

Version	Modifications	Date	Lien de téléchargement
3.7.0	• Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.7.0 sha256 : 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a
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 du support pour le drapeau ouvert « verify-x509-name ». VPN • 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

Version	Modifications	Date	Lien de téléchargement
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
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	• Surveillance DNS du serveur ajoutée pendant la connexion. Les paramètres seront reconfigurés s'ils ne correspondent pas aux VPN paramètres. • 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.

Version	Modifications	Date	Lien de téléchargement
1.3.5	• Ajout du support pour Open VPN flags : 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.
1.3.4	• Ajout du support pour Open VPN flag : dhcp-option. • Correctifs de bogues mineurs et améliorations	4 août 2021	N'est plus pris en charge.
1.3.3	• Ajout du support pour Open VPN flags : inactive, 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.

Version	Modifications	Date	Lien de téléchargement
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.
1.3.1	• Ajout de la prise en charge de macOS Big Sur (10.16). • Correction d'un problème qui supprimait DNS les paramètres 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 du support pour la directive ouverte VPN « route-ipv6 ». • Correctifs de bogues 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.

Version	Modifications	Date	Lien de téléchargement
1.2.3	• Ajout du support pour les commentaires dans la VPN configuration Open. • Ajout d'un message d'erreur pour les erreurs de TLS poignée de main. • Correction d'un bug de désinstallation affectant certains utilisateurs.	8 octobre 2020	N'est plus pris en charge.
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'SAMLauthentification fédérée basée sur la version 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 qui ne se DNS résolvait pas. • Correction d'un problème de panne d'application causé par des connexions plus longues. • Correction d'un MFA problème.	2 avril 2020	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.1.0	• Ajout du support pour la DNS configuration de macOS. • Ajout de la prise en charge de la fonctionnalité Open VPN static challenge echo pour masquer ou afficher le texte affiché dans l'interface utilisateur. • Correctifs de bogues 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 Linux

Ces sections décrivent l'installation du client AWS fourni pour Linux, puis l'établissement d'une VPN connexion 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 18.04 LTS ou Ubuntu 20.04 LTS (uniquement) AMD64

Le client réserve le TCP port 8096 sur votre ordinateur. Pour les VPN terminaux clients qui utilisent l'authentification fédérée SAML basée (authentification unique), le client réserve TCP le port 35001.

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Rubriques

- Installez le client AWS fourni pour Linux
- Connectez-vous au client AWS fourni pour Linux
- AWS Client VPN notes de mise à jour pour Linux

Installez le client AWS fourni 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 AWS VPN client 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 applicable pour ajouter le référentiel à votre système d'exploitation Ubuntu, en fonction de votre version d'Ubuntu :

   Ubuntu 18.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

   Ubuntu 20.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-20.04 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 depuis le VPNtéléchargement du AWS client 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'dpkgutilitaire.

```
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 depuis le VPNtéléchargement du AWS client.
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 client AWS fourni 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 le fichier VPN de configuration, accédez au fichier de configuration que vous avez reçu de l'VPNadministrateur de votre client. Choisissez Open.
6. Choisissez Add Profile (Ajouter un profil).
7. Dans la fenêtre AWS VPN Client, assurez-vous que votre profil est sélectionné, puis sélectionnez Connect (Connexion). Si le point de VPN terminaison du client 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.

8. Pour afficher les statistiques de votre connexion, choisissez Connection (Connexion), Show Details (Afficher les détails).
9. Pour vous déconnecter, dans la fenêtre AWS VPN Client, sélectionnez Disconnect (Déconnexion).

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
3,15,0	• Ajout du support pour le VPN drapeau `tap-sleep` ouvert. • Mise à jour des SSL bibliothèques Open VPN et Open.	12 août 2024	Télécharger la version 3.15.0 sha256 : 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012
3,14,0	• Mise à jour des SSL bibliothèques Open VPN et Open.	29 juillet 2024	Télécharger la version 3.14.0

Version	Modifications	Date	Lien de téléchargement
			sha256 : bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3,13,0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change.	21 mai 2024	Télécharger la version 3.13.0 sha256 : e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1
3.12.2	• Résolution d'un problème SAML d'authentification avec les navigateurs basés sur Chromium depuis la version 123.	11 avril 2024	Télécharger la version 3.12.2 sha256 : f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d

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	• Correction de problèmes de connectivité pour certaines LAN configurations.	19 décembre 2023	Télécharger la version 3.12.0 sha256 : 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Annulation pour « Problèmes de connectivité résolus pour certaines LAN configurations ». • 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	• Correction de problèmes de connectivité pour certaines LAN configurations. • 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 du support pour le drapeau ouvert « verify-x509-name ». VPN	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 Open VPN flags : 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 Open VPN flags : inactive, pull-filter, route. • Correctifs de bogues 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.

Se connecter à un point de VPN terminaison client à l'aide d'un VPN client Open

Vous pouvez vous connecter à un point de VPN terminaison client à l'aide d'applications VPN client Open courantes.

> **Important**
>
> Si le point de VPN terminaison client a été configuré pour utiliser l'authentification fédérée SAML basée, vous ne pouvez pas utiliser le VPN client VPN basé sur Open pour vous connecter à un point de VPN terminaison client.

Applications clientes

- Connectez-vous à un point de VPN terminaison client à l'aide d'une application cliente Windows
- Connectez-vous à un point de VPN terminaison client à l'aide d'une application VPN cliente Android ou iOS
- Connectez-vous à un point de VPN terminaison client à l'aide d'une application cliente macOS
- Connectez-vous à un point de VPN terminaison client à l'aide d'une application VPN client ouverte

Connectez-vous à un point de VPN terminaison client à l'aide d'une application cliente Windows

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

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés aux VPN connexions client avec des clients Windows.

> **Important**
>
> Si le point de VPN terminaison client a été configuré pour utiliser l'authentification fédérée SAML basée, vous ne pouvez pas utiliser le VPN client VPN basé sur Open pour vous connecter à un point de VPN terminaison client.

Tâches

- Utiliser un certificat du Windows Certificate System Store avec Open VPN
- Utilisez l'Open VPN GUI
- Utiliser le client Open VPN Connect

Utiliser un certificat du Windows Certificate System Store avec Open VPN

Vous pouvez configurer le VPN client Open pour utiliser un certificat et une clé privée provenant du Windows Certificate System Store. Cette option est utile lorsque vous utilisez une carte à puce dans le cadre de votre VPN connexion client. Pour plus d'informations sur l'option Open VPN client cryptoapicert, consultez le manuel de référence pour Open VPN on the Open website. VPN

> **Note**
>
> Le certificat doit être stocké sur l'ordinateur local.

Pour utiliser l'option cryptoapicert avec Open VPN

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 Comment : afficher les certificats à l'aide du MMC composant logiciel enfichable 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 Rights to see the local computer certificates store (Droits pour afficher le magasin de certificats de l'ordinateur local) sur le site Web Microsoft Technet.

4. Mettez à jour le fichier VPN de configuration Open et spécifiez le certificat en utilisant soit l'objet du certificat, soit l'empreinte numérique du certificat.

   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 How to: Retrieve the Thumbprint of a Certificate (Procédure : récupérer l'empreinte d'un certificat)sur le site Web Microsoft Technet.

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

Une fois la configuration terminée, utilisez Open VPN pour établir une connexion.

Utilisez l'Open VPN GUI

La procédure suivante indique comment établir une VPN connexion à l'aide de l'application VPN GUI client Open sur un ordinateur Windows.

> **Note**
>
> Pour plus d'informations sur l'application VPN client Open, consultez la section Téléchargements communautaires sur le VPN site Web Open.

Pour établir une VPN connexion

1. Démarrez l'application VPN client Open.
2. Dans la barre des tâches de Windows, choisissez Afficher/Masquer les icônes. Cliquez avec le bouton droit sur Ouvrir VPN GUI, puis sélectionnez Importer un fichier.
3. Dans la boîte de dialogue Ouvrir, sélectionnez le fichier de configuration que vous avez reçu de VPN l'administrateur du client et choisissez Ouvrir.
4. Dans la barre des tâches de Windows, choisissez Afficher/Masquer les icônes. Cliquez avec le bouton droit sur Ouvrir VPN GUI, puis sélectionnez Connect.

Utiliser le client Open VPN Connect

La procédure suivante indique comment établir une VPN connexion à l'aide de l'application Open VPN Connect Client sur un ordinateur Windows.

> **Note**
>
> Pour plus d'informations, voir Connexion au serveur Access avec Windows sur le VPN site Web Open.

Pour établir une VPN connexion

1. Démarrez l'application Open VPN Connect Client.
2. Dans la barre des tâches de Windows, choisissez Afficher/Masquer les icônes. Cliquez avec le bouton droit sur Ouvrir VPN, puis sélectionnez Importer le profil.
3. Choisissez Importer depuis un fichier et sélectionnez le fichier de configuration que vous avez reçu de l'VPNadministrateur de votre client.
4. Pour commencer la connexion, choisissez le profil de connexion.

Connectez-vous à un point de VPN terminaison client à l'aide d'une application VPN cliente Android ou iOS

> **Important**
>
> Si le point de VPN terminaison client a été configuré pour utiliser l'authentification fédérée SAML basée, vous ne pouvez pas utiliser le VPN client VPN basé sur Open pour vous connecter à un point de VPN terminaison client.

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

> **Note**
>
> Pour plus d'informations sur le téléchargement et l'utilisation de l'application VPN client Open pour iOS ou Android, consultez le guide de l'utilisateur Open VPN Connect sur le VPN site Web d'Open.

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Pour établir la connexion, démarrez l'application VPN client Open, puis importez le fichier que vous avez reçu de VPN l'administrateur du client.

Connectez-vous à un point de VPN terminaison client à l'aide d'une application cliente macOS

Ces sections décrivent comment établir une VPN connexion à l'aide de clients basés sur macOSVPN.

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés aux VPN connexions des clients avec les clients macOS.

> **Important**
>
> Si le point de VPN terminaison client a été configuré pour utiliser l'authentification fédérée SAML basée, vous ne pouvez pas utiliser le VPN client VPN basé sur Open pour vous connecter à un point de VPN terminaison client.

Rubriques

- Lancez Tunnelblick pour établir une connexion AWS Client VPN
- Connectez-vous à un AWS Client VPN point de terminaison à l'aide du client Open VPN Connect

Lancez Tunnelblick pour établir une connexion AWS Client VPN

La procédure suivante indique comment établir une VPN connexion 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 VPN connexion

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 VPN administrateur dans le panneau Configurations.
3. Sélectionnez le fichier de configuration dans le volet Configurations et choisissez Connect (Se connecter).

Connectez-vous à un AWS Client VPN point de terminaison à l'aide du client Open VPN Connect

La procédure suivante indique comment établir une VPN connexion à l'aide de l'application Open VPN Connect Client sur un ordinateur macOS.

> **Note**
>
> Pour plus d'informations, voir Connexion à Access Server avec macOS sur le VPN site Web Open.

Pour établir une VPN connexion

1. Lancez l'VPNapplication Open, puis choisissez Importer, À partir d'un fichier local... .
2. Accédez au fichier de configuration que vous avez reçu de votre VPN administrateur, puis choisissez Ouvrir.

Connectez-vous à un point de VPN terminaison client à l'aide d'une application VPN client ouverte

Ces sections décrivent comment établir une VPN connexion à l'aide de VPN clients VPN basés sur Open.

Avant de commencer, assurez-vous que votre VPN administrateur client a créé un point de VPN terminaison client et qu'il vous a fourni le fichier de configuration du VPN point de terminaison client.

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés aux VPN connexions client avec des clients basés sur Linux.

> **Important**
>
> Si le point de VPN terminaison client a été configuré pour utiliser l'authentification fédérée SAML basée, vous ne pouvez pas utiliser le VPN client VPN basé sur Open pour vous connecter à un point de VPN terminaison client.

Rubriques

- Créez une connexion à AWS Client VPN l'aide d'Open VPN - Network Manager
- Création d'une connexion à l' AWS Client VPN aide d'Open VPN

Créez une connexion à AWS Client VPN l'aide d'Open VPN - Network Manager

La procédure suivante indique comment établir une VPN connexion à l'aide de l'VPNapplication Open via le gestionnaire de réseau GUI sur un ordinateur Ubuntu.

Pour établir une VPN connexion

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 (+) à côté de VPN, puis choisissez Importer depuis un fichier... .
4. Accédez au fichier de configuration que vous avez reçu de votre VPN administrateur et choisissez Ouvrir.
5. Dans la VPN fenêtre Ajouter, choisissez Ajouter.
6. Démarrez la connexion en activant le bouton situé à côté du VPN profil que vous avez ajouté.

Création d'une connexion à l' AWS Client VPN aide d'Open VPN

La procédure suivante indique comment établir une VPN connexion à l'aide de l'VPNapplication Open sur un ordinateur Ubuntu.

Pour établir une VPN connexion

1. Installez Open VPN 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 VPN administrateur.

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

Résolution des problèmes liés à votre VPN connexion 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 VPN terminaison client.

Rubriques

Résolution des problèmes liés aux VPN terminaux clients pour les administrateurs

Vous pouvez effectuer certaines étapes de ce guide. Les autres étapes doivent être effectuées par votre VPN administrateur client sur le point de VPN terminaison client 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 aux VPN terminaux clients, consultez la section Résolution des problèmes liés VPN au client dans le guide de l'AWS Client VPN administrateur.

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.

Envoi 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 VPN connexions client avec des clients Windows

Les sections suivantes contiennent des informations sur les problèmes que vous pouvez rencontrer lors de l'utilisation de clients Windows pour vous connecter à un point de VPN terminaison client.

Rubriques

AWS client fourni

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.
- VPNJournaux ouverts : contiennent des informations sur VPN les processus ouverts. 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
```

Rubriques

Le client ne parvient pas à se connecter

Problème

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

Cause

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

- Un autre VPN processus Open 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 VPN applications Open sont en cours d'exécution sur votre ordinateur. Si tel est le cas, arrêtez ou quittez ces processus et réessayez de vous connecter au point de VPN terminaison client. Vérifiez la présence d'erreurs dans les VPN journaux ouverts et demandez à VPN l'administrateur de votre client 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 le CRL est toujours valide. Pour plus d'informations, consultez la section Clients incapables de se connecter à un point de VPN terminaison client dans le Guide de l'AWS Client VPN administrateur.

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

Problème

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

Le client est bloqué à l'état de reconnexion

Problème

Le client AWS fourni essaie de se connecter au point de VPN terminaison 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 DNS nom d'hôte ne se résout pas en adresse IP.
- Un VPN processus Open essaie indéfiniment de se connecter au point de terminaison.

Solution

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

VPNle processus de connexion s'arrête de façon inattendue

Problème

Lors de la connexion à un point de VPN terminaison client, 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

. NETLe Framework 4.7.2 ou supérieur 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 VPN terminaison du client utilise l'authentification mutuelle, le fichier de configuration (.ovpn) ne contient ni le certificat ni la clé du client.

Solution

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

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 VPN de configuration. 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. Accédez au VPNtéléchargement AWS du client 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 à jour l'application, vous pouvez également supprimer ou renommer les DLL fichiers. 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 DLL fichiers 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, DBROverlayIconBackuped par exemple .dll.bak.

VPNse déconnecte à l'aide d'un message contextuel

Problème

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

Cause

TAP-L'adaptateur 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
```

Ouvert VPN GUI

Les informations de dépannage suivantes ont été testées sur les versions 11.10.0.0 et 11.11.0.0 du VPN GUI logiciel Open sous Windows 10 Home (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
```

Ouvrez le client VPN Connect

Les informations de dépannage suivantes ont été testées sur les versions 2.6.0.100 et 2.7.1.101 du logiciel Open VPN Connect Client sous Windows 10 Home (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 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 DNS nom ne peut pas être résolu. Le client doit ajouter une chaîne aléatoire au DNS nom pour empêcher la DNS mise en cache ; toutefois, certains clients ne le font pas.

Solution

Consultez la solution pour l'impossibilité de résoudre le DNS nom du point de VPN terminaison du client dans le guide de AWS Client VPN l'administrateur.

PKIAlias manquant

Problème

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

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

Cause

Le logiciel Open VPN Connect Client présente un problème connu : 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 client et un certificat aléatoires dans le fichier VPN de configuration du client et importez la nouvelle configuration dans le logiciel Open VPN Connect Client. Vous pouvez également utiliser un autre client, tel que le VPN GUI client Open (v11.12.0.0) ou le client Viscosity (v.1.7.14).

Résolution des problèmes liés aux VPN connexions des clients avec les 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.

Rubriques

- AWS client fourni
- Tunnelblick
- Ouvert VPN

AWS client fourni

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.

- VPNJournaux ouverts : contiennent des informations sur VPN les processus ouverts. 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.

```
/tmp/AcvcHelperErrLog.txt
/tmp/AcvcHelperOutLog.txt
```

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

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

Rubriques

Le client ne parvient pas à se connecter

Problème

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

Cause

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

- Un autre VPN processus Open 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 VPN applications Open sont en cours d'exécution sur votre ordinateur. Si tel est le cas, arrêtez ou quittez ces processus et réessayez de vous connecter au point de VPN

terminaison client. Vérifiez la présence d'erreurs dans les VPN journaux ouverts et demandez à VPN l'administrateur de votre client 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 le CRL est toujours valide. Pour plus d'informations, consultez la section Clients incapables de se connecter à un point de VPN terminaison client dans le Guide de l'AWS Client VPN administrateur.

Le client est bloqué à l'état de reconnexion

Problème

Le client AWS fourni essaie de se connecter au point de VPN terminaison 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 DNS nom d'hôte ne se résout pas en adresse IP.
- Un VPN processus Open essaie indéfiniment de se connecter au point de terminaison.

Solution

Vérifiez que votre ordinateur est connecté à Internet. Demandez à votre VPN administrateur client de vérifier que la `remote` directive du fichier de configuration correspond à une adresse IP valide. Vous pouvez également déconnecter la VPN session en choisissant Déconnecter dans la fenêtre du AWS VPN client, puis en réessayant 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 VPN terminaison du client utilise l'authentification mutuelle, le fichier de configuration (.ovpn) ne contient ni le certificat ni la clé du client.

Solution

Assurez-vous que VPN l'administrateur du client ajoute le certificat client et la clé 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 leVPN.

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

Solution

Consultez l'article suivant sur AWS Re:Post. AWSVPNClient - L'outil d'assistance est requis (erreur)

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 la verbosité du journal, ouvrez l'application Tunnelblick, choisissez Paramètres et ajustez la valeur en fonction du niveau du 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 VPN version ouverte qui ne prend pas en charge l'algorithme de chiffrement AES -256-. GCM

Solution

Choisissez une VPN version Open compatible en procédant comme suit :

1. Ouvrez l'application Tunnelblick.
2. Sélectionnez Settings (Paramètres).
3. Pour la VPNversion ouverte, choisissez 2.4.6 - SSL La version ouverte 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 l'VPNadministrateur de votre client.

Utilisation étendue des clés (EKU)

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

Solution

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

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 VPN administrateur client.

Ouvert VPN

Les informations de dépannage suivantes ont été testées sur la version 2.7.1.100 du logiciel Open VPN Connect Client sous 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 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

Open VPN Connect ne parvient pas à résoudre le VPN DNS nom du client.

Solution

Consultez la solution pour l'impossibilité de résoudre le DNS nom du point de VPN terminaison du client dans le guide de AWS Client VPN l'administrateur.

Résolution des problèmes liés aux VPN connexions client 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 client fourni
- Ouvrir VPN (ligne de commande)
- Ouvrir VPN via le Gestionnaire de réseau (GUI)

AWS client fourni

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

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

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

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

Problème

Dans certains cas, une fois la VPN connexion établie, les DNS requêtes seront toujours envoyées au serveur de noms du système par défaut, au lieu des serveurs de noms configurés pour le point de terminaison du client. VPN

Cause

Le client interagit avec systemd-resolved, un service disponible sur les systèmes Linux, qui constitue un élément central de gestion. DNS Il est utilisé pour configurer les DNS serveurs qui sont poussés depuis le point de VPN terminaison du client. Le problème se produit parce que systemd-resolved ne définit pas la priorité la plus élevée pour DNS les serveurs fournis par le point de terminaison clientVPN. Il ajoute plutôt les serveurs à la liste existante des DNS serveurs configurés sur le système local. Par conséquent, les DNS serveurs d'origine peuvent toujours avoir la priorité la plus élevée, et donc être utilisés pour résoudre les DNS requêtes.

Solution

1. Ajoutez la directive suivante sur la première ligne du fichier de VPN configuration Open, pour vous assurer que toutes les DNS requêtes sont envoyées au VPN tunnel.

   ```
   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 voulez pas que les DNS requêtes soient résolues par systemd en proxy, mais que vous souhaitez plutôt que les requêtes soient envoyées directement aux vrais DNS serveurs de noms, créez un lien symbolique vers. `/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

   ```
   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 DNS réponses, la DNS configuration par interface, l'DNSSecapplication, etc. Cette option est particulièrement utile lorsque vous devez remplacer un DNS enregistrement public par un enregistrement privé lorsque vous êtes connecté àVPN. Par exemple, vous pouvez avoir un DNS résolveur privé dans votre espace privé VPC

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.

Ouvrir VPN (ligne de commande)

Problème

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

Cause

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

Solution

Procédez comme suit pour vérifier que le DNS serveur est configuré et fonctionne correctement.

1. Assurez-vous qu'une entrée de DNS serveur est présente dans les journaux. Dans l'exemple suivant, le DNS serveur `192.168.0.2` (configuré dans le point de VPN terminaison du client) 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 DNS serveur n'est spécifié, demandez à votre VPN administrateur client de modifier le point de VPN terminaison du client et assurez-vous qu'un DNS serveur (par exemple, le VPC DNS serveur) a été spécifié pour le point de VPN terminaison du client. Pour plus d'informations, voir Client VPN Endpoints dans le Guide de l'AWS Client VPN administrateur.
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 VPN de configuration du client (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
```

Ouvrir VPN via le Gestionnaire de réseau (GUI)

Problème

Lorsque vous utilisez le VPN client Network Manager Open, 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 l'impossibilité de résoudre le DNS nom du point de VPN terminaison du client dans le guide de AWS Client VPN l'administrateur.

Résolution des problèmes courants VPN liés aux clients

Les problèmes courants que vous pouvez rencontrer lorsque vous utilisez un client pour vous connecter à un point de VPN terminaison client sont les suivants.

TLSéchec de la négociation clé

Problème

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

Solution

Vérifiez si les règles de pare-feu de votre ordinateur bloquent le trafic entrant ou sortant ou le UDP trafic sur les ports 443 TCP ou 1194. Demandez à VPN l'administrateur de votre client de vérifier les informations suivantes :

- Que les règles de pare-feu pour le point de VPN terminaison du client ne bloquent TCP pas le UDP trafic 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 le CRL est toujours valide. Pour plus d'informations, consultez la section Clients incapables de se connecter à un point de VPN terminaison client dans le Guide de l'AWS Client VPN administrateur.

Historique du document

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

Modification	Description	Date
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 client fourni (3.14.0) pour Windows publié	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 client fourni (3.13.0) pour Windows publié	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 client fourni (3.12.1) pour Windows publié	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 client fourni (3.12.0) pour Windows publié	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 le client fourni pour Ubuntu 18.04 LTS et Ubuntu LTS 20.04 est sorti	Vous pouvez utiliser le client AWS fourni sur Ubuntu 18.04 LTS et Ubuntu 20.04. LTS	11 juin 2021

Support pour Open VPN à l'aide d'un certificat du Windows Certificate System Store	Vous pouvez utiliser Open VPN avec un certificat du Windows Certificate System Store.	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 VPN terminaison client.	4 février 2020
Première version	Cette version présente AWS ClientVPN.	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.