Guide de l’utilisateur

AWS Client VPN

AWS Client VPN: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'AWS Client VPN ?

AWS Client VPN est un service VPN géré, basé sur le client, qui vous permet d'accéder de façon sécurisée aux ressources AWS et aux ressources de votre réseau sur site.

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

Composants

Voici les composants clés pour utiliser AWS Client VPN.

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

Ressources supplémentaires

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

Mise en route avec Client VPN

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

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

Rubriques

Prerequisites

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

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

Étape 1 : Obtenir une application cliente VPN

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

Le client fourni par AWS est pris en charge sur Windows, macOS, Ubuntu 18.04 LTS et Ubuntu 20.04 LTS. Vous pouvez télécharger le client depuis le téléchargement d'AWS Client VPN.

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

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

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

Sinon, si votre administrateur Client VPN a configuré un portail libre-service pour le point de terminaison Client VPN, vous pouvez télécharger vous-même la dernière version du client fourni par AWS et la dernière version du fichier de configuration du point de terminaison Client VPN. Pour plus d'informations, consultez Utiliser le portail en libre-service.

Étape 3 : Connexion au réseau VPN

Importez le fichier de configuration du point de terminaison Client VPN sur le client fourni par AWS ou dans votre application cliente OpenVPN et connectez-vous au VPN. Pour savoir comment se connecter à un VPN, consultez les rubriques suivantes :

- Se connecter à l'aide AWS d'un client fourni
- Se connecter à l'aide d'un client OpenVPN

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

Pour les points de terminaison Client VPN qui utilisent l'authentification fédérée basée sur SAML (authentification unique), le client fourni par AWS ouvre une fenêtre de navigateur sur votre

ordinateur. Vous serez invité à saisir vos informations d'identification d'entreprise avant de pouvoir vous connecter au point de terminaison Client VPN.

Utiliser le portail en libre-service

Votre administrateur de point de terminaison Client VPN peut configurer un portail en libre-service pour le point de terminaison Client VPN. Le portail en libre-service est une page web qui vous permet de télécharger la dernière version du client fourni par AWS et la dernière version du fichier de configuration du point de terminaison Client VPN. Pour plus d'informations sur la configuration du portail en libre-service, consultez Points de terminaison Client VPN dans le Guide de l'administrateur AWS Client VPN.

Avant de commencer, vous devez disposer de l'ID du point de terminaison Client VPN. Votre administrateur de point de terminaison Client VPN peut vous fournir l'ID ou une URL de portail en libre-service qui inclut l'ID.

Pour accéder au portail en libre-service

1. Accédez au portail en libre-service à l'adresse https://self-service.clientvpn.amazonaws.com/ ou utilisez l'URL qui vous a été fournie par votre administrateur.
2. Si nécessaire, entrez l'ID du point de terminaison Client VPN, par exempl, `cvpn-endpoint-0123456abcd123456`. Choisissez Suivant.
3. Entrez votre nom d'utilisateur et votre mot de passe, puis choisissez Sign In (Se connecter). Il s'agit du même nom d'utilisateur et mot de passe que vous utilisez pour vous connecter au point de terminaison Client VPN.
4. Dans le portail en libre-service, vous pouvez effectuer les opérations suivantes :

   - Téléchargez la dernière version du fichier de configuration client pour le point de terminaison Client VPN.
   - Téléchargez la dernière version du client fourni par AWS pour votre plateforme.

Se connecter à l'aide AWS d'un client fourni

Vous pouvez vous connecter à un point de terminaison Client VPN à l'aide du client fourni par AWS. Le client fourni par AWS est pris en charge sur Windows, macOS, Ubuntu 18.04 LTS et Ubuntu 20.04 LTS.

Clients

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

Directives OpenVPN

Le client fourni par AWS prend en charge les directives OpenVPN 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
- key
- 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

La procédure suivante montre comment établir une connexion VPN à l'aide du client AWS fourni pour Windows. Vous pouvez télécharger et installer le client depuis la page de téléchargement de AWS Client VPN. Le client AWS fourni ne prend pas en charge les mises à jour automatiques.

Table des matières

Prérequis

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

- Système d'exploitation Windows 10 64 bits, processeur x64
- .NET Framework 4.7.2 ou version ultérieure

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

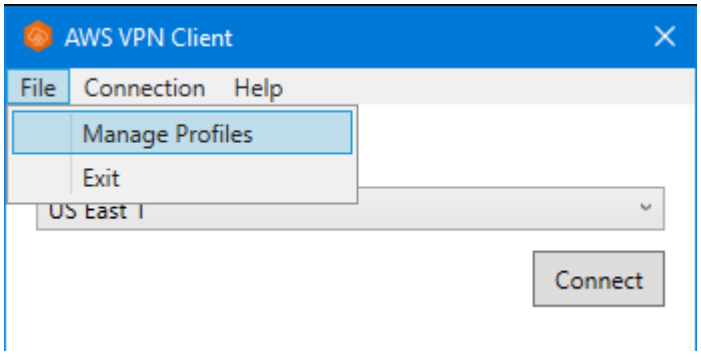
Avant de commencer, assurez-vous que votre administrateur Client VPN a créé un point de terminaison Client VPN et vous a fourni le fichier de configuration du point de terminaison Client VPN.

Connexion

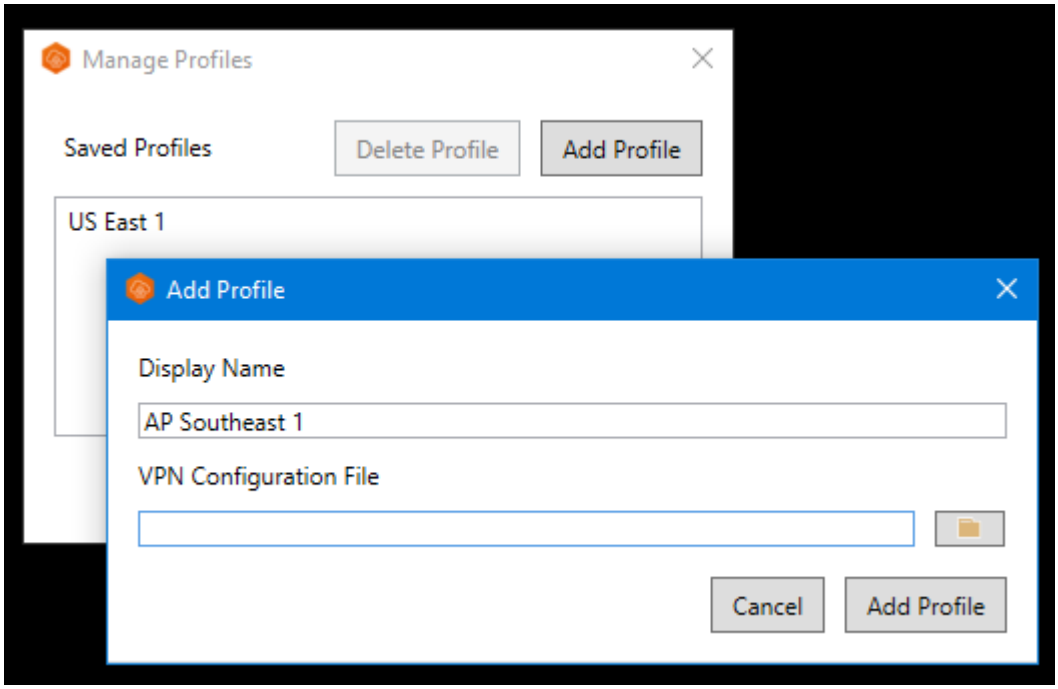
Avant de commencer, prenez connaissance des prérequis. Le client AWS fourni est également appelé AWS VPN client dans les étapes suivantes.

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

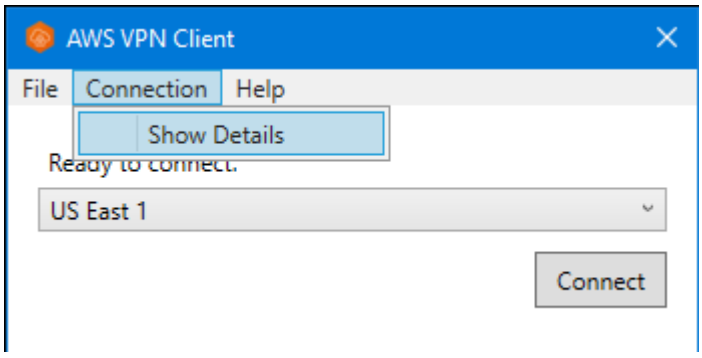
1. Ouvrez l'application AWS VPN Client.
2. Choisissez File (Fichier), Manage Profiles (Gérer les profils).



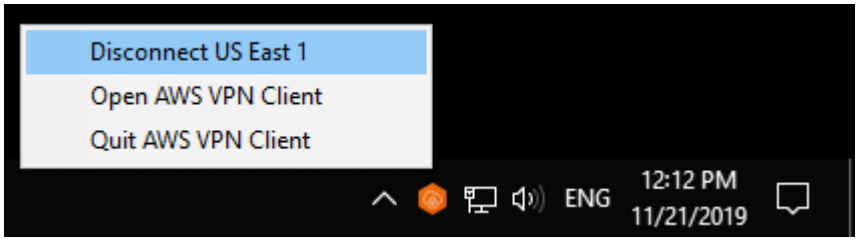
3. Choisissez Add Profile (Ajouter un profil).



4. Pour Profile name (Nom du profil), entrez un nom pour le profil.
5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN et sélectionnez-le, puis choisissez Add Profile (Ajouter un profil).
6. Dans la fenêtre AWS VPN Client, assurez-vous que votre profil est sélectionné, puis sélectionnez Connect (Connexion). Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe.
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).



Notes de mise à jour

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. Consultez les notes de publication pour plus de détails.

Version	Modifications	Date	Lien de téléchargement et SHA256
3.12.0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change. • Suppression du focus automatique sur les applications lors de la connexion à des points de terminaison SAML.	21 mai 2024	Télécharger la version 3.12.0 sha256 : fae30c27694a320b86c67e45043435c50c42753bddfdcc9b0112389ea881fba4
3.11.2	• Résolution d'un problème d'authentification SAML avec les navigateurs	11 avril 2024	Télécharger la version 3.11.2

Version	Modifications	Date	Lien de téléchargement et SHA256
	basés sur Chromium depuis la version 123.		sha256 : 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc
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 : fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Correction d'un problème de connectivité causé par les machines virtuelles Windows. • Problèmes de connectivité résolus pour certaines configurations de réseau local. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.11.0 sha256 : 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version	Modifications	Date	Lien de téléchargement et SHA256
3.10.0	• Correction d'un problème de connectivité lorsque NAT64 est activé sur le réseau client. • Correction d'un problème de connectivité lorsque les adaptateurs réseau Hyper-V sont installés sur l'ordinateur client. • Correctifs de bogues mineurs et améliorations	24 août 2023	Télécharger la version 3.10.0 sha256 : d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	• Posture de sécurité améliorée.	3 août 2023	Télécharger la version 3.9.0 sha256 : de9a3800ea2349155540bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
3.8.0	• Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.7.0	• Annulation des modifications apportées à la version 3.6.0.	15 juillet 2023	N'est plus pris en charge
3.6.0	• Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.5.0	Correctifs de bogues mineurs et améliorations	3 avril 2023	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
3.4.0	Annulation des modifications apportées à la version 3.3.0.	28 mars 2023	N'est plus pris en charge
3.3.0	Correctifs de bogues mineurs et améliorations	17 mars 2023	N'est plus pris en charge
3.2.0	• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ». • Détection automatique de la disponibilité des versions mises à jour du client. • Ajout de la possibilité d'installer automatiquement les nouvelles versions du client lorsqu'elles sont disponibles.	23 janvier 2023	N'est plus pris en charge
3.1.0	Posture de sécurité améliorée.	23 mai 2022	N'est plus pris en charge
3.0.0	• Ajout de la prise en charge de Windows 11. • Correction de la dénomination du pilote Windows TAP qui affectait d'autres noms de pilotes. • Correction du message de bannière qui n'était pas affiché lors de l'utilisation de l'authentification fédérée. • Correction de l'affichage du texte de la bannière pour des textes plus longs. • Posture de sécurité améliorée.	3 mars 2022	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
2.0.0	• Ajout de la prise en charge du texte des bannières une fois la nouvelle connexion établie. • Suppression de la possibilité d'utiliser pull-filter par rapport à l'écho, c'est-à-dire pull-filter * écho • Correctifs de bogues mineurs et améliorations	20 janvier 2022	N'est plus pris en charge
1.3.7	• Correction d'une tentative de connexion d'authentification fédérée dans certains cas. • Correctifs de bogues mineurs et améliorations	08 novembre 2021	N'est plus pris en charge
1.3.6	• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Correctifs de bogues mineurs et améliorations	20 septembre 2021	N'est plus pris en charge
1.3.5	Correctif pour supprimer les fichiers journaux volumineux des fenêtres.	16 août 2021	N'est plus pris en charge
1.3.4	• Ajout de la prise en charge de l'indicateur OpenVPN : dhcp-option. • Correctifs de bogue mineurs et améliorations.	4 août 2021	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.3.3	• Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route. • Résolution d'un problème qui bloquait l'application lors de la déconnexion ou de la sortie. • Correction d'un problème avec les noms d'utilisateur Active Directory avec barre oblique inverse. • Correction d'un blocage d'application lors de la manipulation de la liste de profil en dehors de l'application • Correctifs de bogue mineurs et améliorations.	1er juillet 2021	N'est plus pris en charge
1.3.2	• Ajouter la prévention des fuites IPv6, lorsqu'il est configuré. • Correction d'un incident potentiel lorsque vous utilisez l'option Afficher les détails sous Connexion.	12 mai 2021	N'est plus pris en charge
1.3.1	• Ajout de la prise en charge de plusieurs certificats clients avec le même sujet. Les certificats expirés seront ignorés. • Correction de la conservation des journaux locaux pour réduire l'utilisation du disque. • Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'. • Correctifs de bogue mineurs et améliorations.	5 avril 2021	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.3.0	Ajout de fonctionnalités de support, telles que le signalement d'erreurs, l'envoi de journaux de diagnostic et l'analytique.	8 mars 2021	N'est plus pris en charge
1.2.7	• Ajout de la prise en charge de la directive OpenVPN cryptoapicert. • Correction des routes périmées entre connexions. • Correctifs de bogue mineurs et améliorations.	25 février 2021	N'est plus pris en charge
1.2.6	Correctifs de bogue mineurs et améliorations.	26 octobre 2020	N'est plus pris en charge
1.2.5	• Ajout de la prise en charge des commentaires dans la configuration OpenVPN. • Ajout d'un message d'erreur pour les erreurs de liaison TLS.	8 octobre 2020	N'est plus pris en charge
1.2.4	Correctifs de bogue mineurs et améliorations.	1 septembre 2020	N'est plus pris en charge
1.2.3	Annulez les changements dans la version 1.2.2.	20 août 2020	N'est plus pris en charge
1.2.1	Correctifs de bogue mineurs et améliorations.	1er juillet 2020	N'est plus pris en charge
1.2.0	• Ajout de la prise en charge de l'authentification fédérée basée sur SAML 2.0. • Prise en charge obsolète de la plate-forme Windows 7.	19 mai 2020	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement et SHA256
1.1.1	Correctifs de bogue mineurs et améliorations.	21 avril 2020	N'est plus pris en charge
1.1.0	• Ajout de la prise en charge de la fonctionnalité écho « static-challenge » d'OpenVPN pour masquer ou afficher le texte affiché dans l'interface utilisateur. • Correctifs de bogue mineurs et améliorations.	9 mars 2020	N'est plus pris en charge
1.0.0	Version initiale.	4 février 2020	N'est plus pris en charge

AWS Client VPN pour macOS

La procédure suivante montre comment établir une connexion VPN à l'aide du client AWS fourni pour macOS. Vous pouvez télécharger et installer le client depuis la page de téléchargement de AWS Client VPN. Le client AWS fourni ne prend pas en charge les mises à jour automatiques.

Table des matières

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 port TCP 8096 sur votre ordinateur.

- Pour les points de terminaison Client VPN qui utilisent l'authentification fédérée basée sur SAML (authentification unique), le client réserve le port TCP 35001.

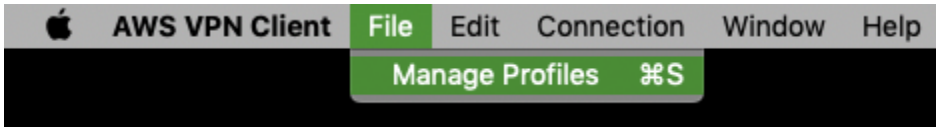
Connexion

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

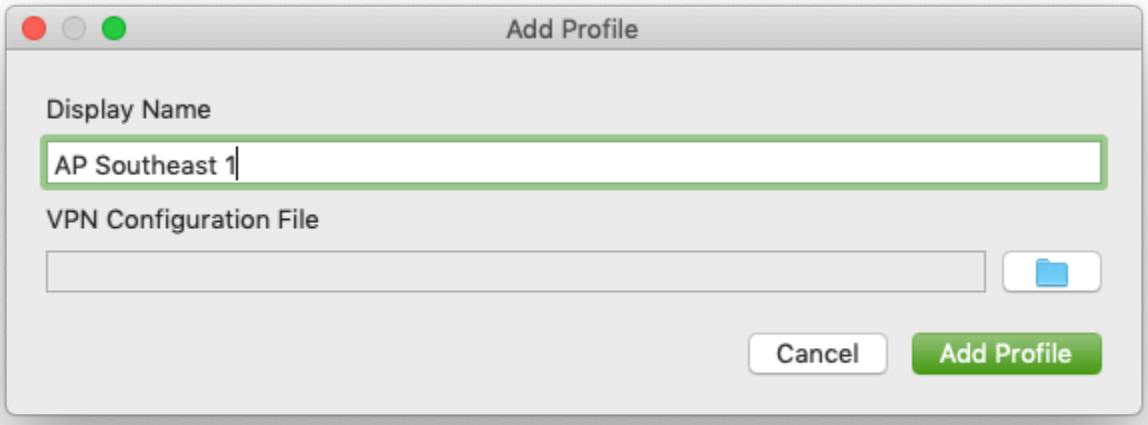
De même, prenez connaissance des prérequis. Le client AWS fourni est également appelé le AWS VPN client dans les étapes suivantes.

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

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



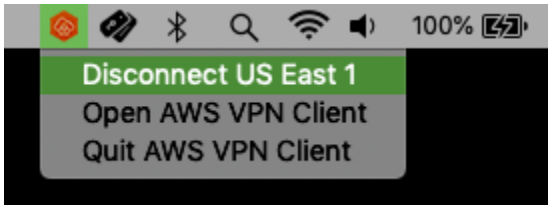
3. Choisissez Add Profile (Ajouter un profil).
4. Pour Profile name (Nom du profil), entrez un nom pour le profil.



5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN. 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 terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe.
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 >.



Notes de mise à jour

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. Consultez les notes de publication pour plus de détails.

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

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

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

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

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

Version	Modifications	Date	Lien de téléchargement
1.3.1	• Ajout de la prise en charge de macOS Big Sur (10.16). • Correction d'un problème qui supprimait les paramètres DNS configurés par d'autres applications. • Correction d'un problème lors de l'utilisation d'un certificat non valide pour l'authentification mutuelle, provoquant des problèmes de connectivité. • Ajout de la prise en charge de la directive OpenVPN 'route-ipv6'. • Correctifs de bogue mineurs et améliorations.	5 avril 2021	N'est plus pris en charge.
1.3.0	Ajout de fonctionnalités de support, telles que le signalement d'erreurs, l'envoi de journaux de diagnostic et l'analytique.	8 mars 2021	N'est plus pris en charge.
1.2.5	Correctifs de bogue mineurs et améliorations.	25 février 2021	N'est plus pris en charge.
1.2.4	Correctifs de bogue mineurs et améliorations.	26 octobre 2020	N'est plus pris en charge.
1.2.3	• Ajout de la prise en charge des commentaires dans la configuration OpenVPN. • Ajout d'un message d'erreur pour les erreurs de liaison TLS. • Correction d'un bug de désinstallation affectant certains utilisateurs.	8 octobre 2020	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.2.2	Correctifs de bogue mineurs et améliorations.	12 août 2020	N'est plus pris en charge.
1.2.1	• Ajout de la prise en charge de la désinstallation de l'application. • Correctifs de bogue mineurs et améliorations.	1er juillet 2020	N'est plus pris en charge.
1.2.0	• Ajout de la prise en charge de l'authentification fédérée basée sur SAML 2.0. • Ajout de la prise en charge de macOS Catalina (10.15).	19 mai 2020	N'est plus pris en charge.
1.1.2	Correctifs de bogue mineurs et améliorations.	21 avril 2020	N'est plus pris en charge.
1.1.1	• Correction d'un problème de non-résolution DNS. • Correction d'un problème de panne d'application causé par des connexions plus longues. • Correction d'un problème d'authentification MFA.	2 avril 2020	N'est plus pris en charge.
1.1.0	• Ajout de la prise en charge de la configuration DNS macOS. • Ajout de la prise en charge de la fonctionnalité écho « static-challenge » d'OpenVPN pour masquer ou afficher le texte affiché dans l'interface utilisateur. • Correctifs de bogue mineurs et améliorations.	9 mars 2020	N'est plus pris en charge.

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

AWS Client VPN pour Linux

Les procédures suivantes indiquent comment installer le client AWS fourni pour Linux et établir une connexion VPN à l'aide du client AWS fourni. Le client AWS fourni pour Linux ne prend pas en charge les mises à jour automatiques.

Table des matières

Prérequis

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

- Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS (AMD64 uniquement)

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

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

Installation

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 paquets

1. Ajoutez la clé publique 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 à partir de Téléchargement de AWS Client VPN ou à l'aide de la commande suivante.

```
curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
 awsvpnclient_amd64.deb
```

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

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

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

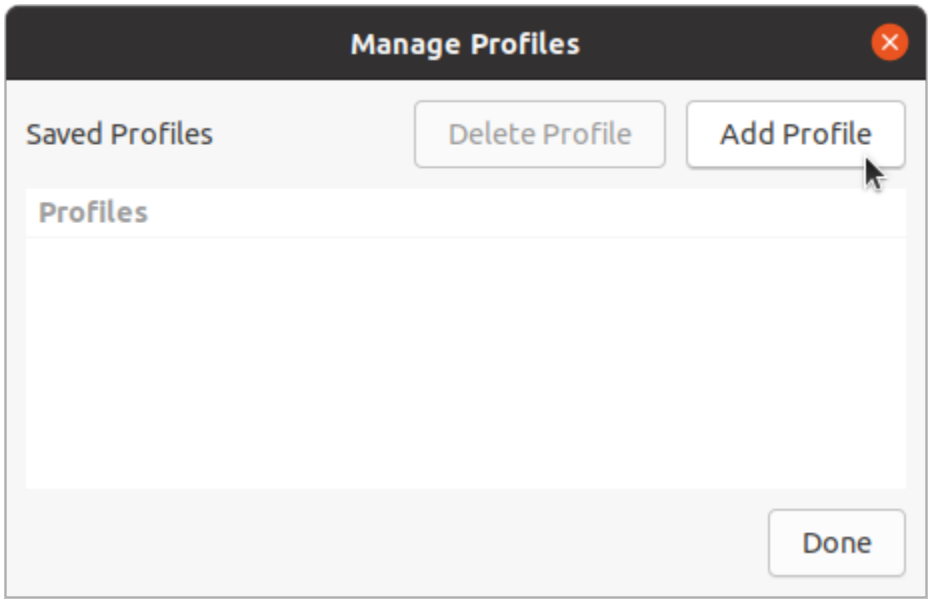
1. Téléchargez le fichier de package .deb à partir deTéléchargement de AWS Client VPN.
2. Après avoir téléchargé le fichier de package .deb, utilisez la Logithèque Ubuntu pour installer le package. Suivez la procédure d'installation à partir d'un paquet .deb autonome à l'aide du Logithèque Ubuntu, comme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

Connexion

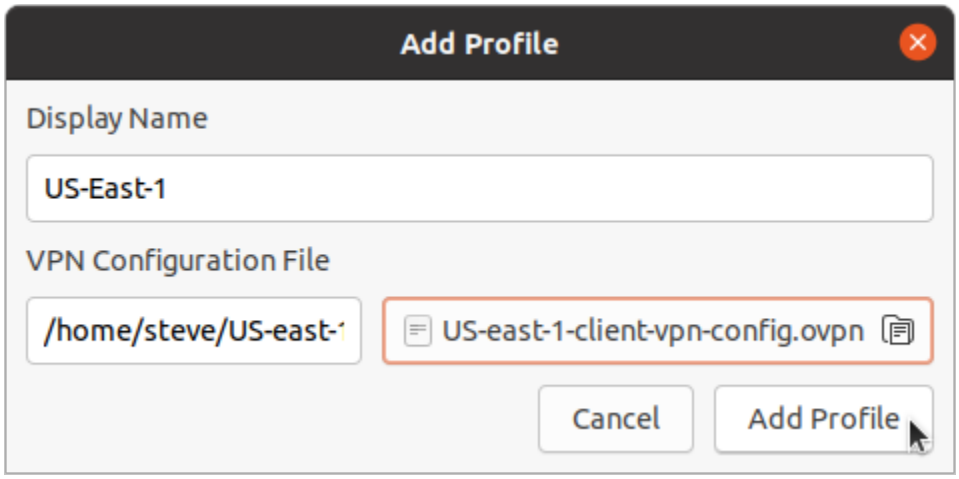
Le client AWS fourni est également appelé le AWS VPN client dans les étapes suivantes.

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

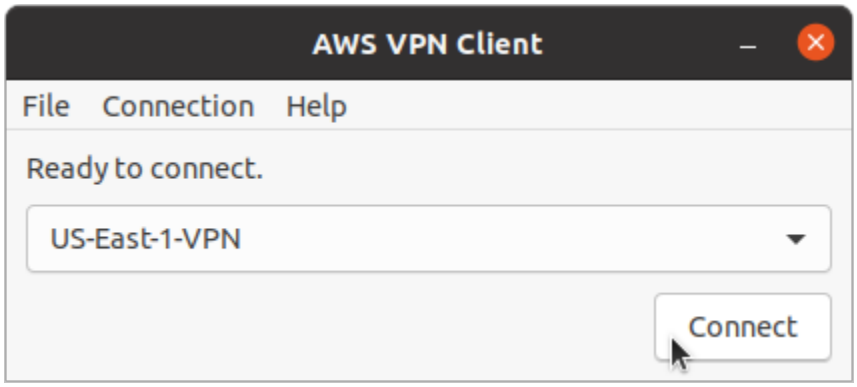
1. Ouvrez l'application AWS VPN Client.
2. Choisissez File (Fichier), Manage Profiles (Gérer les profils).
3. Choisissez Add Profile (Ajouter un profil).



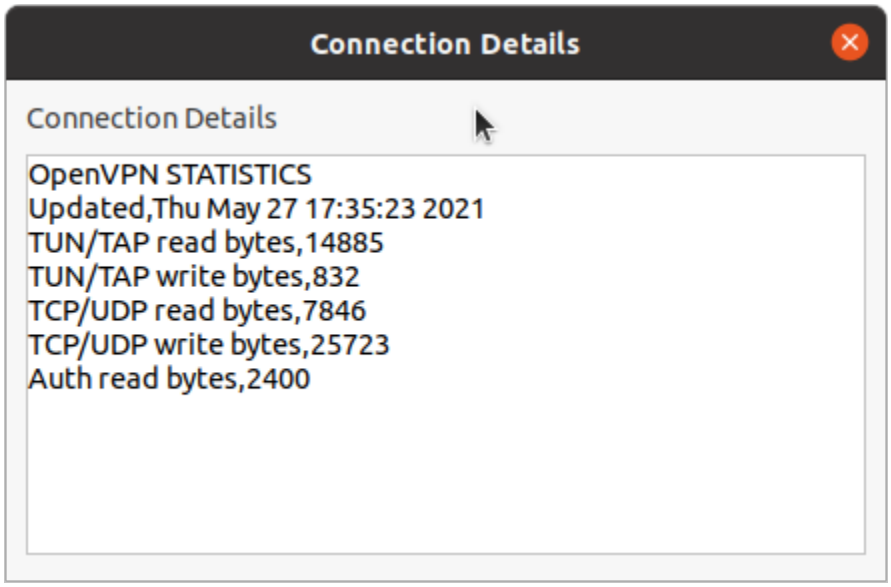
4. Pour Profile name (Nom du profil), entrez un nom pour le profil.
5. Pour VPN Configuration File (Fichier de configuration VPN), accédez au fichier de configuration que vous avez reçu de votre administrateur Client VPN. Choisissez Open.
6. Choisissez Add Profile (Ajouter un profil).



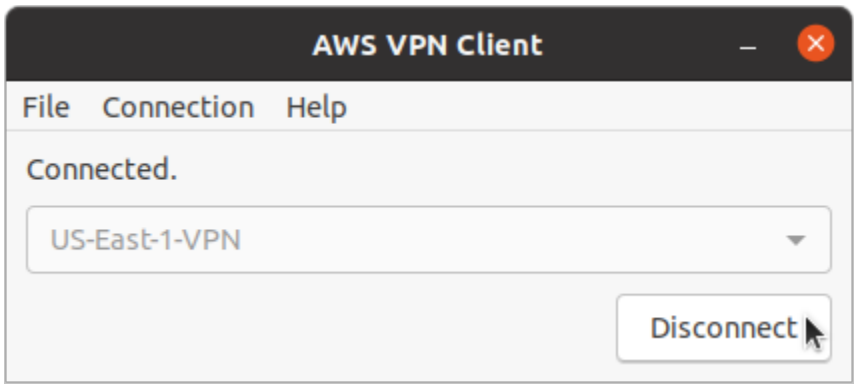
7. Dans la fenêtre AWS VPN Client, assurez-vous que votre profil est sélectionné, puis sélectionnez Connect (Connexion). Si le point de terminaison Client VPN a été configuré pour utiliser l'authentification basée sur les informations d'identification, vous serez invité à saisir un nom d'utilisateur et un mot de passe.



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).



Notes de mise à jour

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. Consultez les notes de publication pour plus de détails.

Version	Modifications	Date	Lien de téléchargement
3,13,0	• Reconnectez-vous automatiquement lorsque la portée du réseau local change.	21 mai 2024	Télécharger la version 3.13.0 sha256 : e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1
3.12.2	• Résolution d'un problème d'authentification SAML avec les navigateurs basés sur Chromium depuis la version 123.	11 avril 2024	Télécharger la version 3.12.2 sha256 : f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
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

Version	Modifications	Date	Lien de téléchargement
3.12.0	• Problèmes de connectivité résolus pour certaines configurations de réseau local.	19 décembre 2023	Télécharger la version 3.12.0 sha256 : 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Restauration pour « Problèmes de connectivité résolus pour certaines configurations de réseau local ». • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.11.0 sha256 : 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• Problèmes de connectivité résolus pour certaines configurations de réseau local. • Accessibilité améliorée.	6 décembre 2023	Télécharger la version 3.10.0 sha256 : e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51

Version	Modifications	Date	Lien de téléchargement
3.9.0	• Correction d'un problème de connectivité lorsque 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
3.7.0	• Posture de sécurité améliorée.	15 juillet 2023	N'est plus pris en charge
3.6.0	• Annulation des modifications apportées à la version 3.5.0.	15 juillet 2023	N'est plus pris en charge
3.5.0	• Posture de sécurité améliorée.	14 juillet 2023	N'est plus pris en charge
3.4.0	• Ajout de la prise en charge de l'indicateur OpenVPN « verify-x509-name ».	14 février 2023	N'est plus pris en charge

Version	Modifications	Date	Lien de téléchargement
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.
1.0.3	• Correction d'une tentative de connexion d'authentification fédérée dans certains cas. • Correctifs de bogues mineurs et améliorations	08 novembre 2021	N'est plus pris en charge.
1.0.2	• Ajout du support pour les drapeaux OpenVPN : connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Correctifs de bogues mineurs et améliorations	28 septembre 2021	N'est plus pris en charge.

Version	Modifications	Date	Lien de téléchargement
1.0.1	• Option activée pour quitter la barre d'application Ubuntu. • Ajout du support pour les drapeaux OpenVPN : inactif, pull-filter, route. • Correctifs de bogue mineurs et améliorations.	4 août 2021	N'est plus pris en charge.
1.0.0	Version initiale.	11 juin 2021	N'est plus pris en charge.

Se connecter à l'aide d'un client OpenVPN

Vous pouvez vous connecter à un point de terminaison Client VPN à l'aide d'applications clientes OpenVPN courantes.

> **Note**
>
> Pour l'authentification fédérée basée sur SAML, vous devez utiliser le client AWSfourni par AWS pour vous connecter au point de terminaison VPN du client. Pour en savoir plus, consultez Se connecter à l'aide AWS d'un client fourni ou contactez votre administrateur VPN.

Applications clientes

- Se connecter à l'aide d'une application cliente Windows
- Se connecter à l'aide d'une application Client VPN Android ou iOS
- Se connecter à l'aide d'une application cliente macOS
- Se connecter à l'aide d'une application cliente OpenVPN

Se connecter à l'aide d'une application cliente Windows

Les procédures suivantes montrent comment établir une connexion VPN à l'aide de clients VPN Windows.

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

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés à Windows.

OpenVPN avec un certificat du magasin de certificats système de Windows

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

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

Pour utiliser l'option cryptoapicert avec OpenVPN

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

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

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   Voici un exemple de spécification du certificat à l'aide d'une empreinte. Microsoft Management Console permet de trouver l'empreinte. Pour plus d'informations, consultez 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 OpenVPN pour établir une connexion.

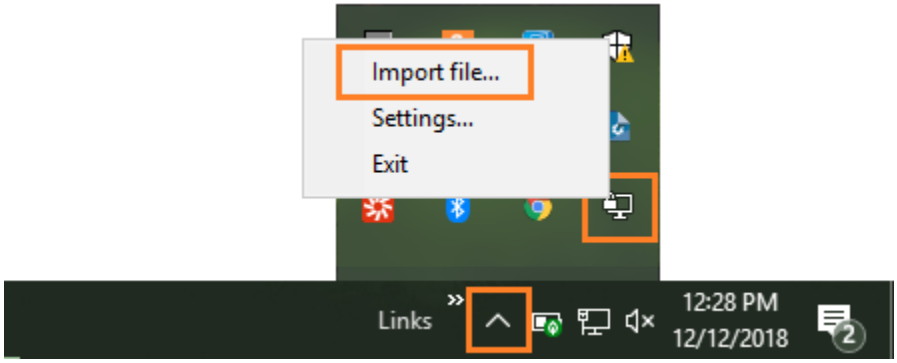
OpenVPN GUI

La procédure suivante montre comment établir une connexion VPN à l'aide de l'application cliente OpenVPN GUI sur un ordinateur Windows.

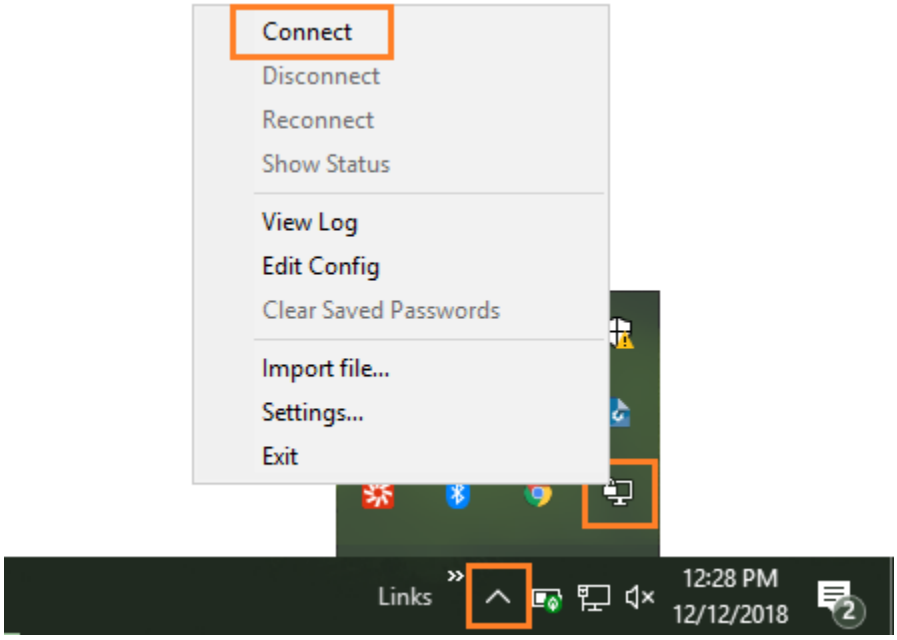
> **Note**
>
> Pour de plus amples informations sur l'application cliente OpenVPN, veuillez consulter Téléchargements de communauté sur le site web OpenVPN.

Pour établir une connexion VPN

1. Démarrez l'application cliente OpenVPN.
2. Sur la barre des tâches Windows, cliquez sur les Show/Hide icons (Afficher/Masquer les icônes), cliquez avec le bouton droit sur OpenVPN GUI et choisissez Import file (Importer le fichier).



3. Dans la boîte de dialogue Open (Ouvrir), sélectionnez le fichier de configuration que vous avez reçu de votre administrateur Client VPN et choisissez Open (Ouvrir).
4. Sur la barre des tâches Windows, cliquez sur Show/Hide icons (Afficher/Masquer les icônes), cliquez avec le bouton droit sur OpenVPN GUI et choisissez Connect (Se connecter).



OpenVPN Connect Client

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

> **Note**
>
> Pour de plus amples informations, veuillez consulter Connexion au serveur d'accès avec Windows sur le site web OpenVPN.

Pour établir une connexion VPN

1. Démarrez l'application OpenVPN Connect Client.
2. Sur la barre des tâches Windows, cliquez sur Show/Hide icons (Afficher/Masquer les icônes), cliquez avec le bouton droit sur OpenVPN et choisissez Import profile (Importer le profil).
3. Choisissez Import from File (Importer à partir du fichier) et sélectionnez le fichier de configuration que vous avez reçu de votre administrateur Client VPN.
4. Pour commencer la connexion, choisissez le profil de connexion.

Se connecter à l'aide d'une application Client VPN Android ou iOS

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

> **Note**
>
> Pour plus d'informations sur l'application cliente OpenVPN pour Android, consultez la section FAQ regarding OpenVPN Connect Android sur le site Web OpenVPN.

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

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

Se connecter à l'aide d'une application cliente macOS

Les procédures suivantes montrent comment établir une connexion VPN à l'aide de clients VPN macOS.

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

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés à macOS.

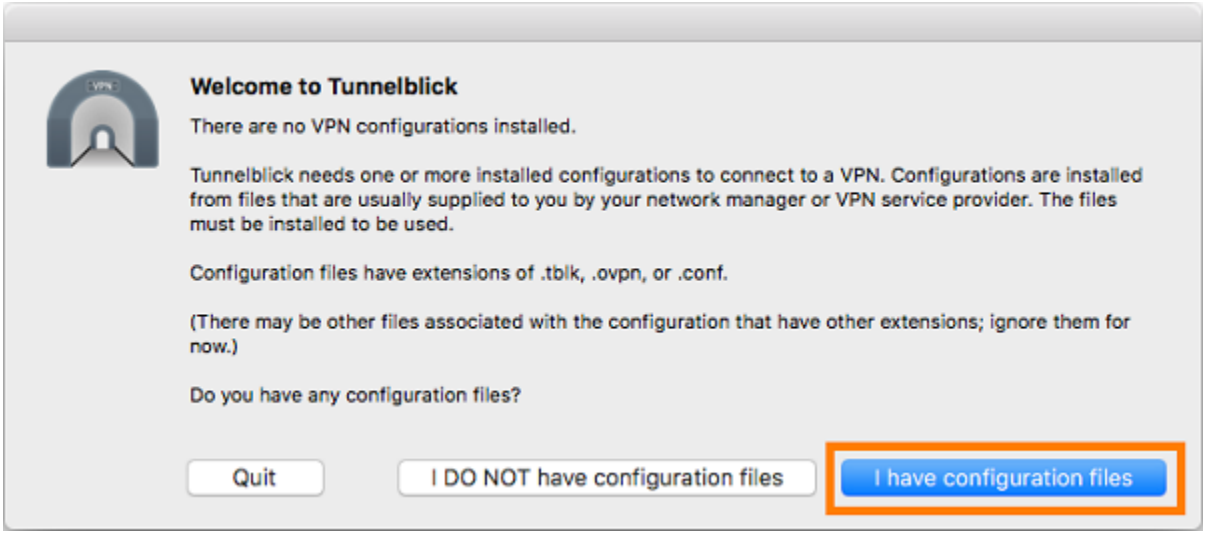
Tunnelblick

La procédure suivante montre comment établir une connexion VPN à l'aide de l'application cliente Tunnelblick sur un ordinateur macOS.

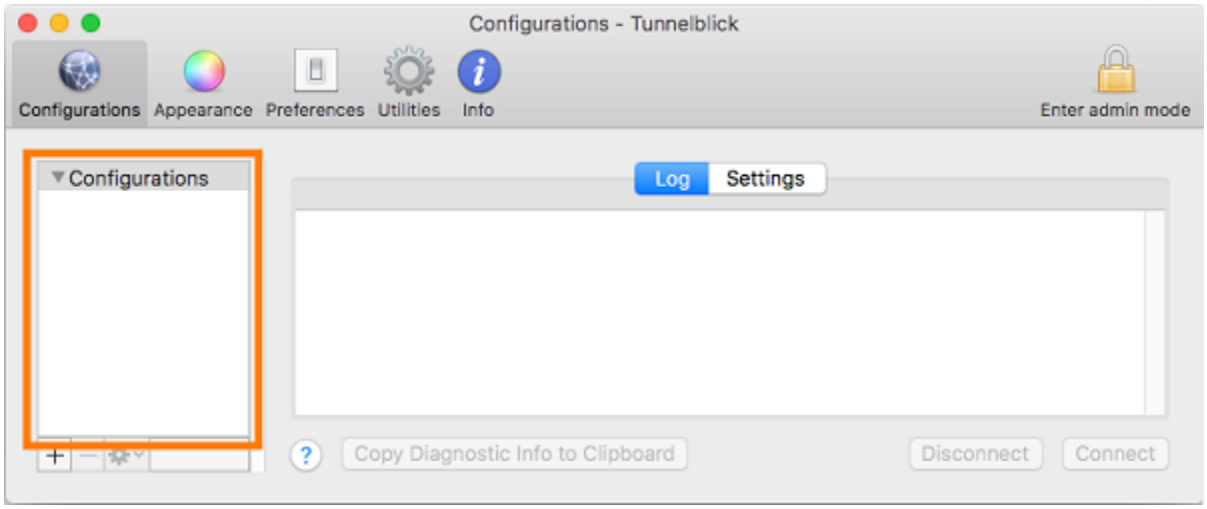
> **Note**
>
> Pour plus d'informations sur l'application cliente Tunnelblick pour macOS, consultez la documentation Tunnelblick sur le site web Tunnelblick.

Pour établir une connexion VPN

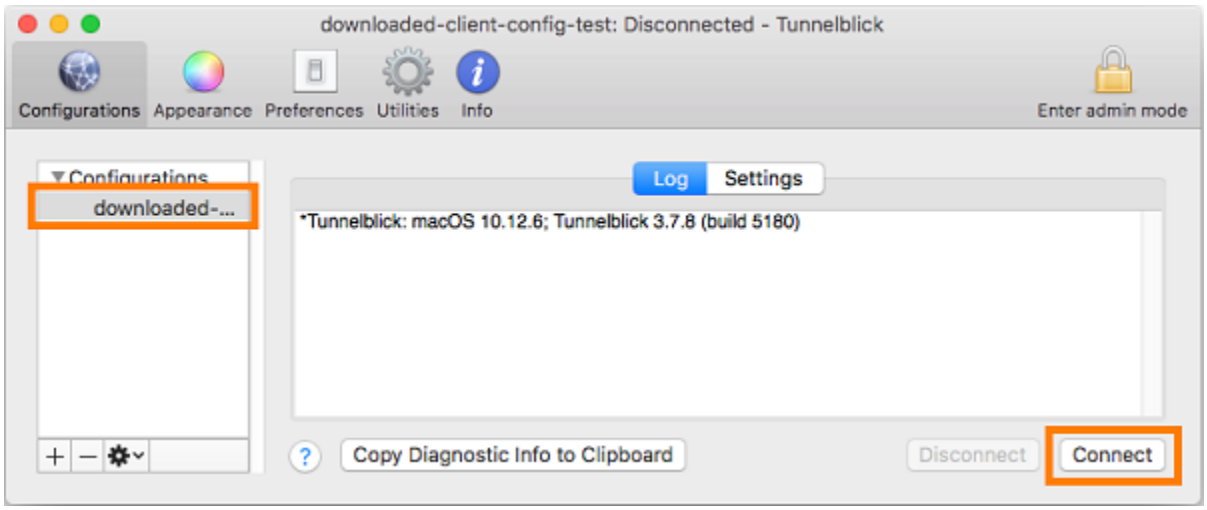
1. Démarrez l'application cliente Tunnelblick et choisissez I have configuration files (Je dispose des fichiers de configuration).



2. Faites glisser le fichier de configuration que vous avez reçu de votre administrateur VPN vers le panneau Configurations.



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



OpenVPN Connect Client

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

> **Note**
>
> Pour de plus amples informations, veuillez consulter Connexion au serveur d'accès avec macOS sur le site Web OpenVPN.

Pour établir une connexion VPN

1. Démarrez l'application OpenVPN et choisissez Import (Importer), From local file... (Depuis le fichier local).
2. Accédez au fichier de configuration que vous avez reçu de votre administrateur VPN et choisissez Open (Ouvrir).

Se connecter à l'aide d'une application cliente OpenVPN

Les procédures suivantes montrent comment établir une connexion VPN à l'aide de clients VPN basés sur OpenVPN.

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

Pour plus d'informations sur le dépannage, consultez Résolution des problèmes liés à Linux.

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

OpenVPN - Network Manager

La procédure suivante montre comment établir une connexion VPN à l'aide de l'application OpenVPN via l'interface graphique Network Manager sur un ordinateur Ubuntu.

Pour établir une connexion VPN

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

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

2. Accédez à Settings (Paramètres), Network (Réseau).
3. Choisissez le symbole plus (+) en regard de VPN, puis choisissez Import from file... (Importer à partir du fichier).

4. Accédez au fichier de configuration que vous avez reçu de votre administrateur VPN et choisissez Open (Ouvrir).
5. Dans la fenêtre Ajouter un VPN choisissez Ajouter.
6. Démarrez la connexion en activant le bouton en regard du profil VPN que vous avez ajouté.

OpenVPN

La procédure suivante montre comment établir une connexion VPN à l'aide de l'application OpenVPN sur un ordinateur Ubuntu.

Pour établir une connexion VPN

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

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

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

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

Résolution des problèmes de votre connexion Client VPN

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

Rubriques

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

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

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

Envoyer les journaux de diagnostic AWS Support au client AWS fourni

Si vous rencontrez des problèmes avec le client AWS fourni et que vous devez le contacter AWS Support pour résoudre le problème, le client 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 la possibilité de copier les informations dans votre presse-papier si vous le souhaitez.

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

Résolution des problèmes liés à Windows

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

Rubriques

AWS client fourni

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.
- Journaux OpenVPN : contiennent des informations sur les processus OpenVPN. Le préfixe « ovpn_aws_vpn_client_ » est ajouté au nom de ces journaux.

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

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

Rubriques

- Le client ne peut pas se connecter et reçoit le message de journal « aucun adaptateur TAP-Windows »
- Le client est bloqué à l'état de reconnexion
- Le processus de connexion VPN se ferme de façon inattendue
- Échec du lancement de l'application
- Le client ne parvient pas à créer de profil
- Un plantage du client se produit sur les ordinateurs Dell qui utilisent Windows 10 ou 11
- Le VPN se déconnecte avec un message contextuel

Le client ne parvient pas à se connecter

Problème

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

Cause

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

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

Solution

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

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

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

Problème

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

Solution

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

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

Le client est bloqué à l'état de reconnexion

Problème

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

Cause

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

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

Solution

Vérifiez que votre ordinateur est connecté à Internet. Demandez à votre administrateur Client VPN de vérifier que la directive `remote` du fichier de configuration est résolue en une adresse IP valide. Vous

pouvez également déconnecter la session VPN en choisissant Déconnecter dans la fenêtre du client AWS VPN, puis réessayer de vous connecter.

Le processus de connexion VPN se ferme de façon inattendue

Problème

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

Cause

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

Solution

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

Échec du lancement de l'application

Problème

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

Cause

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

Solution

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

Le client ne parvient pas à créer de profil

Problème

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

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

Cause

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

Solution

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

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

Problème

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

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

Cause

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

- DBR.dll ShellExtension
- DBR.dll OverlayIconBackuped
- DBR.dll OverlayIconNotBackuped

Solution

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

En outre, effectuez l'une des opérations suivantes :

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

Supprimer ou renommer les fichiers DLL

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

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

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

   - DBR.dll ShellExtension
   - DBR.dll OverlayIconBackuped
   - DBR.dll OverlayIconNotBackuped

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

Le VPN se déconnecte avec un message contextuel

Problème

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

Cause

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

Solution

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

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

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

OpenVPN GUI

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

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

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

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

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

Client de connexion OpenVPN

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

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

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

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

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

Impossible de résoudre le DNS

Problème

La connexion échoue avec l'erreur suivante.

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

Cause

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

Solution

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

Alias PKI manquant

Problème

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

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

Cause

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

Solution

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

Résolution des problèmes liés à 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
- OpenVPN

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.

- Journaux OpenVPN : contiennent des informations sur les processus OpenVPN. Le préfixe « ovpn_aws_vpn_client_ » est ajouté au nom de ces journaux.

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

```
/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
- Le client est bloqué à l'état de reconnexion
- Le client ne parvient pas à créer de profil

Le client ne parvient pas à se connecter

Problème

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

Cause

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

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

Solution

Vérifiez si d'autres applications OpenVPN sont en cours d'exécution sur votre ordinateur. Si une connexion est en cours d'exécution, arrêtez ou quittez ces processus et essayez de vous connecter

à nouveau au point de terminaison Client VPN. Vérifiez les erreurs dans les journaux OpenVPN et demandez à votre administrateur Client VPN de vérifier les informations suivantes :

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

Le client est bloqué à l'état de reconnexion

Problème

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

Cause

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

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

Solution

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

Le client ne parvient pas à créer de profil

Problème

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

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

Cause

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

Solution

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

Tunnelblick

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

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

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

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

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

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

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

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

Algorithme de chiffrement AES-256-GCM introuvable

Problème

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

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

Cause

L'application utilise une version OpenVPN qui ne prend pas en charge l'algorithme de chiffrement AES-256-GCM.

Solution

Choisissez une version OpenVPN compatible en procédant comme suit :

1. Ouvrez l'application Tunnelblick.
2. Sélectionnez Settings (Paramètres).
3. Pour OpenVPN version (Version OpenVPN), choisissez 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - La version OpenSSL est v1.0.2q).

La connexion cesse de répondre et se réinitialise

Problème

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

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

Cause

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

Solution

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

EKU, Extended key usage (Utilisation étendue des clés)

Problème

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

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

Cause

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

Solution

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

Certificat expiré

Problème

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

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

Cause

Le certificat de client a expiré.

Solution

Demandez un nouveau certificat client à votre administrateur Client VPN.

OpenVPN

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

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

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

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

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

Impossible de résoudre le DNS

Problème

La connexion échoue avec l'erreur suivante.

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

Cause

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

Solution

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

Résolution des problèmes liés à 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

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

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

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

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

Problème

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

Cause

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

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

Solution

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

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

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

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

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

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

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

OpenVPN (ligne de commande)

Problème

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

Cause

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

Solution

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

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

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

   Si aucun serveur DNS n'est spécifié, demandez à votre administrateur Client VPN de modifier le point de terminaison Client VPN et assurez-vous qu'un serveur DNS (par exemple, le serveur DNS VPC) a été spécifié pour le point de terminaison Client VPN. Pour plus d'informations, consultez Points de terminaison Client VPN dans le Guide de l'administrateur AWS Client VPN .
2. Assurez-vous que le package `resolvconf` est installé en exécutant la commande suivante.

   ```
   sudo apt list resolvconf
   ```

   La sortie doit renvoyer les informations suivantes.

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

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

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

   ```
   script-security 2
   ```

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

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

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

OpenVPN via Network Manager (interface utilisateur graphique)

Problème

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

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

Cause

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

Solution

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

Problèmes courants

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

Échec de la négociation de clé TLS

Problème

La négociation TLS échoue avec l'erreur suivante.

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

Cause

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

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

Solution

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

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

Historique du document

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

Modification	Description	Date
AWS 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 Le client fourni (3.12.2) pour Ubuntu est sorti	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 Le client fourni (3.10.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	6 décembre 2023
AWS sortie du client fourni (3.9.0) 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 Le client fourni (3.6.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.5.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	15 juillet 2023
AWS sortie du client fourni (3.6.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
AWS sortie du client fourni (3.5.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023

AWS sortie du client fourni (3.4.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	14 juillet 2023
AWS sortie du client fourni (3.3.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	27 avril 2023
AWS sortie du client fourni (3.5.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	3 avril 2023
AWS sortie du client fourni (3.4.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	28 mars 2023
AWS sortie du client fourni (3.3.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	17 mars 2023
AWS sortie du client fourni (3.4.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	14 février 2023
AWS sortie du client fourni (3.2.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
AWS client fourni (3.2.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	23 janvier 2023
AWS sortie du client fourni (3.1.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
AWS sortie du client fourni (3.1.0) pour Windows	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022

AWS sortie du client fourni (3.1.0) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	23 mai 2022
AWS sortie du client fourni (3.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
AWS client fourni (3.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
AWS Le client fourni (3.0.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	3 mars 2022
AWS sortie du client fourni (2.0.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS client fourni (2.0.0) pour Windows publié	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS Le client fourni (2.0.0) pour Ubuntu est sorti	Pour plus d'informations, consultez les notes de mise à jour.	20 janvier 2022
AWS sortie du client fourni (1.4.0) pour macOS	Pour plus d'informations, consultez les notes de mise à jour.	9 novembre 2021
AWS sortie du client fourni pour Windows (1.3.7)	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021
AWS sortie du client fourni (1.0.3) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	8 novembre 2021

AWS sortie du client fourni (1.0.2) pour Ubuntu	Pour plus d'informations, consultez les notes de mise à jour.	28 septembre 2021
AWS le client fourni pour Windows (1.3.6) et macOS (1.3.5) est sorti	Pour plus d'informations, consultez les notes de mise à jour.	20 septembre 2021
AWS client fourni pour Ubuntu 18.04 LTS et Ubuntu 20.04 LTS publié	Vous pouvez utiliser le client AWS fourni sur Ubuntu 18.04 LTS et Ubuntu 20.04 LTS.	11 juin 2021
Support d'OpenVPN avec un certificat du magasin de certificats système de Windows	Vous pouvez utiliser OpenVPN avec un certificat du magasin de certificats système de Windows.	25 février 2021
Portail en libre-service	Vous pouvez accéder à un portail en libre-service pour obtenir le client et le fichier de configuration les plus récents AWS fournis.	29 octobre 2020
AWS client fourni	Vous pouvez utiliser le client AWS fourni pour vous connecter à un point de terminaison VPN client.	4 février 2020
Première version	Cette version introduit AWS le Client VPN.	18 décembre 2018

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.