Guida per l'utente

AWS Cliente VPN

AWS Cliente VPN: Guida per l'utente

Table of Contents

Che cos'è AWS ClientVPN? 1
Componenti del client VPN 1
Risorse aggiuntive per la configurazione del client VPN 1
Inizia con Client VPN 2
Prerequisiti per l'utilizzo di Client VPN 2
Passaggio 1: procurarsi un'applicazione client VPN 2
Fase 2: Ottenete il file di configurazione dell'VPNendpoint del client 3
Fase 3: Connect a VPN 3
Scarica Client VPN 4
Connect utilizzando un client AWS fornito 5
Windows 6
Requisiti 7
Connect utilizzando il client 7
Note di rilascio 8
macOS 16
Requisiti 16
Connect utilizzando il client 17
Note di rilascio 18
Linux 26
Requisiti per la connessione al client VPN con un client AWS fornito per Linux 26
Installa il client 27
Connect utilizzando il client 28
Note di rilascio 29
Connect utilizzando un VPN client Open 35
Windows 35
Usa un certificato 36
Usa Open VPN GUI 37
Usa il client Open VPN Connect 37
Android e iOS 38
macOS 39
Crea una connessione usando Tunnelblick 39
Connessione tramite Open VPN Connect Client 40
Linux 40
Connect utilizzando Open VPN - Network Manager 41

Connect usando Open VPN 41
Risoluzione dei problemi 43
Risoluzione dei problemi relativi agli VPN endpoint del client per gli amministratori 43
Invia i log di diagnostica AWS Support al client fornito AWS 43
Invio dei log di diagnostica 17
Risoluzione dei problemi di Windows 45
AWS client fornito 45
Apri VPN GUI 51
Client Open Connect VPN 51
Risoluzione dei problemi di macOS 53
AWS client fornito 53
Tunnelblick 56
Apri VPN 59
Risoluzione dei problemi di Linux 60
AWS client fornito 45
Apri (riga di comando) VPN 61
Apri VPN tramite Network Manager () GUI 63
Problemi comuni 63
TLSnegoziazione chiave non riuscita 63
Cronologia dei documenti 65
..... lxxi

Che cos'è AWS ClientVPN?

AWS Client VPN è un VPN servizio gestito basato su client che consente di accedere in modo sicuro alle AWS risorse e alle risorse della rete locale.

Questa guida fornisce i passaggi per stabilire una VPN connessione a un VPN endpoint Client utilizzando un'applicazione client sul dispositivo.

Componenti del client VPN

Di seguito sono riportati i componenti chiave per l'utilizzo di AWS ClientVPN.

- VPNEndpoint client: VPN l'amministratore del client crea e configura un VPN endpoint client in. AWS L'amministratore controlla a quali reti e risorse puoi accedere quando stabilisci una connessione. VPN
- VPNapplicazione client: l'applicazione software utilizzata per connettersi all'VPNendpoint Client e stabilire una VPN connessione sicura.
- File di configurazione dell'VPNendpoint del client: un file di configurazione fornito dall'amministratore del clientVPN. Il file include informazioni sull'VPNendpoint Client e sui certificati necessari per stabilire una VPN connessione. Questo file viene caricato nell'applicazione VPN client scelta.

Risorse aggiuntive per la configurazione del client VPN

Se sei un VPN amministratore client, consulta la Guida dell'AWS Client VPN amministratore per ulteriori informazioni sulla creazione e la configurazione di un endpoint clientVPN.

Inizia con AWS Client VPN

Prima di poter stabilire una VPN sessione, VPN l'amministratore del client deve creare e configurare un VPN endpoint client. L'amministratore controlla a quali reti e risorse puoi accedere quando stabilisci una VPN sessione. Si utilizza quindi un'applicazione VPN client per connettersi a un VPN endpoint Client e stabilire una VPN connessione sicura.

Se sei un amministratore che deve creare un VPN endpoint Client, consulta la AWS Client VPN Guida per l'amministratore.

Argomenti

- Prerequisiti per l'utilizzo di Client VPN
- Passaggio 1: procurarsi un'applicazione client VPN
- Fase 2: Ottenete il file di configurazione dell'VPNendpoint del client
- Fase 3: Connect a VPN
- Scarica il file AWS Client VPN dal portale self-service

Prerequisiti per l'utilizzo di Client VPN

Per stabilire una VPN connessione, è necessario disporre di quanto segue:

- Accesso a Internet
- Un dispositivo supportato
- Per gli VPN endpoint Client che utilizzano l'autenticazione federata SAML basata (Single Sign-on), uno dei seguenti browser:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Passaggio 1: procurarsi un'applicazione client VPN

È possibile connettersi a un VPN endpoint Client e stabilire una VPN connessione utilizzando il client AWS fornito o un'altra applicazione client VPN basata su Open.

Il client AWS fornito è supportato su Windows, macOS, Ubuntu 18.04 e Ubuntu 20.04LTS. LTS

È possibile scaricare l'VPNapplicazione Client tramite uno dei due metodi seguenti, a seconda che l'amministratore abbia creato il file di configurazione dell'endpoint per l'applicazione:

- Se l'amministratore non ha configurato il file di configurazione dell'endpoint, scaricate e installate il AWS client VPN da Client download. Dopo aver scaricato e installato l'applicazione, procedi the section called “Fase 2: Ottenete il file di configurazione dell'VPNendpoint del client” a richiedere il file di configurazione dell'endpoint all'amministratore.
- Se l'amministratore ha già preconfigurato il file di configurazione dell'endpoint, è possibile scaricare l'VPNapplicazione Client, insieme al file di configurazione, dal portale self-service. Per i passaggi per scaricare il client e il file di configurazione dal portale self-service, consulta. the section called “Scarica Client VPN” Dopo aver scaricato e installato l'applicazione e il file, vai athe section called “Fase 3: Connect a VPN”.

In alternativa, scaricate e installate un'applicazione Open VPN client sul dispositivo dal quale intendete stabilire la VPN connessione.

Fase 2: Ottenete il file di configurazione dell'VPNendpoint del client

Il file di configurazione dell'VPNendpoint del client viene fornito dall'amministratore. Il file di configurazione include le informazioni sull'VPNendpoint Client e i certificati necessari per stabilire una VPN connessione.

In alternativa, se VPN l'amministratore del client ha configurato un portale self-service per l'VPNendpoint Client, è possibile scaricare autonomamente l'ultima versione del client AWS fornito e la versione più recente del file di configurazione dell'VPNendpoint Client. Per ulteriori informazioni, consulta Scarica il file AWS Client VPN dal portale self-service.

Fase 3: Connect a VPN

Importa il file di configurazione dell'VPNendpoint Client nel client AWS fornito o nell'applicazione Open VPN client e connettiti a. VPN Per i passaggi per connettersi a un fileVPN, inclusa l'importazione del file di configurazione dell'endpoint, consulta i seguenti argomenti:

- Connect a un VPN endpoint Client utilizzando un client AWS fornito
- Connect a un VPN endpoint Client utilizzando un Open VPN client

Per gli VPN endpoint client che utilizzano l'autenticazione Active Directory, ti verrà richiesto di inserire il nome utente e la password. Se l'autenticazione a più fattori (MFA) è stata abilitata per la directory, ti verrà anche richiesto di inserire il codice. MFA

Per gli VPN endpoint Client che utilizzano l'autenticazione federata SAML basata (Single Sign-on), il client AWS fornito apre una finestra del browser sul computer. Ti verrà richiesto di inserire le credenziali aziendali prima di poterti connettere all'endpoint Client. VPN

Scarica il file AWS Client VPN dal portale self-service

Il portale self-service è una pagina Web che consente di scaricare la versione più recente del client AWS fornito e l'ultima versione del file di configurazione dell'VPNendpoint Client. Se l'amministratore dell'VPNendpoint Client ha preconfigurato il file di configurazione per il VPN client Client, è possibile scaricare e installare VPN l'applicazione Client insieme al file di configurazione da questo portale.

> **Note**
>
> Se sei un amministratore e desideri configurare il portale self-service, consulta Client VPN endpoints nella Guida per l'amministratore.AWS Client VPN

Prima di iniziare, devi disporre dell'ID dell'endpoint ClientVPN. L'amministratore dell'VPNendpoint Client può fornirti l'ID o fornirti un portale self-service URL che includa l'ID.

Per accedere al portale self-service

1. Vai al portale self-service all'indirizzo https://self-service.clientvpn.amazonaws.com/ o utilizza URL quello che ti è stato fornito dal tuo amministratore.
2. Se necessario, inserisci l'ID dell'VPNendpoint Client, ad esempio. `cvpn-endpoint-0123456abcd123456` Scegli Next (Successivo).
3. Immetti il nome utente e la password e scegli Sign In (Accedi). Si tratta dello stesso nome utente e password utilizzati per connettersi all'VPNendpoint Client.
4. Nel portale self-service puoi effettuare le seguenti operazioni:
   - Scarica la versione più recente del file di configurazione del client per l'VPNendpoint Client.
   - Scarica l'ultima versione del client AWS fornito per la tua piattaforma.

Connect a un VPN endpoint Client utilizzando un client AWS fornito

È possibile connettersi a un VPN endpoint client utilizzando il client AWS fornito. Il client AWS fornito è supportato su Windows, macOS, Ubuntu 18.04 e Ubuntu 20.04LTS. LTS

Client

- AWS Client VPN per Windows
- AWS Client VPN per macOS
- AWS Client VPN per Linux

Direttive aperte VPN

Il client AWS fornito supporta le seguenti VPN direttive Open:

- 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
- Chiave
- nobind
- persist-key
- persist-tun
- ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- route
- route-ipv6
- server-poll-timeout
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN per Windows

Queste sezioni descrivono come stabilire una VPN connessione utilizzando il client AWS fornito per Windows. È possibile scaricare e installare il client da AWS Client VPN download. Il client AWS fornito non supporta gli aggiornamenti automatici.

Requisiti

Per utilizzare il client AWS fornito per Windows, sono necessari i seguenti requisiti:

- Windows 10 o Windows 11 (sistema operativo a 64 bit, processore x64)
- . NETFramework 4.7.2 o versioni successive

Il client riserva la TCP porta 8096 sul tuo computer. Per gli VPN endpoint Client che utilizzano l'autenticazione federata SAML basata (Single Sign-on), il client riserva la porta 35001. TCP

Prima di iniziare, assicurati che l'VPNamministratore del Client abbia creato un endpoint Client e ti abbia fornito il file di configurazione dell'VPNendpoint Client. VPN

Argomenti

- Connect to Client VPN con un client AWS fornito per Windows
- AWS Client VPN per le note di rilascio di Windows

Connect to Client VPN con un client AWS fornito per Windows

Prima di iniziare, assicurati di leggere i requisiti. Il client AWS fornito viene anche denominato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per Windows

1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per File di VPN configurazione, individuate e selezionate il file di configurazione ricevuto dall'VPNamministratore del client, quindi scegliete Aggiungi profilo.
6. Nella finestra Client AWS VPN , assicurati che il profilo sia selezionato, quindi scegli Connect (Connetti). Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di inserire un nome utente e una password.
7. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).

8. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti. In alternativa, scegliere l'icona client sulla barra delle applicazioni di Windows e selezionare Disconnect (Disconnetti).

AWS Client VPN per le note di rilascio di Windows

La tabella seguente contiene le note di rilascio e i collegamenti per il download delle versioni correnti e precedenti di AWS Client VPN per Windows.

> **Note**
>
> Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere influenzate da problemi di usabilità e/o sicurezza. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Link per il download e SHA256
3.14.0	• Aggiunto il supporto per la bandiera `tap-sleep` OpenVPN. • Aggiornate le SSL librerie Open VPN e Open.	12 agosto 2024	Scarica la versione 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516
3.13.0	Aggiornate le librerie Open VPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.13.0 sha256: c9cc896e8 1a7441184

Versione	Modifiche	Data	Link per il download e SHA256
			0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12.1	È stato risolto il problema che impediva alla versione 3.12.0 del client Windows di stabilire la VPN connessione per alcuni utenti.	18 luglio 2024	Scarica la versione 3.12.1 sha256:5e d34aee6c0 3aa281e62 5acdbed27 2896c6704 6364a9e58 46ca697e0 5dbfec08
3.12.0	• Riconnettiti automaticamente quando gli intervalli della rete locale cambiano. • Rimosso il focus automatico dell'appl icazione quando connesso agli SAML endpoint.	21 maggio 2024	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.11.2	È stato risolto un problema di SAML autenticazione con i browser basati su Chromium a partire dalla versione 123.	11 aprile 2024	Scarica la versione 3.11.2 sha256:8b a258dd15b ea3e861ad ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc
3.11.1	• È stata risolta un'azione di buffer overflow che poteva potenzial mente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. • Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• È stato risolto un problema di connettiv ità causato da Windows. VMs • Risolti i problemi di connettività per alcune LAN configurazioni. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Versione	Modifiche	Data	Link per il download e SHA256
3.10.0	• È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. • È stato risolto un problema di connettività in presenza di adattatori di rete Hyper-V installati sul computer client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.10.0 sha256: d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.9.0 sha256: de9a3800ea2349155540bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
3.8.0	Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.7.0	Sono state ripristinate le modifiche rispetto alla versione 3.6.0.	15 luglio 2023	Non è più supportato
3.6.0	Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.5.0	Miglioramenti e correzioni di bug minori.	3 aprile 2023	Non è più supportato
3.4.0	Sono state ripristinate le modifiche rispetto alla versione 3.3.0.	28 marzo 2023	Non è più supportato
3.3.0	Miglioramenti e correzioni di bug minori.	17 marzo 2023	Non è più supportato
3.2.0	• È stato aggiunto il supporto per il flag aperto «verify-x509-name». VPN • Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni. • È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili.	23 gennaio 2023	Non è più supportato
3.1.0	Posizione di sicurezza migliorata.	23 maggio 2022	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.0.0	• Aggiunto il supporto per Windows 11. • È stata corretta la denominazione dei driver di TAP Windows che influiva sui nomi degli altri driver. • Risolto il problema del messaggio del banner che non veniva visualizz ato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato
1.3.7	• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	8 novembre 2021	Non è più supportato
1.3.6	• Aggiunto il supporto per Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	20 settembre 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.5	Patch per eliminare file di log di Windows di grandi dimensioni.	16 agosto 2021	Non è più supportato
1.3.4	• Aggiunto il supporto per Open VPN flag: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato
1.3.3	• Aggiunto il supporto per Open VPN flags: inactive, pull-filter, route. • Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita. • Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata. • Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app. • Miglioramenti e correzioni di bug minori.	1 luglio 2021	Non è più supportato
1.3.2	• Aggiungi la prevenzione delle IPv6 perdite, quando è configurata. • Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione).	12 maggio 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.1	• Aggiunto il supporto per più certificati client con lo stesso oggetto. I certificati scaduti verranno ignorati. • Risolta la conservazione dei log locali per ridurre l'utilizzo del disco. • Aggiunto il supporto per la direttiva Open 'route-ipv6'. VPN • Miglioramenti e correzioni di bug minori.	5 aprile 2021	Non è più supportato
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato
1.2.7	• Aggiunto il supporto per la direttiva cryptoapicert Open. VPN • Sono state risolte le route obsolete tra le connessioni. • Miglioramenti e correzioni di bug minori.	25 febbraio 2021	Non è più supportato
1.2.6	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato
1.2.5	• È stato aggiunto il supporto per i commenti nella configurazione Open. VPN • È stato aggiunto un messaggio di errore per gli errori di TLS handshake.	8 ottobre 2020	Non è più supportato
1.2.4	Miglioramenti e correzioni di bug minori.	1 settembre 2020	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.2.3	Ripristina le modifiche nella versione 1.2.2.	20 agosto 2020	Non è più supportato
1.2.1	Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato
1.2.0	• È stato aggiunto il supporto per l'autenti cazione federata SAML basata su 2.0. • Il supporto per la piattaforma Windows 7 è obsoleto.	19 maggio 2020	Non è più supportato
1.1.1	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato
1.1.0	• È stato aggiunto il supporto per la funzionalità Open VPN static challenge echo per nascondere o mostrare il testo visualizzato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori.	9 marzo 2020	Non è più supportato
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato

AWS Client VPN per macOS

Queste sezioni descrivono come stabilire una VPN connessione utilizzando il client AWS fornito per macOS. Puoi scaricare e installare il client da AWS Client VPN download. Il client AWS fornito non supporta gli aggiornamenti automatici.

Requisiti

Per utilizzare il client AWS fornito per macOS, è necessario quanto segue:

- macOS Monterey (12.0), Ventura (13.0) o Sonoma (14.0).

- Compatibile con il processore x86_64.
- Il client riserva la porta 8096 sul tuo computer. TCP
- Per gli VPN endpoint Client che utilizzano l'autenticazione federata SAML basata (Single Sign-on), il client riserva la porta 35001. TCP

> **Note**
>
> Se utilizzi un Mac con un processore Apple al silicio, devi installare Rosetta 2 per eseguire il software client. Per ulteriori dettagli, consulta Informazioni sull'ambiente di traduzione Rosetta sul sito Web di Apple.

Argomenti

- Connect to Client VPN con un client AWS fornito per macOS
- AWS Client VPN per macOS: note di rilascio

Connect to Client VPN con un client AWS fornito per macOS

Prima di iniziare, assicurati che l'VPNamministratore del client abbia creato un VPN endpoint Client e ti abbia fornito il file di configurazione dell'VPNendpoint Client.

Assicurati, inoltre, di leggere i requisiti. Il client AWS fornito viene anche chiamato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per macOS

1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per File VPN di configurazione, accedi al file di configurazione che hai ricevuto dall'VPNamministratore del tuo client. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).

7. Nella finestra Client AWS VPN assicurati che il tuo profilo sia selezionato, quindi scegli Connetti. Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di inserire un nome utente e una password.
8. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).
9. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti. In alternativa, scegli l'icona del client nella barra dei menu, quindi scegli Disconnetti < >. your-profile-name

AWS Client VPN per macOS: note di rilascio

La tabella seguente contiene le note di rilascio e i link per il download AWS Client VPN per la versione corrente e precedente di macOS.

> **Note**
>
> Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere influenzate da problemi di usabilità e/o sicurezza. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Collegamento per il download
3.12.0	• È stato aggiunto il supporto per il VPN flag `tap-sleep` Open. • Aggiornate le SSL librerie Open VPN e Open.	12 agosto 2024	Scarica la versione 3.12.0 sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13

Versione	Modifiche	Data	Collegamento per il download
3.11.0	• Aggiornate le librerie Open e Open. VPN SSL	29 luglio 2024	Scarica la versione 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f
3.10.0	• Riconnettiti automaticamente quando cambiano gli intervalli della rete locale. • Risolto un problema di DNS ripristino durante lo switch di rete. • È stato rimosso il focus automatico dell'applicazione quando si è connessi agli SAML endpoint.	21 maggio 2024	Scarica la versione 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3.9.2	• Risolto un problema di SAML autenticazione con i browser basati su Chromium a partire dalla versione 123. • È stato aggiunto il supporto per macOS Sonoma. Supporto obsoleto per macOS Big Sur. • Posizione di sicurezza migliorata.	11 aprile 2024	Scarica la versione 3.9.2 sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480

Versione	Modifiche	Data	Collegamento per il download
3.9.1	• È stata risolta un'azione di buffer overflow che poteva potenzial mente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. • Barra di avanzamento del download dell'aggiornamento dell'applicazione fissa. • Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.9.1 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e899e971
3.9.0	• Problemi di connettività risolti per alcune configurazioni. LAN • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8
3.8.0	• È stato risolto un problema di connettiv ità quando NAT64 è abilitato nella rete client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.8.0 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461

Versione	Modifiche	Data	Collegamento per il download
3.7.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.7.0 sha256: 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a
3.6.0	• Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.5.0	• Sono state ripristinate le modifiche rispetto alla versione 3.4.0.	15 luglio 2023	Non è più supportato
3.4.0	• Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato
3.3.0	• Aggiunto il supporto per macOS Ventura (13.0). • Miglioramenti e correzioni di bug minori.	27 aprile 2023	Non è più supportato
3.2.0	• È stato aggiunto il supporto per il flag aperto «verify-x509-name». VPN • Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni. • È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili.	23 gennaio 2023	Non è più supportato

Versione	Modifiche	Data	Collegamento per il download
3.1.0	• È stato aggiunto il supporto per macOS Monterey. • È stato risolto il problema di rilevamento del tipo di unità. • È stata migliorata la posizione di sicurezza.	23 maggio 2022	Non è più supportato
3.0.0	• Risolto il problema del messaggio banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato.
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato.
1.4.0	• Aggiunto il monitoraggio del server durante la connessione. DNS Le impostazioni verranno riconfigurate se non corrispondono VPN alle impostazioni. • In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	9 novembre 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.5	• Aggiunto il supporto per Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	20 settembre 2021	Non è più supportato.
1.3.4	• Aggiunto il supporto per Open VPN flag: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.
1.3.3	• Aggiunto il supporto per Open VPN flags: inactive, pull-filter, route. • Risolto un problema legato ai nomi dei file di configurazione con spazi o Unicode. • Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita. • Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata. • Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app. • Miglioramenti e correzioni di bug minori.	1 luglio 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.2	• Aggiungi la prevenzione delle IPv6 perdite, quando è configurata. • Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione). • Aggiungere la rotazione dei log del daemon.	12 maggio 2021	Non è più supportato.
1.3.1	• Aggiunto il supporto per macOS Big Sur (10.16). • È stato risolto il problema che causava la rimozione DNS delle impostazioni configurate da altre applicazioni. • Risolto un problema che si presentav a durante l'utilizzo di un certificato non valido per l'autenticazione reciproca che causava problemi di connessione. • Aggiunto il supporto per la direttiva Open 'route-ipv6'. VPN • Miglioramenti e correzioni di bug minori.	5 aprile 2021	Non è più supportato.
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato.
1.2.5	Miglioramenti e correzioni di bug minori.	25 febbraio 2021	Non è più supportato.
1.2.4	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.2.3	• È stato aggiunto il supporto per i commenti nella configurazione Open. VPN • È stato aggiunto un messaggio di errore per gli errori di TLS handshake. • Risolto un bug di disinstallazione che interessava alcuni utenti.	8 ottobre 2020	Non è più supportato.
1.2.2	Miglioramenti e correzioni di bug minori.	12 agosto 2020	Non è più supportato.
1.2.1	• Aggiunto il supporto per la disinstal lazione dell'applicazione. • Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato.
1.2.0	• È stato aggiunto il supporto per l'autenti cazione federata SAML basata su 2.0. • Aggiunto il supporto per macOS Catalina (10.15).	19 maggio 2020	Non è più supportato.
1.1.2	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato.
1.1.1	• Risolto il problema che non si DNS risolveva. • Corretto un problema di arresto anomalo dell'app causato da connessio ni più lunghe. • Risolto un MFA problema.	2 aprile 2020	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.1.0	• È stato aggiunto il supporto per la configurazione macOSDNS. • È stato aggiunto il supporto per la funzionalità Open VPN static challenge echo per nascondere o mostrare il testo visualizzato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori.	9 marzo 2020	Non è più supportato.
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato.

AWS Client VPN per Linux

Queste sezioni descrivono l'installazione del client AWS fornito per Linux e quindi la creazione di una VPN connessione utilizzando il client AWS fornito. Il client AWS fornito per Linux non supporta gli aggiornamenti automatici. Per gli aggiornamenti e i download più recenti, consulta ilthe section called "Note di rilascio".

Requisiti per la connessione al client VPN con un client AWS fornito per Linux

Per utilizzare il client AWS fornito per Linux, è necessario quanto segue:

- Ubuntu 18.04 LTS o Ubuntu 20.04 LTS (solo) AMD64

Il client riserva la TCP porta 8096 sul tuo computer. Per gli VPN endpoint Client che utilizzano l'autenticazione federata SAML basata (Single Sign-on), il client riserva la porta 35001. TCP

Prima di iniziare, assicurati che l'VPNamministratore del client abbia creato un endpoint Client e ti abbia fornito il file di configurazione dell'VPNendpoint client. VPN

Argomenti

- Installa il client AWS fornito per Linux

- Connect al client AWS fornito per Linux
- AWS Client VPN note di rilascio per Linux

Installa il client AWS fornito per Linux

Esistono diversi metodi che possono essere utilizzati per installare il client AWS fornito per Linux. Utilizza uno dei metodi forniti dalle seguenti opzioni. Prima di iniziare, assicurati di leggere i requisiti.

Opzione 1: installazione tramite repository di pacchetti

1. Aggiungi la chiave pubblica AWS VPN del client al tuo sistema operativo 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. Usa il comando applicabile per aggiungere il repository al tuo sistema operativo Ubuntu, a seconda della versione di 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. Utilizza il comando riportato di seguito per aggiornare i repository del sistema.

```
sudo apt-get update
```

4. Usa il seguente comando per installare il client AWS fornito per Linux.

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

Opzione 2: Installazione utilizzando il file del pacchetto.deb

1. Scaricate il file.deb da AWS Client VPN download o utilizzando il seguente comando.

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

2. Installa il client AWS fornito per Linux utilizzando l'dpkgutilità.

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

Opzione 3: installazione del pacchetto .deb tramite Ubuntu Software Center

1. Scaricate il file del pacchetto.deb da AWS Client VPN download.
2. Dopo aver scaricato il file del pacchetto .deb, utilizza Ubuntu Software Center per installare il pacchetto. Segui i passaggi per l'installazione da un pacchetto .deb autonomo utilizzando Ubuntu Software Center riportati nel Wiki Ubuntu.

Connect al client AWS fornito per Linux

Il client AWS fornito viene anche chiamato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per Linux

1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per File VPN di configurazione, accedi al file di configurazione che hai ricevuto dall'VPNamministratore del tuo client. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).
7. Nella finestra Client AWS VPN , assicurati che il profilo sia selezionato, quindi scegli Connect (Connetti). Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di inserire un nome utente e una password.
8. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).

9. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti.

AWS Client VPN note di rilascio per Linux

La tabella seguente contiene le note di rilascio e i collegamenti per il download delle versioni correnti e precedenti di AWS Client VPN for Linux.

> **Note**
>
> Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere influenzate da problemi di usabilità e/o sicurezza. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Collegamento per il download
3.15.0	• Aggiunto il supporto per la bandiera `tap-sleep` OpenVPN. • Aggiornate le SSL librerie Open VPN e Open.	12 agosto 2024	Scarica la versione 3.15.0 sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6d89d012
3.14.0	• Aggiornate le librerie Open VPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79

Versione	Modifiche	Data	Collegamento per il download
			e0c5e0020 d379e44f3 19b5334f60
3.13.0	• Riconnettiti automaticamente quando gli intervalli della rete locale cambiano.	21 maggio 2024	Scarica la versione 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1
3.12.2	• Risolto un problema di SAML autenticazione con i browser basati su Chromium a partire dalla versione 123.	11 aprile 2024	Scarica la versione 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	• È stata risolta un'azione di buffer overflow che poteva potenzial mente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. • Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.12.1 sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0

Versione	Modifiche	Data	Collegamento per il download
3.12.0	• Problemi di connettività risolti per alcune configurazioni. LAN	19 dicembre 2023	Scarica la versione 3.12.0 sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• Rollback per «Problemi di connettività risolti per alcune LAN configurazioni». • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• Risolti i problemi di connettività per alcune LAN configurazioni. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51

Versione	Modifiche	Data	Collegamento per il download
3.9.0	• È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.9.0 sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454
3.8.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.6.0	• Sono state ripristinate le modifiche rispetto alla versione 3.5.0.	15 luglio 2023	Non è più supportato
3.5.0	• Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato
3.4.0	• È stato aggiunto il supporto per il flag aperto «verify-x509-name». VPN	14 febbraio 2023	Non è più supportato

Versione	Modifiche	Data	Collegamento per il download
3.1.0	• Risolto il problema di rilevamento del tipo di unità. • È stata migliorata la posizione di sicurezza.	23 maggio 2022	Non è più supportato
3.0.0	• Risolto il problema del messaggio del banner che non veniva visualizz ato quando si utilizza l'autenticazione federata. • Corretta la visualizzazione del testo del banner per testo più lungo e sequenze di caratteri specifiche. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato.
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato.
1.0.3	• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	8 novembre 2021	Non è più supportato.
1.0.2	• Aggiunto il supporto per Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	28 settembre 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.0.1	• Abilitata l'opzione per uscire dalla barra dell'applicazione Ubuntu. • Aggiunto il supporto per Open flags: inactive, pull-filter, route. VPN • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.
1.0.0	Versione iniziale.	11 giugno 2021	Non è più supportato.

Connect a un VPN endpoint Client utilizzando un Open VPN client

È possibile connettersi a un VPN endpoint Client utilizzando le comuni applicazioni Open VPN client.

> **Important**
>
> Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione federata SAML basata, non è possibile utilizzare il VPN client VPN basato su Open per connettersi a un endpoint Client. VPN

Applicazioni client

- Connect a un VPN endpoint Client utilizzando un'applicazione client Windows
- Connect a un VPN endpoint Client utilizzando un'applicazione VPN client Android o iOS
- Connect a un VPN endpoint Client utilizzando un'applicazione client macOS
- Connect a un VPN endpoint Client utilizzando un'applicazione Open VPN client

Connect a un VPN endpoint Client utilizzando un'applicazione client Windows

Queste sezioni descrivono come stabilire una VPN connessione utilizzando client basati su WindowsVPN.

Prima di iniziare, assicurati che l'VPNamministratore del client abbia creato un VPN endpoint client e ti abbia fornito il file di configurazione dell'VPNendpoint client.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di VPN connessione dei client con client basati su Windows.

> **Important**
>
> Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione federata SAML basata, non è possibile utilizzare il client Open VPN based per connettersi a un endpoint VPN Client. VPN

Attività

- Usa un certificato di Windows Certificate System Store con Open VPN
- Usare Open VPN GUI
- Usa il client Open VPN Connect

Usa un certificato di Windows Certificate System Store con Open VPN

È possibile configurare il VPN client Open per utilizzare un certificato e una chiave privata dal Windows Certificate System Store. Questa opzione è utile quando si utilizza una smart card come parte della VPN connessione Client. Per informazioni sull'opzione Open VPN client cryptoapicert, consulta il Manuale di riferimento per il sito web Open VPN on the Open. VPN

> **Note**
>
> Il certificato deve essere memorizzato nel computer locale.

Per utilizzare l'opzione cryptoapicert con Open VPN

1. Crea un file con estensione .pfx contenente il certificato client e la chiave privata.
2. Importa il file con estensione .pfx nell'archivio personale dei certificati, sul computer locale. Per ulteriori informazioni, vedere Procedura: Visualizzazione dei certificati con lo MMC snap-in sul sito Web di Microsoft.
3. Verifica che l'account disponga delle autorizzazioni per leggere il certificato sul computer locale. È possibile utilizzare la console di gestione di Microsoft per modificare le autorizzazioni. Per ulteriori informazioni, consulta Diritti per visualizzare l'archivio dei certificati sul computer locale sul sito Web di Microsoft Technet.
4. Aggiorna il file di VPN configurazione Open e specifica il certificato utilizzando l'oggetto del certificato o l'impronta personale del certificato.

   Di seguito è riportato un esempio di specifica del certificato utilizzando un oggetto.

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

   Di seguito è riportato un esempio di specifica del certificato utilizzando un'identificazione personale. È possibile trovare l'identificazione personale utilizzando la console di gestione di

Microsoft. Per ulteriori informazioni, consulta Come recuperare l'identificazione personale di un certificato sul sito Web di Microsoft Technet.

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

Dopo aver completato la configurazione, si utilizza Open VPN per stabilire una connessione.

Usare Open VPN GUI

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'applicazione Open VPN GUI client su un computer Windows.

> **Note**
>
> Per informazioni sull'applicazione Open VPN client, consultate Community Downloads sul VPN sito Web Open.

Per stabilire una VPN connessione

1. Avviare l'applicazione Open VPN client.
2. Nella barra delle applicazioni di Windows, scegli Mostra/nascondi icone. Fate clic con il pulsante destro del mouse su Apri VPN GUI, quindi scegliete Importa file.
3. Nella finestra di dialogo Apri, selezionate il file di configurazione ricevuto dall'VPNamministratore del client e scegliete Apri.
4. Nella barra delle applicazioni di Windows, scegli Mostra/nascondi icone. Fate clic con il pulsante destro del mouse su Apri VPN GUI, quindi scegliete Connect.

Usa il client Open VPN Connect

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'applicazione Open VPN Connect Client su un computer Windows.

> **Note**
>
> Per ulteriori informazioni, vedere Connessione ad Access Server con Windows sul VPN sito Web Open.

Per stabilire una VPN connessione

1. Avviare l'applicazione Open VPN Connect Client.
2. Nella barra delle applicazioni di Windows, scegli Mostra/nascondi icone. Fate clic con il pulsante destro del mouse su Apri VPN, quindi scegliete Importa profilo.
3. Scegliete Importa da file e selezionate il file di configurazione ricevuto dall'VPNamministratore del client.
4. Scegli il profilo di connessione per avviare la connessione.

Connect a un VPN endpoint Client utilizzando un'applicazione VPN client Android o iOS

> **Important**
>
> Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione federata SAML basata, non è possibile utilizzare il VPN client VPN basato su Open per connettersi a un endpoint Client. VPN

Le seguenti informazioni mostrano come stabilire una VPN connessione utilizzando l'applicazione Open VPN client su un dispositivo mobile Android o iOS. I passaggi per Android e iOS sono uguali.

> **Note**
>
> Per ulteriori informazioni sul download e sull'utilizzo dell'applicazione Open VPN client per iOS o Android, consultate la Open VPN Connect User Guide sul VPN sito Web Open.

Prima di iniziare, assicuratevi che VPN l'amministratore del Client abbia creato un VPN endpoint Client e vi abbia fornito il file di configurazione dell'VPNendpoint Client.

Per stabilire la connessione, avvia l'applicazione Open VPN client, quindi importa il file che hai ricevuto dall'amministratore del clientVPN.

Connect a un VPN endpoint Client utilizzando un'applicazione client macOS

Queste sezioni descrivono come stabilire una VPN connessione utilizzando client basati su macOSVPN.

Prima di iniziare, assicurati che l'VPNamministratore del client abbia creato un VPN endpoint client e ti abbia fornito il file di configurazione dell'VPNendpoint client.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di VPN connessione dei client con i client macOS.

> **Important**
>
> Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione federata SAML basata, non è possibile utilizzare il client Open VPN based per connettersi a un endpoint VPN Client. VPN

Argomenti

- Avvia Tunnelblick per stabilire una connessione AWS Client VPN
- Connettiti a un AWS Client VPN endpoint utilizzando il client Open VPN Connect

Avvia Tunnelblick per stabilire una connessione AWS Client VPN

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'applicazione client Tunnelblick su un computer macOS.

> **Note**
>
> Per ulteriori informazioni sull'applicazione client Tunnelblick per macOS, consulta la documentazione di Tunnelblick sul sito Web Tunnelblick.

Per stabilire una connessione VPN

1. Avviare l'applicazione client Tunnelblick e scegliere I have configuration files (Ho i file di configurazione).
2. Trascina e rilascia il file di configurazione ricevuto dall'VPNamministratore nel pannello Configurazioni.
3. Selezionare il file di configurazione nel riquadro Configurazioni e scegliere Connetti.

Connettiti a un AWS Client VPN endpoint utilizzando il client Open VPN Connect

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'applicazione Open VPN Connect Client su un computer macOS.

> **Note**
>
> Per ulteriori informazioni, vedi Connessione ad Access Server con macOS sul sito Web OpenVPN.

Per stabilire una connessione VPN

1. Avvia l'VPNapplicazione Apri e scegli Importa, Da file locale... .
2. Accedere al file di configurazione ricevuto dall'VPNamministratore e scegliere Apri.

Connect a un VPN endpoint Client utilizzando un'applicazione Open VPN client

Queste sezioni descrivono come stabilire una VPN connessione utilizzando VPN client VPN basati su Open.

Prima di iniziare, assicurati che l'VPNamministratore del Client abbia creato un VPN endpoint Client e ti abbia fornito il file di configurazione dell'VPNendpoint Client.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di VPN connessione dei client con client basati su Linux.

> **Important**
>
> Se l'VPNendpoint Client è stato configurato per utilizzare l'autenticazione federata SAML basata, non è possibile utilizzare il client Open VPN based per connettersi a un endpoint VPN Client. VPN

Argomenti

- Crea una connessione all' AWS Client VPN utilizzo di Open VPN - Network Manager
- Crea una connessione all'utilizzo di Open AWS Client VPN VPN

Crea una connessione all' AWS Client VPN utilizzo di Open VPN - Network Manager

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'VPNapplicazione Open tramite Network Manager GUI su un computer Ubuntu.

Per stabilire una VPN connessione

1. Installare il modulo Network Manager utilizzando il seguente comando.

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

2. Passare a Settings (Impostazioni), Network (Rete).
3. Scegli il simbolo più (+) accanto a VPN, quindi scegli Importa da file... .
4. Vai al file di configurazione che hai ricevuto dal tuo VPN amministratore e scegli Apri.
5. Nella VPN finestra Aggiungi, scegli Aggiungi.
6. Avvia la connessione attivando l'interruttore accanto al VPN profilo che hai aggiunto.

Crea una connessione all'utilizzo di Open AWS Client VPN VPN

La procedura seguente mostra come stabilire una VPN connessione utilizzando l'VPNapplicazione Open su un computer Ubuntu.

Per stabilire una VPN connessione

1. Installa Open VPN usando il seguente comando.

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

2. Avvia la connessione caricando il file di configurazione ricevuto dall'VPNamministratore.

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

Risoluzione dei problemi di VPN connessione con il client

Utilizza i seguenti argomenti per risolvere i problemi che potresti riscontrare quando utilizzi un'applicazione client per connetterti a un endpoint Client. VPN

Argomenti

- Risoluzione dei problemi relativi agli VPN endpoint del client per gli amministratori
- Invia i log di diagnostica AWS Support al client fornito AWS
- Risoluzione dei problemi di VPN connessione dei client con client basati su Windows
- Risoluzione dei problemi di VPN connessione dei client con i client macOS
- Risoluzione dei problemi di VPN connessione dei client con client basati su Linux
- Risoluzione dei problemi più comuni relativi al client VPN

Risoluzione dei problemi relativi agli VPN endpoint del client per gli amministratori

Alcune delle fasi in questa guida possono essere eseguite dall'utente. Gli altri passaggi devono essere eseguiti dall'VPNamministratore del client sull'VPNendpoint Client stesso. Nelle sezioni seguenti viene descritto quando è necessario contattare l'amministratore.

Per ulteriori informazioni sulla risoluzione dei problemi relativi agli VPN endpoint del client, vedere Troubleshooting Client VPN nella Guida per l'AWS Client VPN amministratore.

Invia i log di diagnostica AWS Support al client fornito AWS

Se hai problemi con il client AWS fornito e hai bisogno di contattarci per aiutarti AWS Support a risolverli, il client AWS fornito ha la possibilità di inviare i log di diagnostica a. AWS Support L'opzione è disponibile per le applicazioni client Windows, macOS e Linux.

Prima di inviare i file, devi accettare di consentire l'accesso AWS Support ai registri di diagnostica. Dopo aver accettato, ti forniremo un numero di riferimento a cui puoi fornire AWS Support in modo che possano accedere immediatamente ai file.

Invio dei log di diagnostica

Il cliente AWS fornito viene anche chiamato AWS VPN Cliente nei passaggi seguenti.

Per inviare registri di diagnostica utilizzando il client AWS fornito per Windows

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), esegui una delle seguenti operazioni:

   - Per copiare il numero di riferimento negli Appunti, scegli Sì, quindi scegli OK.
   - Per tenere traccia manualmente del numero di riferimento, seleziona No.

   Quando si contatta AWS Support, è necessario fornire loro il numero di riferimento.

Per inviare registri di diagnostica utilizzando il client AWS fornito per macOS

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Prendi nota del numero di riferimento dalla finestra di conferma, quindi scegli OK.

   Quando contatti AWS Support, dovrai fornire loro il numero di riferimento.

Per inviare registri diagnostici utilizzando il client AWS fornito per Ubuntu

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Invia log di diagnostica, scegli Sì.
4. Prendi nota del numero di riferimento dalla finestra di conferma. Ti viene data la possibilità di copiare le informazioni negli appunti.

   Quando contattate AWS Support, dovrete fornire loro il numero di riferimento.

Risoluzione dei problemi di VPN connessione dei client con client basati su Windows

Le seguenti sezioni contengono informazioni sui problemi che potrebbero verificarsi quando si utilizzano client basati su Windows per connettersi a un endpoint ClientVPN.

Argomenti

- AWS client fornito
- Apri VPN GUI
- Client Open Connect VPN

AWS client fornito

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

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

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- VPNRegistri aperti: contengono informazioni sui processi apertiVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il servizio Windows per eseguire operazioni root. I log dei servizi Windows vengono archiviati nel seguente percorso nel computer.

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

Argomenti

- Il client non è in grado di connettersi
- Il client non può connettersi con il messaggio di registro «no TAP -Windows adapters»
- Il client è bloccato in uno stato di riconnessione
- VPNil processo di connessione si chiude in modo imprevisto

- Impossibile avviare l'applicazione
- Il client non è in grado di creare un profilo
- Si verifica un arresto anomalo del client su Dell PCs che utilizza Windows 10 o 11
- VPNsi disconnette con un messaggio pop-up

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'VPNendpoint Client.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro VPN processo Open che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controllate se sul computer sono in esecuzione altre VPN applicazioni Open. In caso affermativo, interrompi o chiudi questi processi e prova a connetterti nuovamente all'VPNendpoint Client. Verifica la presenza di errori VPN nei registri aperti e chiedi all'VPNamministratore del client di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Questo CRL è ancora valido. Per ulteriori informazioni, consulta Client Unable to Connect to a Client VPN Endpoint nella Guida per l'AWS Client VPN amministratore.

Il client non può connettersi con il messaggio di registro «no TAP -Windows adapters»

Problema

Il client AWS fornito non può connettersi all'VPNendpoint Client e nei registri dell'applicazione viene visualizzato il seguente messaggio di errore: «Non ci sono adattatori TAP -Windows su questo

sistema. Dovresti essere in grado di creare un adattatore TAP -Windows andando su Start -> Tutti i programmi -> TAP -Windows -> Utilità -> Aggiungi un nuovo adattatore ethernet virtuale -Windows». TAP

Soluzione

È possibile risolvere questo problema eseguendo una o più delle seguenti azioni:

- Riavvia l'adattatore -Windows. TAP
- Reinstallare il driver TAP -Windows.
- Crea un nuovo adattatore TAP -Windows.

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'VPNendpoint Client, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il DNS nome host non si risolve in un indirizzo IP.
- Un VPN processo aperto sta tentando a tempo indeterminato di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedete all'VPNamministratore del client di verificare che la `remote` direttiva nel file di configurazione si risolva in un indirizzo IP valido. Puoi anche disconnettere la VPN sessione scegliendo Disconnetti nella finestra AWS VPN Client e riprova a connetterti.

VPNil processo di connessione si chiude in modo imprevisto

Problema

Durante la connessione a un VPN endpoint del client, il client si chiude in modo imprevisto.

Causa

TAP-Windows non è installato sul computer. Questo software è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Impossibile avviare l'applicazione

Problema

In Windows 7, il client AWS fornito non si avvia quando si tenta di aprirlo.

Causa

. NETII framework 4.7.2 o versioni successive non è installato sul computer. Questo è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

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

Causa

Se l'VPNendpoint Client utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave del client.

Soluzione

Assicurati che l'VPNamministratore del client aggiunga il certificato e la chiave del client al file di configurazione. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .

Si verifica un arresto anomalo del client su Dell PCs che utilizza Windows 10 o 11

Problema

Su alcuni dispositivi Dell PCs (desktop e laptop) che eseguono Windows 10 o 11, può verificarsi un arresto anomalo durante la navigazione nel file system per importare un file di VPN configurazione. Se si verifica questo problema, nei log del client AWS fornito verranno visualizzati messaggi come i seguenti:

```
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()
```

Causa

Il sistema di backup e ripristino Dell in Windows 10 e 11 potrebbe causare conflitti con il client AWS fornito, in particolare con i tre seguentiDLLs:

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

Soluzione

Per evitare questo problema, assicurati innanzitutto che il tuo client sia aggiornato con l'ultima versione del client AWS fornito. Vai a AWS Client VPN download e, se è disponibile una versione più recente, esegui l'aggiornamento alla versione più recente.

Devi inoltre eseguire una delle seguenti operazioni:

- Se utilizzi l'applicazione Dell Backup and Recovery, verifica che sia aggiornata. Un post del forum Dell afferma che questo problema è stato risolto nelle versioni più recenti dell'applicazione.
- Se non utilizzi l'applicazione Dell Backup and Recovery, è comunque necessario intraprendere alcune operazioni se si verifica questo problema. Se non desideri aggiornare l'applicazione, in alternativa, puoi eliminare o rinominare i DLL file. Tuttavia, ricorda che ciò impedirà il funzionamento completo dell'applicazione Dell Backup and Recovery.

Eliminare o rinominare i file DLL

1. Accedi a Esplora risorse e individua la posizione in cui è installato Dell Backup and Recovery. In genere è installato nella posizione seguente, ma potrebbe essere necessario cercare per trovarlo.

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

2. Eliminare manualmente i seguenti DLL file dalla directory di installazione o rinominarli. Eseguendo entrambe queste operazioni si evita il caricamento.

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

   È possibile rinominare i file aggiungendo «.bak» alla fine del nome del file, ad esempio .dll.bak. DBROverlayIconBackuped

VPNsi disconnette con un messaggio pop-up

Problema

VPNSi disconnette con un messaggio pop-up che dice: «La VPN connessione viene interrotta perché lo spazio degli indirizzi della rete locale a cui è connesso il dispositivo è cambiato. Stabilisci una nuova VPN connessione».

Causa

TAP-L'adattatore Windows non contiene la descrizione richiesta.

Soluzione

Se il `Description` campo non corrisponde a quello riportato di seguito, rimuovi prima l'adattatore TAP -Windows, quindi esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

```
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
```

Apri VPN GUI

Le seguenti informazioni per la risoluzione dei problemi sono state testate nelle versioni 11.10.0.0 e 11.11.0.0 del VPN GUI software Open su Windows 10 Home (64 bit) e Windows Server 2016 (64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Client Open Connect VPN

Le seguenti informazioni per la risoluzione dei problemi sono state testate nelle versioni 2.6.0.100 e 2.7.1.101 del software Open VPN Connect Client su Windows 10 Home (64 bit) e Windows Server 2016 (64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Impossibile risolvere DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
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.
```

Causa

Il DNS nome non può essere risolto. Il client deve anteporre una stringa casuale al DNS nome per impedire la memorizzazione nella DNS cache; tuttavia, alcuni client non lo fanno.

Soluzione

Consultate la soluzione per Unable to Resolve Client VPN Endpoint DNS Name nella Guida per l'amministratore.AWS Client VPN

Alias mancante PKI

Problema

Una connessione a un VPN endpoint Client che non utilizza l'autenticazione reciproca non riesce con il seguente errore.

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

Causa

Il software Open VPN Connect Client presenta un problema noto a causa del quale tenta di autenticarsi utilizzando l'autenticazione reciproca. Se il file di configurazione non contiene una chiave e un certificato client, l'autenticazione non va a buon fine.

Soluzione

Specificare una chiave client e un certificato casuali nel file di VPN configurazione del client e importare la nuova configurazione nel software Open VPN Connect Client. In alternativa, utilizzate un client diverso, come il client Open (v11.12.0.0) o il VPN GUI client Viscosity (v.1.7.14).

Risoluzione dei problemi di VPN connessione dei client con i client macOS

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo dei client macOS. Verifica di eseguire la versione più recente di questi client.

Argomenti

- AWS client fornito
- Tunnelblick
- Apri VPN

AWS client fornito

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

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

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- VPNRegistri aperti: contengono informazioni sui processi apertiVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il demone client per eseguire operazioni root. I log del daemon vengono archiviati nei seguenti percorsi del computer.

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

Il client AWS fornito memorizza i file di configurazione nella seguente posizione sul computer.

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

Argomenti

- Il client non è in grado di connettersi
- Il client è bloccato in uno stato di riconnessione
- Il client non è in grado di creare un profilo
- Lo strumento di supporto è un errore obbligatorio

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'VPNendpoint Client.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro VPN processo Open che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controllate se sul computer sono in esecuzione altre VPN applicazioni Open. In caso affermativo, interrompi o chiudi questi processi e prova a connetterti nuovamente all'VPNendpoint Client. Verifica la presenza di errori VPN nei registri aperti e chiedi all'VPNamministratore del client di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Questo CRL è ancora valido. Per ulteriori informazioni, consulta Client Unable to Connect to a Client VPN Endpoint nella Guida per l'AWS Client VPN amministratore.

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'VPNendpoint Client, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il DNS nome host non si risolve in un indirizzo IP.
- Un VPN processo aperto sta tentando a tempo indeterminato di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedete all'VPNamministratore del client di verificare che la `remote` direttiva nel file di configurazione si risolva in un indirizzo IP valido. Puoi anche disconnettere la VPN sessione scegliendo Disconnetti nella finestra AWS VPN Client e riprova a connetterti.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

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

Causa

Se l'VPNendpoint Client utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave del client.

Soluzione

Assicurati che l'VPNamministratore del client aggiunga il certificato e la chiave del client al file di configurazione. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .

Lo strumento di supporto è un errore obbligatorio

Problema

Viene visualizzato il seguente errore quando si tenta di connettere ilVPN.

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

Soluzione

Vedi il seguente articolo su AWS Re:POST. AWSVPNClient - Errore richiesto dallo strumento Helper

Tunnelblick

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 3.7.8 (build 5180) del software Tunnelblick su macOS High Sierra 10.13.6.

Il file di configurazione per le configurazioni private viene archiviato nel seguente percorso del computer.

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

Il file di configurazione per le configurazioni condivise viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Per aumentare la verbosità del registro, apri l'applicazione Tunnelblick, scegli Impostazioni e regola il valore per il livello di registro. VPN

Algoritmo di cifratura '-256-' non trovato AES GCM

Problema

La connessione non riesce e restituisce il seguente errore nei log.

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

Causa

L'applicazione utilizza una VPN versione Open che non supporta l'algoritmo di cifratura -256-. AES GCM

Soluzione

Scegliete una VPN versione Open compatibile effettuando le seguenti operazioni:

1. Aprire l'applicazione Tunnelblick.
2. Seleziona Impostazioni.
3. Per la VPNversione aperta, scegli 2.4.6 - La SSL versione aperta è v1.0.2q.

La connessione smette di rispondere e si ripristina

Problema

La connessione non riesce e restituisce il seguente errore nei log.

```
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
```

Causa

Il certificato client è stato revocato. La connessione smette di rispondere dopo aver tentato di autenticarsi e alla fine viene ripristinata dal lato server.

Soluzione

Richiedi un nuovo file di configurazione all'amministratore del client. VPN

Utilizzo esteso delle chiavi (EKU)

Problema

La connessione non riesce e restituisce il seguente errore nei log.

```
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,,,,,
```

Causa

L'autenticazione del server è stata completata. Tuttavia, l'autenticazione del client fallisce perché il certificato client ha il campo extended key usage (EKU) abilitato per l'autenticazione del server.

Soluzione

Verifica di utilizzare il certificato e la chiave client corretti. Se necessario, verificate con l'VPNamministratore del client. Questo errore potrebbe verificarsi se si utilizza il certificato del server e non il certificato client per connettersi all'VPNendpoint Client.

Certificato scaduto

Problema

L'autenticazione del server va a buon fine ma l'autenticazione client non riesce con il seguente errore.

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

Causa

La validità del certificato client è scaduta.

Soluzione

Richiedi un nuovo certificato client all'VPNamministratore del client.

Apri VPN

Le seguenti informazioni per la risoluzione dei problemi sono state testate sulla versione 2.7.1.100 del software Open VPN Connect Client su macOS High Sierra 10.13.6.

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Impossibile risolvere DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
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
```

Causa

Open VPN Connect non è in grado di risolvere il VPN DNS nome del client.

Soluzione

Vedi la soluzione per Unable to Resolve Client VPN Endpoint DNS Name nella Guida per l'AWS Client VPN amministratore.

Risoluzione dei problemi di VPN connessione dei client con client basati su Linux

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo di client basati su Linux. Verifica di eseguire la versione più recente di questi client.

Argomenti

- AWS client fornito
- Apri (riga di comando) VPN
- Apri VPN tramite Network Manager () GUI

AWS client fornito

Il client AWS fornito archivia i file di registro e i file di configurazione nella seguente posizione sul sistema:

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

Il processo daemon client AWS fornito archivia i file di registro nella seguente posizione sul sistema:

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

Problema

In alcune circostanze, dopo aver stabilito una VPN connessione, DNS le query continueranno ad andare al nameserver di sistema predefinito, anziché ai nameserver configurati per l'endpoint Client. VPN

Causa

Il client interagisce con systemd-resolved, un servizio disponibile sui sistemi Linux, che funge da elemento centrale di gestione. DNS Viene utilizzato per configurare i DNS server che vengono inviati dall'endpoint Client. VPN Il problema si verifica perché systemd-resolved non imposta la massima priorità ai DNS server forniti dall'endpoint Client. VPN Invece, aggiunge i server all'elenco esistente di DNS server configurati sul sistema locale. Di conseguenza, i DNS server originali potrebbero continuare ad avere la massima priorità e quindi essere utilizzati per risolvere le DNS interrogazioni.

Soluzione

1. Aggiungi la seguente direttiva nella prima riga del file di VPN configurazione Open, per assicurarti che tutte le DNS query vengano inviate al tunnel. VPN

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

2. Utilizza il resolver stub fornito da systemd-resolved. Per far ciò, collegare simbolicamente `/etc/resolv.conf` a `/run/systemd/resolve/stub-resolv.conf` emettendo il seguente comando sul sistema.

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

3. (Facoltativo) Se non volete che systemd risolva le interrogazioni tramite proxy e desiderate invece che DNS le query vengano inviate direttamente ai DNS nameserver reali, utilizzate invece un collegamento simbolico a. `/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

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

   Potresti voler eseguire questa procedura per aggirare la configurazione risolta da systemd, ad esempio per la memorizzazione nella cache delle DNS risposte, la configurazione per interfaccia, l'applicazione e così via. DNS DNSSec Questa opzione è particolarmente utile quando è necessario sostituire un DNS record pubblico con un record privato quando si è connessi a. VPN Ad esempio, potresti avere un DNS resolver privato in privato VPC con un record per www.example.com, che si risolve in un IP privato. Questa opzione può essere utilizzata per sovrascrivere il record pubblico di www.example.com, che si risolve in un IP pubblico.

Apri (riga di comando) VPN

Problema

La connessione non funziona correttamente perché DNS la risoluzione non funziona.

Causa

Il DNS server non è configurato sull'VPNendpoint Client o non viene rispettato dal software client.

Soluzione

Utilizza i seguenti passaggi per verificare che il DNS server sia configurato e funzioni correttamente.

1. Assicuratevi che nei log sia presente una voce del DNS server. Nell'esempio seguente, il DNS server `192.168.0.2` (configurato nell'VPNendpoint Client) viene restituito nell'ultima riga.

```
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
```

   Se non è stato specificato alcun DNS server, chiedi all'VPNamministratore del client di modificare l'VPNendpoint Client e assicurati che sia stato specificato un DNS server (ad esempio, il VPC DNS server) per l'endpoint ClientVPN. Per ulteriori informazioni, consulta Client VPN Endpoints nella Guida per l'AWS Client VPN amministratore.

2. Per accertarsi che il pacchetto `resolvconf` sia installato, eseguire il comando seguente.

```
sudo apt list resolvconf
```

   Viene restituito l'output seguente.

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

   Se non è installato, installarlo utilizzando il seguente comando.

```
sudo apt install resolvconf
```

3. Apri il file di VPN configurazione del client (il file.ovpn) in un editor di testo e aggiungi le seguenti righe.

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

   Controllare i log per verificare che lo script `resolvconf` sia stato richiamato. I log devono contenere una riga simile alla seguente.

```
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
```

Apri VPN tramite Network Manager () GUI

Problema

Quando si utilizza il VPN client Network Manager Open, la connessione fallisce con il seguente errore.

```
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
```

Causa

Il flag `remote-random-hostname` non è rispettato e il client non può connettersi utilizzando il pacchetto `network-manager-gnome`.

Soluzione

Vedi la soluzione per Unable to Resolve Client VPN Endpoint DNS Name nella Guida per l'AWS Client VPN amministratore.

Risoluzione dei problemi più comuni relativi al client VPN

Di seguito sono riportati i problemi più comuni che si possono verificare quando si utilizza un client per connettersi a un VPN endpoint Client.

TLSnegoziazione chiave non riuscita

Problema

La TLS negoziazione fallisce con il seguente errore.

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

```
TLS Error: TLS handshake failed
```

Causa

La causa del problema può essere una delle seguenti:

- Le regole del firewall bloccano UDP il TCP traffico.
- La chiave e il certificato client utilizzati nel file di configurazione (.ovpn) sono errati.
- L'elenco di revoca dei certificati client (CRL) è scaduto.

Soluzione

Verifica se le regole del firewall sul tuo computer bloccano il traffico in entrata o in uscita o il UDP traffico sulle porte TCP 443 o 1194. Chiedi all'VPNamministratore del tuo client di verificare le seguenti informazioni:

- Che le regole del firewall per l'VPNendpoint Client non blocchino TCP il UDP traffico sulle porte 443 o 1194.
- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Che il sia ancora CRL valido. Per ulteriori informazioni, consulta Client Unable to Connect to a Client VPN Endpoint nella Guida per l'AWS Client VPN amministratore.

Cronologia dei documenti

La tabella seguente descrive gli aggiornamenti della AWS Client VPN User Guide.

Modifica	Descrizione	Data
AWS rilasciato il client fornito (3.15.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.14.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.12.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.14.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.13.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.11.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.12.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	18 luglio 2024
AWS rilasciato il client fornito (3.13.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.12.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.10.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.9.2) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024

AWS rilasciato il client fornito (3.12.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024
AWS rilasciato il client fornito (3.11.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024
AWS rilasciato il client fornito (3.9.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.11.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	19 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.10.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.8.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.10.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023

AWS rilasciato il client fornito (3.9.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.8.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.7.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.8.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.5.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.5.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.3.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	27 aprile 2023

AWS rilasciato il client fornito (3.5.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 aprile 2023
AWS rilasciato il client fornito (3.4.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	28 marzo 2023
AWS rilasciato il client fornito (3.3.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2023
AWS rilasciato il client fornito (3.4.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 febbraio 2023
AWS rilasciato il client fornito (3.2.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.2.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (2.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022

AWS rilasciato il client fornito (2.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (2.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (1.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	9 novembre 2021
AWS rilasciato il client fornito per Windows (1.3.7)	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.3) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	28 settembre 2021
AWS rilasciato il client fornito per Windows (1.3.6) e macOS (1.3.5)	Per informazioni dettagliate, consulta le note di rilascio.	20 settembre 2021
AWS rilasciato il client fornito per Ubuntu 18.04 e Ubuntu 20.04 LTS LTS	È possibile utilizzare il AWS client fornito su Ubuntu 18.04 e Ubuntu 20.04LTS. LTS	11 giugno 2021
Support per Open VPN utilizzando un certificato di Windows Certificate System Store	È possibile utilizzare Open VPN con un certificato disponibile in Windows Certificate System Store.	25 febbraio 2021
Portale self-service	È possibile accedere a un portale self-service per ottenere il client e il file di configurazione più recenti AWS forniti.	29 ottobre 2020

AWS cliente fornito	È possibile utilizzare il client AWS fornito per connettersi a un VPN endpoint Client.	4 febbraio 2020
Versione iniziale	Questa versione introduce Client. AWS VPN	18 dicembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.