Guida per l'utente

AWS Client VPN

AWS Client VPN: Guida per l'utente

Table of Contents

Cos'è AWS Client VPN?

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

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

Componenti Client VPN

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

- Endpoint Client VPN: l'amministratore Client VPN crea e configura un endpoint Client VPN in. AWS L'amministratore controlla le reti e le risorse cui è possibile accedere quando si stabilisce una connessione VPN.
- Applicazione client VPN: l'applicazione software utilizzata per connettersi all'endpoint Client VPN e stabilire una connessione VPN sicura.
- File di configurazione dell'endpoint Client VPN: un file di configurazione fornito dall'amministratore Client VPN. Il file include informazioni sull'endpoint Client VPN e sui certificati necessari per stabilire una connessione VPN. Il file viene caricato nell'applicazione client VPN scelta. Il client AWS fornito consente di connettersi a cinque sessioni simultanee, ciascuna sessione con il proprio file di configurazione fornito dall'amministratore Client VPN. Per ulteriori informazioni sulle sessioni simultanee, vedere. Support per connessioni simultanee

Risorse aggiuntive per la configurazione di Client VPN

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

Inizia con AWS Client VPN

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

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

Argomenti

Prerequisiti per l'utilizzo di Client VPN

Per stabilire una connessione VPN, è necessario quanto segue:

- Accesso a Internet
- Un dispositivo supportato
- Una versione supportata di Windows, macOS o Linux.
- Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), uno dei seguenti browser:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Fase 1: ottenere un'applicazione client VPN

Puoi connetterti a un endpoint Client VPN e stabilire una connessione VPN utilizzando il client fornito da AWS o un'altra applicazione client basata su OpenVPN.

È possibile scaricare l'applicazione Client VPN 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 i file di configurazione degli endpoint, scarica e installa il AWS client da Client VPN download. Dopo aver scaricato e installato l'applicazione, procedi the section called “Fase 2: ottenere il file di configurazione dell'endpoint Client VPN” a richiedere il file di configurazione dell'endpoint all'amministratore. Se ti connetti a più profili, avrai bisogno di un file di configurazione per ogni profilo.
- Se l'amministratore ha già preconfigurato il file di configurazione dell'endpoint, è possibile scaricare l'applicazione Client VPN, 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: Connettersi alla VPN”.

In alternativa, scarica e installa un'applicazione client OpenVPN sul dispositivo da cui vuoi stabilire la connessione VPN.

Fase 2: ottenere il file di configurazione dell'endpoint Client VPN

Ottieni il file di configurazione degli endpoint Client VPN dal tuo amministratore. Il file di configurazione include le informazioni sugli endpoint Client VPN e i certificati richiesti per stabilire una connessione VPN.

In alternativa, se l'amministratore di Client VPN ha configurato un portale self-service per l'endpoint Client VPN, puoi scaricare tu stesso l'ultima versione del client AWS fornito e l'ultima versione del file di configurazione dell'endpoint Client VPN. Per ulteriori informazioni, consulta Scarica il file AWS Client VPN dal portale self-service.

Fase 3: Connettersi alla VPN

Importa il file di configurazione dell'endpoint Client VPN nel client AWS fornito o nell'applicazione client OpenVPN e connettiti alla VPN. Per i passaggi per connettersi a una VPN, inclusa

l'importazione di uno o più file di configurazione degli endpoint per un AWS determinato client, consulta i seguenti argomenti:

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

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

Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client AWS fornito apre una finestra del browser sul computer. Ti verrà richiesto di immettere le credenziali aziendali prima di connetterti 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 le versioni più recenti dei file di configurazione degli endpoint Client VPN. Se l'amministratore dell'endpoint Client VPN ha preconfigurato uno o più file di configurazione per il client Client VPN, è possibile scaricare e installare l'applicazione Client VPN insieme a tali file di configurazione da questo portale.

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

Prima di iniziare, devi disporre dell'ID di ogni endpoint Client VPN che desideri scaricare. L'amministratore dell'endpoint Client VPN può fornirti l'ID o può fornirti un URL del portale self-service che includa l'ID. Per connessioni endpoint multiple avrai bisogno dell'ID endpoint per ogni profilo a cui desideri connetterti.

Per accedere al portale self-service

1. Vai al portale self-service all'indirizzo https://self-service.clientvpn.amazonaws.com/o utilizza l'URL che ti è stato fornito dall'amministratore.

2. Se necessario, immetti l'ID dell'endpoint Client VPN, ad esempi, `cvpn-endpoint-0123456abcd123456`. Scegli Next (Successivo).
3. Immetti il nome utente e la password e scegli Sign In (Accedi). È lo stesso nome utente e la stessa password che hai utilizzato per connetterti all'endpoint Client VPN.
4. Nel portale self-service puoi effettuare le seguenti operazioni:
   - Scaricare la versione più recente del file di configurazione del client per l'endpoint Client VPN. Se desideri connetterti a più endpoint, dovrai scaricare il file di configurazione per ogni endpoint.
   - Scarica l'ultima versione del client AWS fornito per la tua piattaforma.
5. Ripeti questi passaggi per ogni file di configurazione dell'endpoint per cui desideri creare un profilo di connessione.

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

È possibile connettersi a un endpoint Client VPN utilizzando il client AWS fornito, supportato su Windows, macOS e Ubuntu. Il client AWS fornito supporta anche fino a cinque connessioni simultanee e direttive OpenVPN.

Argomenti

Support per connessioni simultanee utilizzando un client AWS fornito

Il client AWS fornito consente di connettersi a più sessioni simultanee. Ciò è utile se hai bisogno di accedere alle risorse in più AWS ambienti e disponi di endpoint diversi per tali risorse. Ad esempio, potresti aver bisogno di accedere a un database in un ambiente su un endpoint diverso dall'endpoint a cui sei attualmente connesso, ma non desideri disconnettere la connessione corrente. Per consentire al client AWS fornito di connettersi alle sessioni correnti, scaricate il file di configurazione creato dall'amministratore per ogni endpoint e quindi create un profilo di connessione per ogni file. Utilizzando il client AWS fornito, è quindi possibile connettersi a più sessioni senza disconnettersi da nessuna sessione attualmente aperta. Questa funzionalità è supportata solo per i client AWS forniti. Per i passaggi per connettersi a sessioni simultanee, consulta quanto segue:

- Connect utilizzando il client AWS fornito per Windows
- Connect utilizzando il client AWS fornito per macOS
- Connect utilizzando il client AWS fornito per Linux

Quando ci si connette a più endpoint, Client VPN implementa controlli per garantire che non vi siano conflitti con altre connessioni endpoint aperte, ad esempio, se due sessioni hanno blocchi CIDR o politiche di routing in conflitto; o se sei già connesso con una connessione tunnel completa. Se il controllo rileva conflitti, non verrà stabilita una connessione finché non si sceglie una connessione

diversa che non sia in conflitto con la connessione aperta o non ci si disconnette dalla sessione aperta che causa il conflitto.

Le connessioni DNS simultanee sono consentite. Verrà applicato il server DNS di una delle connessioni abilitate al DNS. A seconda del server DNS, è possibile che venga richiesta l'autenticazione durante la riconnessione.

> **Note**
>
> Il numero massimo di sessioni simultanee consentite è cinque.

Direttive OpenVPN

Il client AWS fornito supporta le seguenti direttive OpenVPN. Per ulteriori informazioni su queste direttive, consulta la documentazione sul sito Web di OpenVPN.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb

  dhcp-option
- ifconfig-ipv6

- inactive
- keepalive
- Chiave
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- uscita 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
- tocca e dormi
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN per Windows

Queste sezioni descrivono come stabilire una connessione VPN utilizzando il client AWS fornito per Windows. Puoi scaricare e installare il client dalla pagina Download di Client VPN AWS. 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)
- .NET Framework 4.7.2 o superiore

Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client riserva le porte TCP 8096-8115 sul computer.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Argomenti

Connect AWS Client VPN a un client AWS fornito per Windows

Prima di iniziare, assicurati 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 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 VPN Configuration File (File di configurazione VPN), seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Add Profile (Aggiungi profilo).

6. Se desideri creare più connessioni, ripeti la procedura Aggiungi profilo per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
7. Nella finestra AWS VPN Client, scegli il profilo a cui desideri connetterti, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

   > **Note**
   >
   > Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

8. Per visualizzare le statistiche relative a una connessione, scegli Connessione nella finestra del client AWS VPN, scegli Mostra dettagli, quindi scegli la connessione di cui desideri visualizzare i dettagli.
9. Per disconnettere una connessione, scegli una connessione nella finestra del client AWS VPN, quindi scegli Disconnetti. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente. 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 affette da problemi di and/or sicurezza relativi all'usabilità. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Link per il download e SHA256
5.2.2	Posizione di sicurezza migliorata.	2 giugno 2025	Scarica la versione 5.2.2 sha256: f27cb0eed7c9c5354caa5d7e37595eefbb048d7481bf698b2e5fb653b667c190
5.2.1	• È stato aggiunto il supporto per il `ping-exit` flag OpenVPN. • Aggiornata la libreria OpenSSL. • Miglioramenti e correzioni di bug minori.	21 aprile 2025	Non è più supportato.
5.2.0	• Miglioramenti minori. • È stato aggiunto il supporto per Client Route Enforcement.	8 aprile 2025	Non è più supportato.
5.1.0	• È stato risolto un problema che causava la riconnessione automatica della AWS Client VPN versione 5.0.x alla VPN dopo una disconnessione per un timeout di inattività. • Miglioramenti e correzioni di bug minori.	17 marzo 2025	Non è più supportato.
5.0.2	• È stato risolto un problema DNS per le connessioni simultanee. • Risolti alcuni problemi sporadici che si verificavano durante l'installazione di nuovi adattatori TAP.	24 febbraio 2025	Non è più supportato.

Versione	Modifiche	Data	Link per il download e SHA256
5.0.1	È stato risolto un problema che causava sporadici errori di connessione VPN nella versione 5.0.0 del client Windows.	30 gennaio 2025	Non è più supportato.
5.0.0	• È stato aggiunto il supporto per le connessioni simultanee. • Aggiornata la versione del driver TAP. • È stata aggiornata l'interfaccia utente grafica. • Miglioramenti e correzioni di bug minori.	21 gennaio 2025	Non è più supportato.
4.1.0	Miglioramenti e correzioni di bug minori.	12 novembre 2024	Non è più supportato.
4.0.0	Miglioramenti minori.	25 settembre 2024	Scarica la versione 4.0.0 sha256:65 32f911385 ec8fac149 4d0847c8f 90a999b3b d7380844e 2ea4318e9 db4a2ebc

Versione	Modifiche	Data	Link per il download e SHA256
3.14.2	È stato aggiunto il supporto per il `mssfix` flag OpenVPN.	4 settembre 2024	Scarica la versione 3.14.2 sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Miglioramenti e correzioni di bug minori.	22 agosto 2024	Scarica la versione 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14,0	• È stato aggiunto il supporto per il `tap-sleep` flag OpenVPN. • Aggiornate le librerie OpenVPN e OpenSSL.	12 agosto 2024	Scarica la versione 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516

Versione	Modifiche	Data	Link per il download e SHA256
3.13.0	Aggiornate le librerie OpenVPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.13.0 sha256: c9cc896e81a7441184 0951e349eed9384507 c53337fb703c5ec64d 522c29388b
3.12.1	È stato risolto il problema che impediva alla versione 3.12.0 del client Windows di stabilire una connessione VPN per alcuni utenti.	18 luglio 2024	Scarica la versione 3.12.1 sha256:5ed34aee6c0 3aa281e625acdbed27 2896c67046364a9e58 46ca697e05dbfec08
3.12.0	• Riconnettiti automaticamente quando gli intervalli della rete locale cambiano. • È stato rimosso il focus automatico dell'applicazione quando si è connessi agli endpoint SAML.	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 autentica zione SAML 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 • Problemi di connettività risolti per alcune configurazioni LAN. • 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 OpenVPN «verify-x509-name». • 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. • Risolto il problema del nome del driver di Windows TAP che influenzava altri nomi di driver. • Risolto il problema del messaggio del 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
1.3.7	• 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 i flag OpenVPN: 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 il flag OpenVPN: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato
1.3.3	• Aggiunto il supporto per i flag OpenVPN: 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	• IPv6 Aggiungi la prevenzione delle fughe, 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 OpenVPN 'route-ipv6'. • 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 OpenVPN 'cryptoapicert'. • 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	• Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS.	8 ottobre 2020	Non è più supportato
1.2.4	Miglioramenti e correzioni di bug minori.	1 settembre 2020	Non è più supportato
1.2.3	Ripristina le modifiche nella versione 1.2.2.	20 agosto 2020	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.2.1	Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato
1.2.0	• Aggiunto il supporto per l'autenticazione federata basata su SAML 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	• Aggiunto il supporto per la funzionalità OpenVPN 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 connessione VPN utilizzando il client AWS fornito per macOS. Puoi scaricare e installare il client dalla pagina Download di Client VPN AWS. Il client AWS fornito non supporta gli aggiornamenti automatici.

Requisiti

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

- macOS Ventura (13.0), Sonoma (14.0) o Sequoia (15.0).
- Compatibile con il processore x86_64.

- Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client riserva le porte TCP 8096-8115 sul computer.

> **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 AWS Client VPN a un client AWS fornito per macOS

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

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 VPN Configuration File (File di configurazione VPN), seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Add Profile (Aggiungi profilo).
6. Se desideri creare più connessioni, ripeti la procedura Aggiungi profilo per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
7. Nella finestra AWS VPN Client, scegli il profilo a cui desideri connetterti, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali,

ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

> **Note**
>
> Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

8. Per visualizzare le statistiche relative a una connessione, scegli Connessione nella finestra del client AWS VPN, scegli Mostra dettagli, quindi scegli la connessione di cui desideri visualizzare i dettagli.
9. Per disconnettere una connessione, scegli una connessione nella finestra del client AWS VPN, quindi scegli Disconnetti. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente.

AWS Client VPN per le note di rilascio di macOS

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 and/or sicurezza relativi all'usabilità. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Collegamento per il download
5.2.1	• È stato aggiunto il supporto per il flag OpenVPN ping-exit. • Aggiornata la libreria OpenSSL. • Posizione di sicurezza migliorata.	18 giugno 2025	Scarica la versione 5.2.1 sha256:90 6f77fbca3

Versione	Modifiche	Data	Collegamento per il download
	• Miglioramenti e correzioni di bug minori.		334fbdcd1 145dd6f27 25beab82a 30b9b51ea fd1a25c3f e7d669eb
5.2.0	• Miglioramenti minori. • È stato aggiunto il supporto per Client Route Enforcement.	8 aprile 2025	Scarica la versione 5.2.0 sha256: f062e971a 84e98d8a6 1caced3d7 f6be322c2 8dab02ec8 1194c0f9a 3e62bd8249
5.1.0	• È stato risolto un problema che causava la riconnessione automatic a della versione 5.0.x alla VPN dopo una disconnessione per un timeout di inattività. AWS Client VPN • È stato risolto un problema che AWS Client VPN impediva di stabilire una connessione VPN per i file di configura zione con terminazioni di riga in stile Windows. • Miglioramenti e correzioni di bug minori.	17 marzo 2025	Scarica la versione 5.1.0 sha256: ef7ff34ae 85a29f902 12514568c 93849ef6e 67f30b2c8 3ae1494d3 07f7650e10

Versione	Modifiche	Data	Collegamento per il download
5.0.3	Miglioramenti e correzioni di bug minori.	6 marzo 2025	Scarica la versione 5.0.3 sha256:8c e0f91ce81 c322cead3 ed27948dd eda4d5a61 f5ed5a611 5ab8e18f5 d8963f6b
5.0.2	È stato risolto un problema che causava errori sporadici nella scelta di Connect.	17 febbraio 2025	Scarica la versione 5.0.2 sha256: e81287746 08147e65b 14f992a4b 5a6d75364 6424fe3b6 8fab23181 0addac1f7c
5.0.1	È stato risolto un problema che impediva alla versione client 5.0.0 di stabilire una connessione VPN per i nomi di profilo contenenti spazi.	22 gennaio 2025	Scarica la versione 5.0.1 sha256:7d 9de8c8915 4c9a99bfd 56b196600 a9a09eb6a 952cb10a7 b16d01bdb adb0e57a

Versione	Modifiche	Data	Collegamento per il download
5.0.0	• È stato aggiunto il supporto per le connessioni simultanee. • È stata aggiornata l'interfaccia utente grafica. • Miglioramenti e correzioni di bug minori.	21 gennaio 2025	Scarica la versione 5.0.0 sha256:e9c95ecdd6d582e72e1af0b05d03fe678f96b8b1028b5f569f962902943ecf02
4.1.0	Miglioramenti e correzioni di bug minori.	12 novembre 2024	Scarica la versione 4.1.0 sha256:afe1ec8a6d7e2e1d618a6507f44a8c41db744fb55f93e318d75bc5e96cd269
4.0.0	Miglioramenti minori.	25 settembre 2024	Scarica la versione 4.0.0 sha256:ad574475a80b614499c97ae75612ef1ff905bb4aa1b5f7109420e80bf95aefcbd

Versione	Modifiche	Data	Collegamento per il download
3.12.1	È stato aggiunto il supporto per il `mssfix` flag OpenVPN.	4 settembre 2024	Scarica la versione 3.12.1 sha256: a5c31d3e0 e8bf89376 82805c9ff f76ca9205 875e009e9 49ad1b053 2f449cee47
3.12.0	• È stato aggiunto il supporto per il `tap-sleep` flag OpenVPN. • Aggiornate le librerie OpenVPN e OpenSSL.	12 agosto 2024	Scarica la versione 3.12.0 sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13
3.11.0	• Aggiornate le librerie OpenVPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f

Versione	Modifiche	Data	Collegamento per il download
3.10.0	• Riconnettiti automaticamente quando cambiano gli intervalli della rete locale. • Risolto un problema di ripristino DNS durante lo switch di rete. • È stato rimosso il focus automatico dell'applicazione quando si è connessi agli endpoint SAML.	21 maggio 2024	Scarica la versione 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3.9.2	• Risolto un problema di autentica zione SAML 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
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

Versione	Modifiche	Data	Collegamento per il download
3.9.0	• Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• È stato risolto un problema di connettività quando è abilitato nella rete client. NAT64 • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.8.0 sha256: d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.7.0 sha256: 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a

Versione	Modifiche	Data	Collegamento per il download
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 OpenVPN «verify-x509-name». • 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	• È stato aggiunto il supporto per macOS Monterey. • È stato risolto il problema di rilevamen to del tipo di unità. • È stata migliorata la posizione di sicurezza.	23 maggio 2022	Non è più supportato

Versione	Modifiche	Data	Collegamento per il download
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 DNS durante la connessione. Se non corrispondono alle impostazioni della VPN le impostazioni verranno riconfigu rate. • 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.
1.3.5	• Aggiunto il supporto per i flag OpenVPN: 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	Collegamento per il download
1.3.4	• Aggiunto il supporto per il flag OpenVPN: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.
1.3.3	• Aggiunto il supporto per i flag OpenVPN: 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.
1.3.2	• Aggiungi la prevenzione delle perdite, quando è configurata. IPv6 • 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.

Versione	Modifiche	Data	Collegamento per il download
1.3.1	• Aggiunto il supporto per macOS Big Sur (10.16). • Risolto un problema che eliminava le impostazioni DNS 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 OpenVPN 'route-ipv6'. • 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.
1.2.3	• Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS. • 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.

Versione	Modifiche	Data	Collegamento per il download
1.2.1	• Aggiunto il supporto per la disinstallazione dell'applicazione. • Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato.
1.2.0	• Aggiunto il supporto per l'autenticazione federata basata su SAML 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	• Corretto un problema di risoluzione DNS. • Corretto un problema di arresto anomalo dell'app causato da connessioni più lunghe. • Corretto un problema MFA.	2 aprile 2020	Non è più supportato.
1.1.0	• Aggiunto il supporto per la configurazione DNS macOS. • Aggiunto il supporto per la funzionalità OpenVPN 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 connessione VPN 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 a Client VPN con un client AWS fornito per Linux

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

- Ubuntu 22.04 LTS (AMD64) o Ubuntu 24.04 LTS (solo) AMD64

Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client riserva le porte TCP 8096-8115 sul computer.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Argomenti

- Installa il fornito AWS Client VPN per Linux
- Connect al provider AWS Client VPN per Linux
- AWS Client VPN note di rilascio per Linux

Installa il fornito AWS Client VPN 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 del client AWS VPN 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 seguente comando per aggiungere il repository al tuo sistema operativo Ubuntu (versione 22.04 e successive):

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

3. 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. Scarica il file .deb da Download di Client VPN AWS 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'`dpkg`utilità.

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

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

1. Scarica il file del pacchetto .deb da Download di Client VPN AWS.
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 provider AWS Client VPN 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 VPN Configuration File (File di configurazione VPN) seleziona il file di configurazione ricevuto dall'amministratore Client VPN. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).
7. Se desideri creare più connessioni, ripeti i passaggi Aggiungi profilo per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
8. Nella finestra AWS VPN Client, scegli il profilo a cui desideri connetterti, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

   > **Note**
   >
   > Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

9. Per visualizzare le statistiche relative a una connessione, scegli Connessione nella finestra del client AWS VPN, scegli Mostra dettagli, quindi scegli la connessione di cui desideri visualizzare i dettagli.
10. Per disconnettere una connessione, scegli una connessione nella finestra del client AWS VPN, quindi scegli Disconnetti. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente.

AWS Client VPN note di rilascio per Linux

La tabella seguente contiene le note di rilascio e i link 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
5.2.0	• Miglioramenti minori. • È stato aggiunto il supporto per Client Route Enforcement.	8 aprile 2025	Scarica la versione 5.2.0 sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• È stato risolto un problema che causava la riconnessione automatic a della versione 5.0.x alla VPN dopo una disconnessione per un timeout di inattività. AWS Client VPN • Miglioramenti e correzioni di bug minori.	17 marzo 2025	Scarica la versione 5.1.0 sha256:14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba

Versione	Modifiche	Data	Collegamento per il download
5.0.0	• È stato aggiunto il supporto per più connessioni simultanee. • È stata aggiornata l'interfaccia utente grafica. • Miglioramenti e correzioni di bug minori.	21 gennaio 2025	Scarica la versione 5.0.0 sha256:64 5126b5698 cb550e9dc 822e58ed8 99a5730d2 e204f28f4 023ec6719 15fdda0c
4.1.0	• Aggiunto il supporto per Ubuntu 22.04 e 24.04. • Correzioni di bug.	12 novembre 2024	Scarica la versione 4.1.0 sha256:33 4d0022245 8fbfe9dad e16c99fe9 7e9ebcbd5 1fff017d0 d6b1d1b76 4e7af472
4.0.0	Miglioramenti minori.	25 settembre 2024	Scarica la versione 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686

Versione	Modifiche	Data	Collegamento per il download
3.15.1	Aggiunto il supporto per il `mssfix` flag OpenVPN.	4 settembre 2024	Scarica la versione 3.15.1 sha256: ffb65c0bc93e8d611cbce2deb6b82f600e6434e4d03c6b44c53d61a2efcaadc2
3.15.0	• Aggiunto il supporto per il `tap-sleep` flag OpenVPN. • Aggiornate le librerie OpenVPN e OpenSSL.	12 agosto 2024	Scarica la versione 3.15.0 sha256:5cf3eb08de96821b0ad3d0c93174b2e308041d5490a3edb772dfd89a6d89d012
3.14.0	• Aggiornate le librerie OpenVPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.14.0 sha256: bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60

Versione	Modifiche	Data	Collegamento per il download
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 autentica zione SAML 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 configurazioni LAN". • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• Problemi di connettività risolti per alcune configurazioni LAN. • 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 è abilitato nella rete client. NAT64 • 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 OpenVPN «verify-x509-name».	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 i flag OpenVPN: 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 i flag OpenVPN: inactive, pull-filter, route. • 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 AWS Client VPN endpoint utilizzando un client OpenVPN

È possibile stabilire una connessione a un endpoint Client VPN utilizzando le comuni applicazioni client Open VPN. Client VPN è supportato sui seguenti sistemi operativi:

- Windows

  Usa un certificato e una chiave privata da Windows Certificate Store. Dopo aver generato il certificato e la chiave, puoi stabilire una connessione AWS Client utilizzando l'applicazione client OpenVPN GUI o OpenVPN GUI Connect Client. Per i passaggi per creare il certificato e la chiave, vedi. Stabilisci una connessione VPN utilizzando un certificato su Windows

- Android e iOS

  Stabilisci una connessione VPN utilizzando l'applicazione client OpenVPN su un dispositivo Android o iOS. Per ulteriori informazioni, consulta Connessioni Client VPN su Android e iOS.

- macOS

  Stabilisci una connessione VPN utilizzando un file di configurazione per Tunnelblick basato su macOS o per Client VPN. AWS Per ulteriori informazioni, consulta Stabilisci una connessione VPN su macOS.

- Linux

  Stabilisci una connessione VPN su Linux utilizzando l'interfaccia OpenVPN - Network Manager o l'applicazione OpenVPN. Per utilizzare l'interfaccia OpenVPN - Network Manager devi prima installare il modulo di gestione della rete se non è già installato. Per ulteriori informazioni, consulta Stabilire una connessione VPN su Linux.

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN. Ciò include qualsiasi architettura basata su ARM. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi Windows basati su

ARM), devi utilizzare endpoint VPN basati su SAML con il AWS client fornito anziché client OpenVPN.

Applicazioni client

- Connect a un AWS Client VPN endpoint utilizzando un'applicazione client Windows
- AWS Client VPN connessioni su applicazioni Android e iOS
- Connect a un AWS Client VPN endpoint utilizzando un'applicazione client macOS
- Connect a un AWS Client VPN endpoint utilizzando un'applicazione client OpenVPN

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

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

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi delle connessioni AWS Client VPN con client basati su Windows.

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN. Ciò include qualsiasi architettura basata su ARM. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi Windows basati su ARM), devi utilizzare endpoint VPN basati su SAML con il AWS client fornito anziché client OpenVPN.

Attività

- Utilizzare un certificato e stabilire una connessione AWS Client VPN su Windows

Utilizzare un certificato e stabilire una connessione AWS Client VPN su Windows

È possibile configurare il client OpenVPN in modo che utilizzi un certificato e una chiave privata dall'archivio del sistema di certificati di Windows. Questa opzione è utile quando si utilizza una smart card per la connessione Client VPN. Per informazioni sull'opzione cryptoapicert del client OpenVPN, consulta il Manuale di riferimento per OpenVPN sul sito Web di OpenVPN.

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

Per utilizzare un certificato e stabilire una connessione

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, consulta Come visualizzare i certificati con lo snap-in MMC 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, vedere Diritti di visualizzazione dell'archivio dei certificati del computer locale sul sito Web di Microsoft.
4. Aggiorna il file di configurazione OpenVPN e specifica il certificato utilizzando l'oggetto del certificato o l'identificazione 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, vedere Procedura: Recuperare l'impronta digitale di un certificato sul sito Web di Microsoft.

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

5. Dopo aver completato la configurazione, usa OpenVPN per stabilire una connessione VPN effettuando una delle seguenti operazioni:

   - Usa l'applicazione client GUI OpenVPN
     1. Avviare l'applicazione client OpenVPN.
     2. Nella barra delle applicazioni di Windows, scegli Mostra/nascondi icone. Fai clic con il pulsante destro del mouse su OpenVPN GUI, quindi scegli Importa file.
     3. Nella finestra di dialogo di apertura, seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Open (Apri).
     4. Nella barra delle applicazioni di Windows, scegli Mostra/nascondi icone. Fai clic con il pulsante destro del mouse su OpenVPN GUI, quindi scegli Connect.

   - Usa il client OpenVPN GUI Connect
     1. Avvia l'applicazione OpenVPN e scegli Importa, Da file locale... .
     2. Passa al file di configurazione ricevuto dall'amministratore VPN e seleziona Apri.

AWS Client VPN connessioni su applicazioni Android e iOS

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN. Ciò include qualsiasi architettura basata su ARM. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi Windows basati su ARM), devi utilizzare endpoint VPN basati su SAML con il AWS client fornito anziché client OpenVPN.

La procedura seguente mostra come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN 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 client OpenVPN per iOS o Android, consulta la Guida per l'utente di OpenVPN Connect sul sito Web di OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per stabilire la connessione, avvia l'applicazione client OpenVPN, quindi importa il file ricevuto dall'amministratore Client VPN.

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

Queste sezioni descrivono come stabilire una connessione VPN utilizzando il client VPN basato su macOS, Tunnelblick o Client VPN. AWS

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi delle connessioni AWS Client VPN con client macOS.

> **Important**
>
> Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN. Ciò include qualsiasi architettura basata su ARM. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi Windows basati su ARM), devi utilizzare endpoint VPN basati su SAML con il AWS client fornito anziché client OpenVPN.

Argomenti

Stabilire una AWS Client VPN connessione su macOS

È possibile stabilire una connessione VPN 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 utilizzando Tunnelblick

1. Avviare l'applicazione client Tunnelblick e scegliere I have configuration files (Ho i file di configurazione).
2. Trascinare il file di configurazione ricevuto dall'amministratore VPN nel riquadro Configurations (Configurazioni).
3. Selezionare il file di configurazione nel riquadro Configurazioni e scegliere Connetti.

Per stabilire una connessione VPN utilizzando AWS Client VPN.

1. Avvia l'applicazione OpenVPN e scegli Importa, Dal file locale....
2. Passa al file di configurazione ricevuto dall'amministratore VPN e seleziona Apri.

Connect a un AWS Client VPN endpoint utilizzando un'applicazione client OpenVPN

Queste sezioni descrivono come stabilire una connessione VPN utilizzando OpenVPN - Network Manager o OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN. Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi delle connessioni AWS Client VPN con client basati su Linux.

> **Important**
>
> Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN. Ciò include qualsiasi architettura basata su ARM. Se utilizzi un

dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi Windows basati su ARM), devi utilizzare endpoint VPN basati su SAML con il AWS client fornito anziché client OpenVPN.

Argomenti

Stabilisci una connessione su Linux AWS Client VPN

Stabilisci una connessione VPN utilizzando la GUI di Network Manager su un computer Ubuntu o l'applicazione OpenVPN.

Per stabilire una connessione VPN utilizzando OpenVPN - Network Manager

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. Scegliere il simbolo più (+) accanto a VPN, quindi selezionare Import from file... (Importa da file...).
4. Passare al file di configurazione ricevuto dall'amministratore VPN e scegliere Open (Apri).
5. Nella finestra Aggiungi VPN scegli Aggiungi.
6. Avviare la connessione abilitando l'interruttore accanto al profilo VPN aggiunto.

Per stabilire una connessione VPN utilizzando OpenVPN

1. Installare OpenVPN usando il seguente comando.

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

2. Avviare la connessione caricando il file di configurazione ricevuto dall'amministratore VPN.

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

Risoluzione dei problemi relativi alle connessioni AWS Client VPN

Utilizza gli argomenti seguenti per risolvere i problemi che si potrebbero verificare durante l'utilizzo di un'applicazione client per connettersi a un endpoint Client VPN.

Argomenti

Risoluzione dei problemi degli endpoint Client VPN per gli amministratori

Alcune delle fasi in questa guida possono essere eseguite dall'utente. Altre fasi devono essere eseguite dall'amministratore Client VPN sull'endpoint Client VPN stesso. Nelle sezioni seguenti viene descritto quando è necessario contattare l'amministratore.

Per ulteriori informazioni sulla risoluzione dei problemi relativi agli endpoint Client VPN, consulta Risoluzione dei problemi di Client VPN nella Guida per l'amministratore di AWS Client VPN .

Invia i log di diagnostica al client Supporto AWS fornito AWS

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

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

Inviare registri di diagnostica

Il client 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 Supporto AWS, 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 Supporto AWS, 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 Supporto AWS, dovrete fornire loro il numero di riferimento.

Risoluzione dei problemi delle connessioni AWS Client VPN con client basati su Windows

Nelle sezioni seguenti sono riportate informazioni sui problemi che potrebbero verificarsi durante l'utilizzo di client basati su Windows per connettersi a un endpoint Client VPN.

AWS ha fornito i registri degli eventi del client

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_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. 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 sulla risoluzione dei problemi

- Il client non è in grado di connettersi
- Il client non può connettersi con il messaggio di registro “nessun adattatore TAP-Windows”
- Il client è bloccato in uno stato di riconnessione
- Il processo di connessione VPN si chiude in maniera imprevista
- Impossibile avviare l'applicazione
- Il client non è in grado di creare un profilo
- La VPN si disconnette con un messaggio pop-up
- Si verifica un arresto anomalo del client su Dell che utilizza Windows 10 o 11 PCs
- OpenVPN GUI
- Client OpenVPN Connect

- Impossibile risolvere il DNS
- Alias PKI mancante

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

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

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN 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 .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Il client non può connettersi con il messaggio di registro “nessun adattatore TAP-Windows”

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN e nei registri delle applicazioni 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 Avvio -> Tutti i programmi -> TAP-Windows -> Utilità -> Aggiungi un nuovo adattatore Ethernet virtuale TAP-Windows.

Soluzione

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

- Riavvia l'adattatore TAP-Windows.
- Reinstalla 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'endpoint Client VPN, 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 nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

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

Il processo di connessione VPN si chiude in maniera imprevista

Problema

Durante la connessione a un endpoint Client VPN, il client si chiude in maniera imprevista.

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

.NET Framework 4.7.2 o versione successiva non è installato nel 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'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

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

La VPN si disconnette con un messaggio pop-up

Problema

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

Causa

L'adattatore TAP-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
```

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

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 configurazione VPN.

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 seguenti DLLs:

- 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 su Download Client VPN AWS 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, è possibile eliminare o rinominare i file DLL. Tuttavia, ricorda che ciò impedirà il funzionamento completo dell'applicazione Dell Backup and Recovery.

Elimina o rinomina 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. Elimina manualmente i seguenti file DLL dalla directory di installazione o rinominali. 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. DBROverlay IconBackuped

OpenVPN GUI

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 11.10.0.0 e 11.11.0.0 del software OpenVPN GUI in Windows 10 Home (a 64 bit) e Windows Server 2016 (a 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 OpenVPN Connect

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 2.6.0.100 e 2.7.1.101 del software OpenVPN Connect Client in Windows 10 Home (64 bit) e Windows Server 2016 (a 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 il 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

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

Soluzione

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Alias PKI mancante

Problema

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

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

Causa

Il software OpenVPN Connect Client presenta un problema noto in cui tenta di eseguire l'autenticazione 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

Specifica una chiave e un certificato client casuali nel file di configurazione Client VPN e importa la nuova configurazione nel software OpenVPN Connect Client. In alternativa, utilizzare un client diverso, ad esempio il client GUI OpenVPN (v11.12.0.0) o il client Viscosity (v.1.7.14).

Risoluzione dei problemi delle connessioni AWS Client VPN con 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.

AWS ha fornito i registri degli eventi del client

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_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. 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.

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

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

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

Argomenti sulla risoluzione dei problemi

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

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

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN 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 .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'endpoint Client VPN, 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 nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedi all'amministratore Client VPN di verificare che la direttiva `remote` nel file di configurazione venga risolta in un indirizzo IP valido. Puoi anche disconnettere la sessione VPN selezionando Disconnetti nella finestra del client AWS VPN 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'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

Assicurati che l'amministratore Client VPN aggiunga il certificato e la chiave 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

Quando tenti di connettere la VPN, viene visualizzato il seguente errore.

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

Soluzione

Vedi il seguente articolo su AWS re:POST. Client AWS VPN: lo strumento di supporto è un errore obbligatorio

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 il dettaglio dei log, aprire l'applicazione Tunnelblick, scegliere Settings (Impostazioni) e regolare il valore per VPN log level (Livello di log VPN).

Impossibile trovare l'algoritmo di cifratura 'AES-256-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 versione OpenVPN che non supporta l'algoritmo di crittografia AES-256-GCM.

Soluzione

Scegliere una versione di OpenVPN compatibile nel modo seguente:

1. Aprire l'applicazione Tunnelblick.
2. Seleziona Impostazioni.
3. Per OpenVPN version (Versione di OpenVPN), scegliere 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - la versione OpenSSL 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 dall'amministratore Client VPN.

Utilizzo chiave esteso (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 client non va a buon fine perché il campo Utilizzo chiave esteso (EKU) del certificato client è abilitato per l'autenticazione del server.

Soluzione

Verifica di utilizzare il certificato e la chiave client corretti. Se necessario, verifica con l'amministratore VPN Client. Questo errore può verificarsi se usi il certificato server e non il certificato client per connetterti all'endpoint Client VPN.

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'amministratore Client VPN.

OpenVPN

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 2.7.1.100 del software OpenVPN 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

OpenVPN Connect non è in grado di risolvere il nome DNS Client VPN.

Soluzione

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Risoluzione dei problemi delle connessioni AWS Client VPN 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 ha fornito i registri degli eventi del client
- Le query DNS vanno a un nameserver predefinito
- OpenVPN (riga di comando)
- OpenVPN tramite Network Manager (GUI)

AWS ha fornito i registri degli eventi del client

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/
```

Ad esempio, è possibile controllare i seguenti file di registro per trovare errori negli up/down script DNS che causano l'interruzione della connessione:

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

Le query DNS vanno a un nameserver predefinito

Problema

In alcuni casi, dopo aver stabilito una connessione VPN, le query DNS continueranno a passare al server dei nomi di sistema predefinito anziché ai server dei nomi configurati per l'endpoint Client VPN.

Causa

Il Client interagisce con systemd-resolved, un servizio disponibile sui sistemi Linux, che funge da elemento centrale della gestione DNS. Viene utilizzato per configurare i server DNS che vengono spinti dall'endpoint Client VPN. Il problema si verifica perché systemd-resolved non imposta la priorità più alta per i server DNS forniti dall'endpoint Client VPN. Al contrario, i server vengono aggiunti all'elenco esistente dei server DNS configurati nel sistema locale. Di conseguenza, i server DNS originali potrebbero ancora avere la priorità più alta e quindi essere utilizzati per risolvere le query DNS.

Soluzione

1. Aggiungi la seguente direttiva nel file di configurazione di OpenVPN per essere certo che tutte le query DNS vengano inviate nel 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 vuoi che systemd-resolved utilizzi un proxy per le query DNS ma desideri che le query vengano inviate direttamente ai server dei nomi DNS reali, stabilisci un collegamento simbolico da `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`.

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

   È possibile eseguire questa procedura per aggirare la configurazione risolta dal sistema, ad esempio per la memorizzazione nella cache delle risposte DNS, la configurazione DNS per interfaccia, l'applicazione e così via. DNSSec Questa opzione è particolarmente utile quando è necessario sovrascrivere un record DNS pubblico con un record privato quando si è connessi a VPN. Ad esempio, è possibile che nel VPC privato sia presente un resolver DNS privato con un record per www.example.com, che viene risolto 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.

OpenVPN (riga di comando)

Problema

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

Causa

Il server DNS non è configurato nell'endpoint Client VPN o non viene accettato dal software client.

Soluzione

Utilizzare le fasi seguenti per verificare che il server DNS sia configurato e funzioni correttamente.

1. Accertarsi che una voce del server DNS sia presente nei log. Nell'esempio seguente, il server DNS `192.168.0.2` (configurato nell'endpoint Client VPN) 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 specificato alcun server DNS, chiedi all'amministratore Client VPN di modificare l'endpoint Client VPN assicurandosi che per l'endpoint Client VPN sia specificato un server DNS

(ad esempio il server DNS VPC). Per ulteriori informazioni, consulta Endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

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 configurazione Client VPN (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
```

OpenVPN tramite Network Manager (GUI)

Problema

Quando si utilizza il client Network Manager OpenVPN, la connessione non riesce 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

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Risoluzione dei problemi più comuni relativi a AWS Client VPN

Di seguito sono riportati i problemi comuni che possono verificarsi quando utilizzi un client per connetterti a un endpoint Client VPN.

Negoziazione chiave TLS non riuscita

Problema

La negoziazione TLS non va a buon fine 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 il traffico UDP o TCP.
- La chiave e il certificato client utilizzati nel file di configurazione (.ovpn) sono errati.
- L'elenco di revoche di certificati (CRL) del client è scaduto.

Soluzione

Verifica che le regole del firewall sul computer non blocchino il traffico TCP o UDP in ingresso o in uscita sulle porte 443 o 1194. Chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Le regole del firewall per l'endpoint Client VPN non blocchino il traffico TCP o UDP 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 .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Cronologia dei documenti

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

Modifica	Descrizione	Data
AWS rilasciato il client fornito (5.2.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	18 giugno 2025
AWS rilasciato il client fornito (5.2.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	2 giugno 2025
AWS rilasciato il client fornito (5.2.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 aprile 2025
AWS rilasciato il client fornito (5.2.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025
AWS rilasciato il client fornito (5.2.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025
AWS rilasciato il client fornito (5.2.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025
AWS rilasciato il client fornito (5.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
AWS rilasciato il client fornito (5.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
AWS rilasciato il client fornito (5.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
È stato rimosso il supporto per macOS Monterey e aggiunto il supporto per macOS Sonoma (14.0)	Per i dettagli, consulta i requisiti di Client VPN per macOS.	12 marzo 2025

È stato rimosso il supporto sia per Ubuntu 18.0.4 (LTS) che per Ubuntu 20.04 LTS (solo) AMD64	Per ulteriori informazioni, consulta Client VPN for Linux Requisiti.	12 marzo 2025
AWS rilasciato il client fornito (5.0.3) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	6 marzo 2025
AWS rilasciato il client fornito (5.0.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	24 febbraio 2025
AWS rilasciato il client fornito (5.0.2) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	17 febbraio 2025
AWS rilasciato il client fornito (5.0.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	30 gennaio 2025
AWS rilasciato il client fornito (5.0.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	22 gennaio 2025
Il client AWS fornito ora supporta fino a cinque connessioni simultanee	Vedi Support per connessioni simultanee utilizzando un client AWS fornito per i dettagli.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024

AWS rilasciato il client fornito (4.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (4.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (4.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (3.15.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024
AWS rilasciato il client fornito (3.14.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024
AWS rilasciato il client fornito (3.12.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024
AWS rilasciato il client fornito (3.14.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	22 agosto 2024
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 LTS e Ubuntu 20.04 LTS	È possibile utilizzare il AWS client fornito su Ubuntu 18.04 LTS e Ubuntu 20.04 LTS.	11 giugno 2021
Supporto per OpenVPN tramite un certificato dall'archivio del sistema di certificati di Windows	Puoi utilizzare OpenVPN con un certificato dall'archivio del sistema di certificati di Windows	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 endpoint Client VPN.	4 febbraio 2020
Versione iniziale	Questa versione introduce AWS Client 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.