Panduan Pengguna

AWS Client VPN

AWS Client VPN: Panduan Pengguna

Table of Contents

Apa yang dimaksud dengan AWS Client VPN?

AWS Client VPN adalah layanan VPN berbasis klien terkelola yang memungkinkan Anda mengakses sumber daya AWS dan sumber daya di jaringan on-premise Anda dengan aman.

Panduan ini menyajikan langkah-langkah membuat koneksi VPN ke titik akhir Client VPN menggunakan aplikasi klien pada perangkat Anda.

Komponen

Berikut ini adalah komponen kunci untuk menggunakan AWS Client VPN.

- Titik akhir Client VPN — Administrator Client VPN Anda membuat dan mengonfigurasi titik akhir Client VPN di AWS. Administrator mengontrol jaringan dan sumber daya yang dapat Anda akses ketika Anda membuat koneksi VPN.
- Aplikasi Client VPN — Aplikasi perangkat lunak yang Anda gunakan untuk terhubung ke titik akhir Client VPN dan membuat koneksi VPN yang aman.
- File konfigurasi titik akhir Client VPN — File konfigurasi yang diberikan oleh administrator Client VPN Anda. File tersebut mencakup informasi tentang titik akhir Client VPN dan sertifikat yang diperlukan untuk membuat koneksi VPN. Anda memuat file ini ke aplikasi klien VPN pilihan Anda.

Sumber daya tambahan

Jika Anda adalah administrator Client VPN, lihat Panduan Administrator AWS Client VPN untuk informasi selengkapnya tentang membuat dan mengonfigurasi titik akhir Client VPN.

Mulai dengan Client VPN

Sebelum Anda dapat membuat sesi VPN, administrator Client VPN Anda harus membuat dan mengonfigurasi titik akhir Client VPN. Administrator Anda mengontrol jaringan dan sumber daya yang dapat Anda akses saat membuat sesi VPN. Kemudian Anda menggunakan aplikasi klien VPN agar terhubung ke titik akhir Client VPN dan membuat koneksi VPN yang aman.

Jika Anda adalah administrator yang perlu membuat titik akhir Client VPN, lihat Panduan Administrator AWS Client VPN.

Topik

Prasyarat

Untuk membuat koneksi VPN, Anda harus melakukan hal berikut:

- Mengakses ke internet
- Perangkat yang didukung
- Untuk titik akhir Client VPN yang menggunakan autentikasi gabungan berbasis SAML (sistem masuk tunggal), lihat salah satu peramban berikut:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Langkah 1: Dapatkan aplikasi klien VPN

Anda dapat terhubung ke titik akhir Client VPN dan membuat koneksi VPN menggunakan klien AWS yang disediakan atau aplikasi klien berbasis OpenVPN lainnya.

Klien yang disediakan oleh AWS didukung di Windows, macOS, Ubuntu 18.04 LTS, dan Ubuntu 20.04 LTS. Anda dapat mengunduh klien di Unduhan AWS Client VPN.

Atau, unduh dan instal aplikasi klien OpenVPN pada perangkat yang Anda inginkan untuk membuat koneksi VPN.

Langkah 2: Dapatkan file konfigurasi titik akhir Client VPN

Anda harus mendapatkan file konfigurasi titik akhir Client VPN dari administrator Anda. File konfigurasi mencakup informasi tentang titik akhir Client VPN dan sertifikat yang diperlukan untuk membuat koneksi VPN.

Selain itu, jika administrator Client VPN Anda telah mengonfigurasi portal layanan mandiri untuk titik akhir Client VPN, Anda dapat mengunduh sendiri klien AWS yang disediakan versi terbaru dan file konfigurasi titik akhir Client VPN versi terbaru. Untuk informasi selengkapnya, lihat Menggunakan portal layanan mandiri.

Langkah 3: Connect ke VPN

Impor file konfigurasi titik akhir Client VPN ke klien AWS yang disediakan atau aplikasi klien OpenVPN Anda dan hubungkan ke VPN. Untuk langkah-langkah menghubungkan ke VPN, lihat topik berikut:

- Hubungkan menggunakan klien AWS yang disediakan
- Hubungkan menggunakan klien OpenVPN

Untuk titik akhir Client VPN yang menggunakan autentikasi Direktori Aktif, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi Anda. Jika autentikasi multi-faktor (MFA) telah diaktifkan untuk direktori tersebut, Anda juga akan diminta untuk memasukkan kode MFA.

Untuk titik akhir Client VPN yang menggunakan autentikasi gabungan berbasis SAML (sistem masuk tunggal), klien AWS yang disediakan membuka jendela peramban pada komputer Anda. Anda akan diminta untuk memasukkan kredensial perusahaan Anda sebelum terhubung ke titik akhir Client VPN.

Menggunakan portal layanan mandiri

Administrator titik akhir Client VPN Anda dapat mengonfigurasi portal layanan mandiri untuk titik akhir Client VPN. Portal layanan mandiri adalah halaman web yang memungkinkan Anda mengunduh versi

terbaru klien AWS yang disediakan dan versi terbaru dari file konfigurasi titik akhir Client VPN. Untuk informasi selengkapnya tentang mengonfigurasi portal layanan mandiri, lihat Titik akhir Client VPN di Panduan Administrator AWS Client VPN.

Sebelum memulai, Anda harus memiliki ID titik akhir Client VPN. Administrator titik akhir Client VPN Anda dapat memberikan ID, atau dapat memberikan URL portal layanan mandiri yang menyertakan ID.

Untuk mengakses portal layanan mandiri

1. Buka portal layanan mandiri di https://self-service.clientvpn.amazonaws.com/, atau gunakan URL yang disediakan oleh administrator Anda.
2. Jika diperlukan, masukkan ID titik akhir Client VPN, misalnya, `cvpn-endpoint-0123456abcd123456`. Pilih Selanjutnya.
3. Masukkan nama pengguna dan kata sandi Anda dan pilih Masuk. Ini adalah nama pengguna dan kata sandi yang sama yang Anda gunakan untuk terhubung ke titik akhir Client VPN.
4. Di portal layanan mandiri, Anda dapat melakukan hal berikut:
   - Mengunduh file konfigurasi klien versi terbaru untuk titik akhir Client VPN.
   - Mengunduh versi terbaru klien AWS yang disediakan untuk platform Anda.

Hubungkan menggunakan klien AWS yang disediakan

Anda dapat menghubungkan ke titik akhir Client VPN menggunakan klien AWS yang disediakan. Klien yang disediakan oleh AWS didukung di Windows, macOS, Ubuntu 18.04 LTS dan Ubuntu 20.04 LTS.

Klien

- AWS Client VPN untuk Windows
- AWS Client VPN untuk macOS
- AWS Client VPN untuk Linux

Arahan OpenVPN

Klien yang disediakan oleh AWS mendukung arahan OpenVPN sebagai berikut:

- auth-federasi
- auth-nocache
- authentikasi kembali
- auth-user-pass
- ca
- sertifikat
- cipher
- klien
- sambungkan-coba lagi
- connect-retry-max
- cryptoapicert
- dev
- tipe dev-
- dhcp-opsi
- ifconfig-ipv6
- tidak aktif

- keepalive
- kunci
- bangsawan
- kunci persisten
- persist-tun
- ping
- ping restart
- proto
- tarik
- saring-tarik
- rcvbuf
- terpencil
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- selesaikan-coba lagi
- rute
- rute-ipv6
- server-poll-timeout
- tantangan statis
- tun-mtu
- tun-mtu-extra
- kata kerja
- verify-x509-nama

AWS Client VPN untuk Windows

Prosedur berikut menunjukkan cara membuat koneksi VPN menggunakan klien yang AWS disediakan untuk Windows. Anda dapat mengunduh dan menginstal klien di mengunduh AWS Client VPN. Klien yang AWS disediakan tidak mendukung pembaruan otomatis.

Daftar Isi

Persyaratan

Untuk menggunakan klien yang AWS disediakan untuk Windows, berikut ini diperlukan:

- Sistem operasi Windows 10 64-bit, x64 processor
- .NET Framework 4.7.2 atau lebih tinggi

Klien mencadangkan port TCP 8096 pada komputer Anda. Untuk titik akhir Client VPN yang menggunakan autentikasi gabungan berbasis SAML (sistem masuk tunggal), klien mencadangkan port TCP 35001.

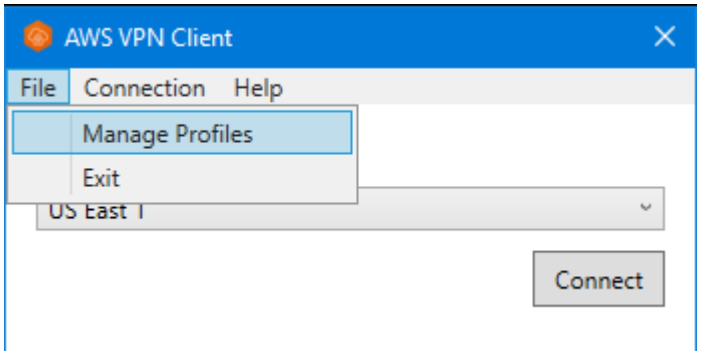
Sebelum memulai, pastikan administrator Client VPN Anda telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Terhubung

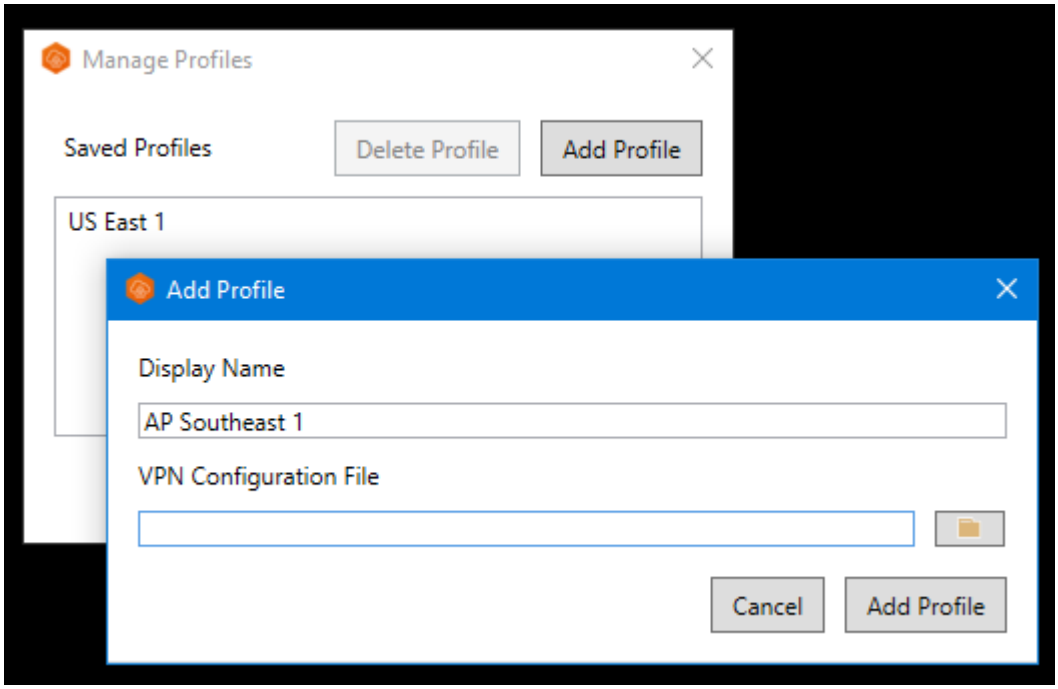
Sebelum memulai, pastikan Anda telah membaca persyaratan. Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk Windows

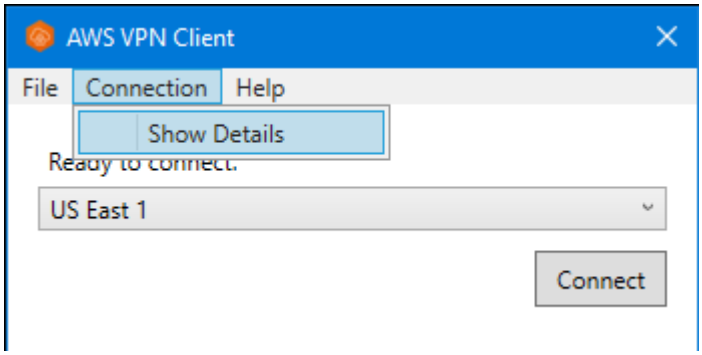
1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola Profil.



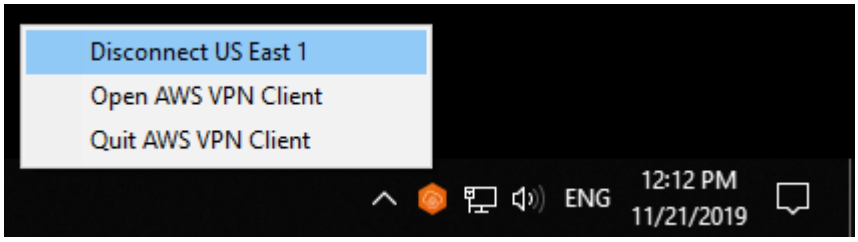
3. Pilih Tambah Profil.



4. Untuk Nama Tampilan, masukkan nama untuk profil.
5. Untuk File Konfigurasi VPN, jelajah dan kemudian pilih file konfigurasi yang Anda terima dari administrator Client VPN Anda, lalu pilih Tambah Profil.
6. Di jendela AWS VPN Klien, pastikan bahwa profil Anda dipilih, lalu pilih Hubungkan. Jika titik akhir Client VPN telah dikonfigurasi untuk menggunakan autentikasi berbasis kredensial, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.
7. Untuk melihat statistik koneksi Anda, pilih Koneksi, Tampilkan Detail.



8. Untuk memutuskan hubungan, di jendela AWS VPN Klien, pilih Putuskan Hubungan. Atau, pilih ikon klien pada taskbar Windows, kemudian pilih Putuskan Hubungan.



Catatan rilis

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi Windows saat ini dan sebelumnya. AWS Client VPN

> **Note**
>
> Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin terpengaruh oleh masalah kegunaan dan/atau keamanan, lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.12.0	• Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah. • Fokus aplikasi otomatis dihapus saat terhubung dengan titik akhir SAMP.	21 Mei 2024	Unduh versi 3.12.0 sha256: fae30c27694a320b86c67e45043435c50c42753bddfdcc9b0112389ea881fba4
3.11.2	• Menyelesaikan masalah otentikasi SAMP dengan browser berbasis Chromium sejak versi 123.	April 11, 2024	Unduh versi 3.11.2 sha256:8ba258dd15bea3e861ad

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
			ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc
3.11.1	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan. • Postur keamanan yang ditingkatkan.	Februari 16, 2024	Unduh versi 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Memperbaiki masalah konektivitas yang disebabkan oleh Windows VM. • Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Unduh versi 3.11.0 sha256:9b 6b7def99d 76c59a97b 067b6a73b dc6ee1c6b 89a206328 6f542e96b 32df5ae9

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.10.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Memperbaiki masalah konektivitas saat adaptor jaringan Hyper-V diinstal pada mesin klien. • Perbaikan bug minor dan peningkatan.	24 Agustus 2023	Unduh versi 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	• Postur keamanan yang ditingkatkan.	3 Agustus 2023	Unduh versi 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8d82 67a0e1fb2 173a8aae21ed
3.8.0	• Postur keamanan yang ditingkatkan.	15 Juli 2023	Tidak lagi didukung
3.7.0	• Menggulung kembali perubahan dari 3.6.0.	15 Juli 2023	Tidak lagi didukung
3.6.0	• Postur keamanan yang ditingkatkan.	14 Juli 2023	Tidak lagi didukung
3.5.0	Perbaikan bug minor dan peningkatan.	3 April 2023	Tidak lagi didukung
3.4.0	Menggulung kembali perubahan dari versi 3.3.0.	Maret 28, 2023	Tidak lagi didukung
3.3.0	Perbaikan bug minor dan peningkatan.	Maret 17, 2023	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.2.0	• Menambahkan dukungan untuk bendera OpenVPN “verify-x509-name”. • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Ditambahkan kemampuan untuk secara otomatis menginstal versi klien baru bila tersedia.	23 Januari 2023	Tidak lagi didukung
3.1.0	Postur keamanan yang ditingkatkan.	23 Mei 2022	Tidak lagi didukung
3.0.0	• Menambahkan dukungan Windows 11. • Memperbaiki nama driver TAP Windows yang menyebabkan nama driver lain terpengaruh. • Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks banner tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan.	3 Maret 2022	Tidak lagi didukung
2.0.0	• Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo • Perbaikan bug minor dan peningkatan.	20 Januari 2022	Tidak lagi didukung
1.3.7	• Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus. • Perbaikan bug minor dan peningkatan.	November 8, 2021	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.3.6	• Menambahkan dukungan untuk flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Perbaikan bug minor dan peningkatan.	September 20, 2021	Tidak lagi didukung
1.3.5	Patch untuk menghapus file log windows besar.	16 Agustus 2021	Tidak lagi didukung
1.3.4	• Ditambahkan dukungan untuk bendera OpenVPN: dhcp-option. • Perbaikan bug minor dan peningkatan.	4 Agustus 2021	Tidak lagi didukung
1.3.3	• Penambahan dukungan untuk tanda OpenVPN: tidak aktif, pull-filter, rute. • Perbaikan masalah yang menyebabk an aplikasi terganggu saat koneksi terputus atau keluar. • Perbaikan masalah dengan nama pengguna Direktori Aktif dengan garis miring terbalik. • Perbaikan kerusakan aplikasi saat memanipulasi daftar profil di luar aplikasi. • Perbaikan bug minor dan penyempur naan.	1 Juli 2021	Tidak lagi didukung
1.3.2	• Menambahkan pencegahan kebocoran IPv6, saat dikonfigurasi. • Perbaikan potensi gangguan ketika Anda menggunakan opsi Tampilkan Detail di bawah Koneksi.	12 Mei 2021	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.3.1	• Penambahan dukungan untuk beberapa sertifikat klien dengan subjek yang sama. Sertifikat kedaluwarsa akan diabaikan. • Perbaikan retensi log lokal dalam mengurangi penggunaan disk. • Penambahan dukungan untuk arahan OpenVPN 'route-ipv6'. • Perbaikan bug minor dan penyempur naan.	5 April 2021	Tidak lagi didukung
1.3.0	Penambahan fitur dukungan seperti pelaporan kesalahan, pengiriman log diagnostik, dan analitik.	8 Maret 2021	Tidak lagi didukung
1.2.7	• Penambahan dukungan untuk arahan OpenVPN cryptoapicert. • Perbaikan rute usang antar koneksi. • Perbaikan bug minor dan penyempur naan.	25 Februari 2021	Tidak lagi didukung
1.2.6	Perbaikan bug minor dan penyempur naan.	26 Oktober 2020	Tidak lagi didukung
1.2.5	• Penambahan dukungan untuk komentar dalam konfigurasi OpenVPN. • Penambahan pesan kesalahan untuk kesalahan handshake TLS.	8 Oktober 2020	Tidak lagi didukung
1.2.4	Perbaikan bug minor dan penyempur naan.	1 September 2020	Tidak lagi didukung
1.2.3	Kembali ke perubahan dalam versi 1.2.2.	20 Agustus 2020	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.2.1	Perbaikan bug minor dan penyempur naan.	1 Juli 2020	Tidak lagi didukung
1.2.0	• Penambahan dukungan untuk Autentikasi gabungan berbasis SAML 2.0. • Dukungan tidak lagi digunakan pada platform Windows 7.	19 Mei 2020	Tidak lagi didukung
1.1.1	Perbaikan bug minor dan penyempur naan.	21 April 2020	Tidak lagi didukung
1.1.0	• Penambahan dukungan fungsionalitas echo respons statis OpenVPN untuk menyembunyikan atau menampilkan teks yang ditampilkan dalam antarmuka pengguna. • Perbaikan bug minor dan penyempur naan.	9 Maret 2020	Tidak lagi didukung
1.0.0	Rilis awal.	4 Februari 2020	Tidak lagi didukung

AWS Client VPN untuk macOS

Prosedur berikut menunjukkan cara membuat koneksi VPN menggunakan klien yang AWS disediakan untuk macOS. Anda dapat mengunduh dan menginstal klien di mengunduh AWS Client VPN. Klien yang AWS disediakan tidak mendukung pembaruan otomatis.

Daftar Isi

Persyaratan

Untuk menggunakan klien yang AWS disediakan untuk macOS, berikut ini diperlukan:

- macOS Monterey (12.0), Ventura (13.0), atau Sonoma (14.0).
- prosesor x86_64 kompatibel.
- Klien mencadangkan port TCP 8096 pada komputer Anda.
- Untuk titik akhir Client VPN yang menggunakan autentikasi gabungan berbasis SAML (sistem masuk tunggal), klien mencadangkan port TCP 35001.

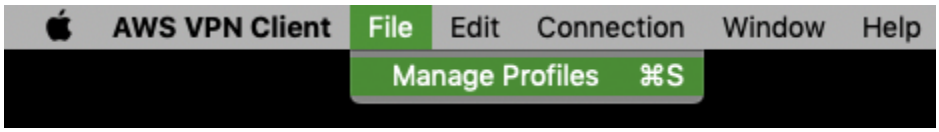
Terhubung

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

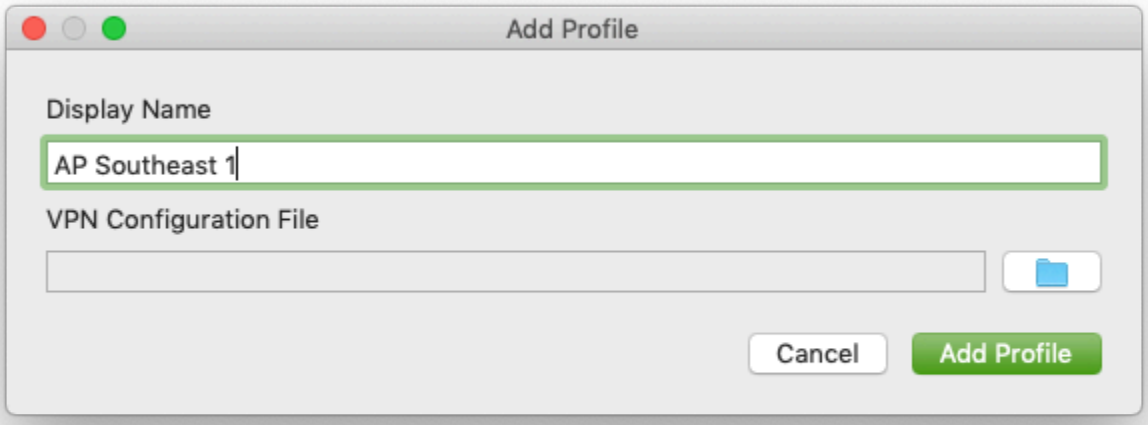
Juga, pastikan bahwa Anda telah membaca persyaratan. Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk macOS

1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola profil.

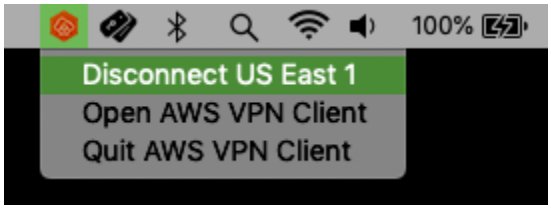


3. Pilih Tambah profil.
4. Untuk Nama tampilan, masukkan nama untuk profil.



5. Untuk File Konfigurasi VPN, jelajahi file konfigurasi yang Anda terima dari administrator Client VPN Anda. Pilih Buka.
6. Pilih Tambah profil.
7. Di jendela AWS VPN Klien, pastikan bahwa profil Anda dipilih, lalu pilih Hubungkan. Jika titik akhir Client VPN telah dikonfigurasi untuk menggunakan autentikasi berbasis kredensial-, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.
8. Untuk melihat statistik koneksi Anda, pilih Koneksi, Tampilkan detail.

9. Untuk memutuskan koneksi, di jendela AWS VPN Client, pilih Putuskan. Atau, pilih ikon klien pada bilah menu, lalu pilih Putuskan sambungan < your-profile-name >.



Catatan rilis

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi macOS saat ini dan sebelumnya. AWS Client VPN

> **Note**
>
> Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin terpengaruh oleh masalah kegunaan dan/atau keamanan, lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
3.10.0	• Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah. • Memperbaiki masalah restorasi DNS selama sakelar jaringan. • Fokus aplikasi otomatis dihapus saat terhubung dengan titik akhir SAMP.	21 Mei 2024	Unduh versi 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3.9.2	• Menyelesaikan masalah otentikas i SAMP dengan browser berbasis Chromium sejak versi 123. • Menambahkan dukungan untuk macOS Sonoma. Menanggalkan dukungan untuk macOS Big Sur. • Postur keamanan yang ditingkatkan.	April 11, 2024	Unduh versi 3.9.2 sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480
3.9.1	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan. • Bilah kemajuan unduhan pembaruan aplikasi tetap.	Februari 16, 2024	Unduh versi 3.9.1 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306

Versi	Perubahan	Tanggal	Tautan unduh
	• Postur keamanan yang ditingkatkan.		179fac8e5 00e2c7af4 e899e971
3.9.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Unduh versi 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8
3.8.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Perbaikan bug minor dan peningkatan.	24 Agustus 2023	Unduh versi 3.8.0 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	• Postur keamanan yang ditingkatkan.	3 Agustus 2023	Unduh versi 3.7.0 sha256:4a 34b25b482 33b02d610 7638a3868 f7e419a84 d20bb4989 f7b394aae 9a9de00a
3.6.0	• Postur keamanan yang ditingkatkan.	15 Juli 2023	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduh
3.5.0	• Perubahan yang digulirkan kembali dari 3.4.0.	15 Juli 2023	Tidak lagi didukung
3.4.0	• Postur keamanan yang ditingkatkan.	14 Juli 2023	Tidak lagi didukung
3.3.0	• Menambahkan dukungan untuk macOS Ventura (13.0). • Perbaikan bug minor dan peningkatan.	27 April 2023	Tidak lagi didukung
3.2.0	• Menambahkan dukungan untuk bendera OpenVPN “verify-x509-name”. • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Ditambahkan kemampuan untuk secara otomatis menginstal versi klien baru bila tersedia.	23 Januari 2023	Tidak lagi didukung
3.1.0	• Menambahkan dukungan untuk macOS Monterey. • Memperbaiki masalah untuk deteksi tipe drive. • Postur keamanan yang ditingkatkan.	23 Mei 2022	Tidak lagi didukung
3.0.0	• Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks banner tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan.	3 Maret 2022	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
2.0.0	• Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo • Perbaikan bug minor dan peningkatan.	20 Januari 2022	Tidak lagi didukung.
1.4.0	• Menambahkan pemantauan server DNS selama koneksi. Pengaturan akan dikonfigurasi ulang jika tidak cocok dengan pengaturan VPN. • Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus. • Perbaikan bug minor dan peningkatan.	November 9, 2021	Tidak lagi didukung.
1.3.5	• Menambahkan dukungan untuk flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Perbaikan bug minor dan peningkatan.	September 20, 2021	Tidak lagi didukung.
1.3.4	• Ditambahkan dukungan untuk bendera OpenVPN: dhcp-option. • Perbaikan bug minor dan peningkatan.	4 Agustus 2021	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.3.3	• Penambahan dukungan untuk tanda OpenVPN: tidak aktif, pull-filter, rute. • Perbaikan masalah pada nama file konfigurasi dengan spasi atau Unicode. • Perbaikan masalah yang menyebabkan aplikasi terganggu saat koneksi terputus atau keluar. • Perbaikan masalah dengan nama pengguna Direktori Aktif dengan garis miring terbalik. • Perbaikan kerusakan aplikasi saat memanipulasi daftar profil di luar aplikasi. • Perbaikan bug minor dan penyempurnaan.	1 Juli 2021	Tidak lagi didukung.
1.3.2	• Menambahkan pencegahan kebocoran IPv6, saat dikonfigurasi. • Perbaikan potensi gangguan ketika Anda menggunakan opsi Tampilkan Detail di bawah Koneksi. • Tambahkan rotasi log daemon.	12 Mei 2021	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.3.1	• Penambahan dukungan untuk macOS Big Sur (10.16). • Perbaikan masalah yang menghapus konfigurasi pengaturan DNS oleh aplikasi lain. • Perbaikan masalah saat menggunak an sertifikat non-valid untuk autentikasi bersama yang menyebabkan masalah konektivitas. • Penambahan dukungan untuk arahan OpenVPN 'route-ipv6'. • Perbaikan bug minor dan penyempur naan.	5 April 2021	Tidak lagi didukung.
1.3.0	Penambahan fitur dukungan seperti pelaporan kesalahan, pengiriman log diagnostik, dan analitik.	8 Maret 2021	Tidak lagi didukung.
1.2.5	Perbaikan bug minor dan penyempur naan.	25 Februari 2021	Tidak lagi didukung.
1.2.4	Perbaikan bug minor dan penyempur naan.	26 Oktober 2020	Tidak lagi didukung.
1.2.3	• Penambahan dukungan untuk komentar dalam konfigurasi OpenVPN. • Penambahan pesan kesalahan untuk kesalahan handshake TLS. • Perbaikan bug penghapusan instalan yang memengaruhi beberapa pengguna.	8 Oktober 2020	Tidak lagi didukung.
1.2.2	Perbaikan bug minor dan penyempur naan.	12 Agustus 2020	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.2.1	• Penambahan dukungan untuk menghapus aplikasi. • Perbaikan bug minor dan penyempur naan.	1 Juli 2020	Tidak lagi didukung.
1.2.0	• Penambahan dukungan untuk Autentikasi gabungan berbasis SAML 2.0. • Penambahan dukungan untuk macOS Catalina (10.15).	19 Mei 2020	Tidak lagi didukung.
1.1.2	Perbaikan bug minor dan penyempur naan.	21 April 2020	Tidak lagi didukung.
1.1.1	• Perbaikan masalah DNS yang tidak diselesaikan. • Perbaikan masalah kerusakan aplikasi yang disebabkan oleh koneksi yang terlalu lama. • Perbaikan masalah MFA.	2 April 2020	Tidak lagi didukung.
1.1.0	• Penambahan dukungan untuk konfigurasi DNS macOS. • Penambahan dukungan fungsionalitas echo static challenge OpenVPN untuk menyembunyikan atau menampilkan teks yang ditampilkan dalam antarmuka pengguna. • Perbaikan bug minor dan penyempur naan.	9 Maret 2020	Tidak lagi didukung.
1.0.0	Rilis awal.	4 Februari 2020	Tidak lagi didukung.

AWS Client VPN untuk Linux

Prosedur berikut menunjukkan cara menginstal klien yang AWS disediakan untuk Linux, dan untuk membuat koneksi VPN menggunakan klien yang AWS disediakan. Klien yang AWS disediakan untuk Linux tidak mendukung pembaruan otomatis.

Daftar Isi

Persyaratan

Untuk menggunakan klien yang AWS disediakan untuk Linux, berikut ini diperlukan:

- Ubuntu 18.04 LTS atau Ubuntu 20.04 LTS (hanya AMD64)

Klien cadangan TCP port 8096 pada komputer Anda. Untuk titik akhir Client VPN yang menggunakan autentikasi federasi berbasis SAML (sistem masuk tunggal) klien mencadangkan port TCP 35001.

Sebelum memulai, pastikan administrator Client VPN Membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Penginstalan

Ada beberapa metode yang dapat digunakan untuk menginstal klien yang AWS disediakan untuk Linux. Gunakan salah satu metode yang disediakan dalam pilihan berikut. Sebelum memulai, pastikan Anda telah membaca persyaratan.

Opsi 1 — Instal melalui repositori paket

1. Tambahkan kunci publik AWS VPN Client ke OS Ubuntu Anda.

```
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. Gunakan perintah yang berlaku untuk menambah repositori ke OS Ubuntu Anda, tergantung pada versi Ubuntu Anda:

   Ubuntu 18.04

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

   Ubuntu 20.04

   ```
   echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
    ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
   ```

3. Gunakan perintah berikut untuk memperbarui repositori pada sistem Anda.

   ```
   sudo apt-get update
   ```

4. Gunakan perintah berikut untuk menginstal klien yang AWS disediakan untuk Linux.

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

Opsi 2 — Instal menggunakan paket file .deb

1. Unduh file .deb dari mengunduh AWS Client VPN atau dengan menggunakan perintah berikut ini.

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

2. Instal klien AWS yang disediakan untuk Linux menggunakan `dpkg` utilitas.

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

Opsi 3 — Instal paket .deb menggunakan Ubuntu Software Center

1. Unduh paket file .deb dari mengunduh AWS Client VPN .

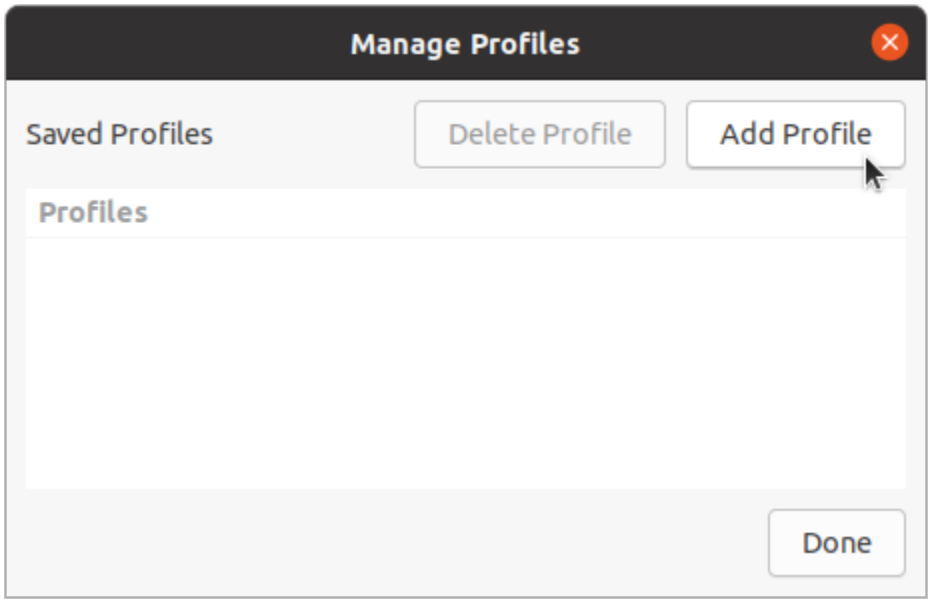
2. Setelah men-download paket file .deb, gunakan Ubuntu Software Center untuk menginstal paket. Ikuti langkah-langkah untuk menginstal dari paket .deb mandiri menggunakan Ubuntu Software Center, seperti yang dijelaskan pada Wiki Ubuntu.

Terhubung

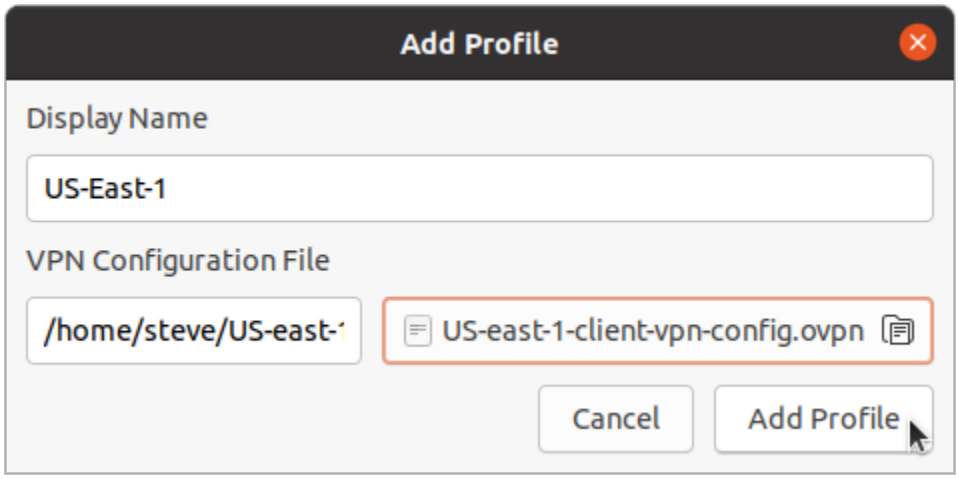
Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk Linux

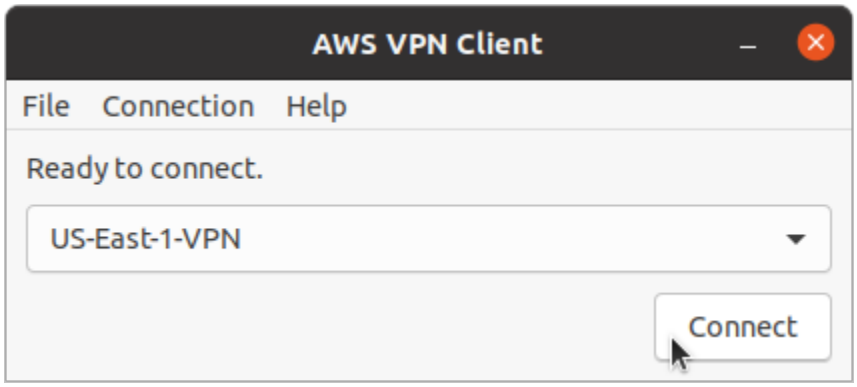
1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola Profil.
3. Pilih Tambah Profil.



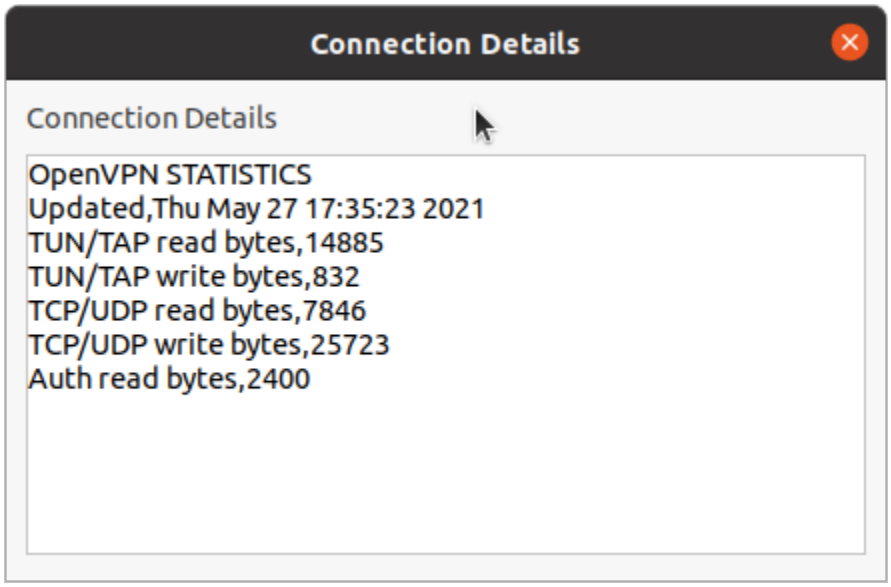
4. Untuk Nama Tampilan, masukkan nama untuk profil.
5. Untuk File Konfigurasi VPN, jelajahi file konfigurasi yang Anda terima dari administrator Client VPN Anda. Pilih Buka.
6. Pilih Tambah Profil.



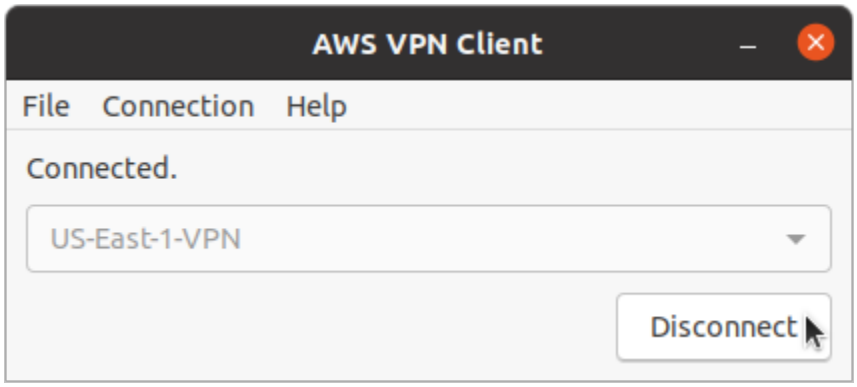
7. Di jendela AWS VPN Client, pastikan bahwa profil Anda dipilih, dan kemudian pilih Connect. Jika titik akhir Client VPN telah dikonfigurasi untuk menggunakan autentikasi berbasis kredensial, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.



8. Untuk melihat statistik hubungan Anda, pilih Koneksi, Tampilkan detail.



9. Untuk memutuskan koneksi, di jendela AWS VPN Client, pilih Putuskan Koneksi.



Catatan rilis

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi Linux saat ini dan sebelumnya. AWS Client VPN

> **Note**
>
> Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin terpengaruh oleh masalah kegunaan dan/atau keamanan, lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
3.13.0	• Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah.	21 Mei 2024	Unduh versi 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1
3.12.2	• Menyelesaikan masalah otentikas i SAMB dengan browser berbasis Chromium sejak versi 123.	April 11, 2024	Unduh versi 3.12.2

Versi	Perubahan	Tanggal	Tautan unduh
			sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan. • Postur keamanan yang ditingkatkan.	Februari 16, 2024	Unduh versi 3.12.1 sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0
3.12.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN.	Desember 19, 2023	Unduh versi 3.12.0 sha256:9b 73987309f 1dca1960a 322c5dd86 eec1568ed 270bfd25f 78cc430e3 b5f85cc1

Versi	Perubahan	Tanggal	Tautan unduh
3.11.0	• Rollback untuk “Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN”. • Peningkatan aksesibilitas.	6 Desember 2023	Unduh versi 3.11.0 sha256:86 c0fa1bf1c 971940828 35a739ec7 f1c87e540 194955f41 4a35c679b 94538970
3.10.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Unduh versi 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Perbaikan bug minor dan peningkatan.	24 Agustus 2023	Unduh versi 3.9.0 sha256:6c de9cfff82 754119e6a 68464d4bb 350da3cb3 e1ebf9140 dacf24e4f d2197454

Versi	Perubahan	Tanggal	Tautan unduh
3.8.0	• Postur keamanan yang ditingkatkan.	3 Agustus 2023	Unduh versi 3.8.0 sha256:5f e479236cc 0a1940ba3 7fe168e55 1096f8dae 4c68d4556 0a164e41e dea3e5bd
3.7.0	• Postur keamanan yang ditingkatkan.	15 Juli 2023	Tidak lagi didukung
3.6.0	• Menggulung kembali perubahan dari 3.5.0.	15 Juli 2023	Tidak lagi didukung
3.5.0	• Postur keamanan yang ditingkatkan.	14 Juli 2023	Tidak lagi didukung
3.4.0	• Menambahkan dukungan untuk bendera OpenVPN “verify-x509-name”.	14 Februari 2023	Tidak lagi didukung
3.1.0	• Memperbaiki masalah untuk deteksi tipe drive. • Postur keamanan yang ditingkatkan.	23 Mei 2022	Tidak lagi didukung
3.0.0	• Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks spanduk tetap untuk teks yang lebih panjang dan urutan karakter tertentu. • Postur keamanan yang ditingkatkan.	3 Maret 2022	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
2.0.0	• Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo • Perbaikan bug minor dan peningkatan.	20 Januari 2022	Tidak lagi didukung.
1.0.3	• Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus. • Perbaikan bug minor dan peningkatan.	November 8, 2021	Tidak lagi didukung.
1.0.2	• Menambahkan dukungan untuk flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Perbaikan bug minor dan peningkatan.	September 28, 2021	Tidak lagi didukung.
1.0.1	• Opsi yang diaktifkan untuk berhenti dari bilah aplikasi Ubuntu. • Penambahan dukungan untuk tanda OpenVPN: tidak aktif, pull-filter, rute. • Perbaikan bug minor dan peningkatan.	4 Agustus 2021	Tidak lagi didukung.
1.0.0	Rilis awal.	11 Juni 2021	Tidak lagi didukung.

Hubungkan menggunakan klien OpenVPN

Anda dapat terhubung ke titik akhir Client VPN menggunakan aplikasi klien Open VPN umum.

> **Note**
>
> Untuk autentikasi federasi berbasis SAML, Anda harus menggunakanAWSmenyediakan klien untuk terhubung ke titik akhir Client VPN. Untuk informasi selengkapnya, lihatHubungkan menggunakan klien AWS yang disediakanatau hubungi administrator VPN Anda.

Aplikasi klien

- Hubungkan menggunakan aplikasi klien Windows
- Terhubung menggunakan aplikasi klien Android atau iOS VPN
- Hubungkan menggunakan aplikasi klien macOS
- Hubungkan menggunakan aplikasi klien OpenVPN

Hubungkan menggunakan aplikasi klien Windows

Prosedur berikut menunjukkan cara membuat koneksi VPN menggunakan koneksi VPN berbasis Windows.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Untuk informasi pemecahan masalah, lihat Pemecahan masalah Windows.

OpenVPN menggunakan sertifikat dari Windows Certificate System Store

Anda dapat mengonfigurasi klien OpenVPN untuk menggunakan sertifikat dan kunci privat dari Windows Certificate System Store. Opsi ini berguna ketika Anda menggunakan kartu pintar sebagai bagian dari koneksi Client VPN Anda. Untuk informasi tentang opsi klien OpenVPN cryptoapicert, lihat Manual Referensi untuk OpenVPN di situs web OpenVPN.

> **Note**
>
> Sertifikat harus disimpan di komputer lokal.

Untuk menggunakan opsi cryptoapicert dengan OpenVPN

1. Buat file .pfx yang berisi sertifikat klien dan kunci privat.
2. Impor file .pfx ke penyimpanan sertifikat pribadi Anda, pada komputer lokal. Untuk informasi selengkapnya, lihatCara: Lihat sertifikat dengan snap-in MMCdi situs web Microsoft.
3. Verifikasi bahwa akun Anda memiliki izin untuk membaca sertifikat komputer lokal. Anda juga dapat menggunakan Konsol Manajemen Microsoft untuk mengubah izin. Untuk informasi selengkapnya, lihat Hak untuk melihat penyimpanan sertifikat komputer lokal di situs web Microsoft Technet.
4. Perbarui file konfigurasi OpenVPN dan tentukan sertifikat dengan menggunakan subjek sertifikat, atau sidik jari sertifikat.

   Berikut ini adalah contoh untuk menentukan sertifikat dengan menggunakan subjek.

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

   Berikut ini adalah contoh untuk menentukan sertifikat dengan menggunakan sidik jari. Anda dapat menemukan sidik jari dengan menggunakan Konsol Manajemen Microsoft. Untuk informasi selengkapnya, lihatCara: Mengambil Sidik Jari Sertifikatdi situs web Microsoft Technet.

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

Setelah menyelesaikan konfigurasi, Anda menggunakan OpenVPN untuk membuat koneksi.

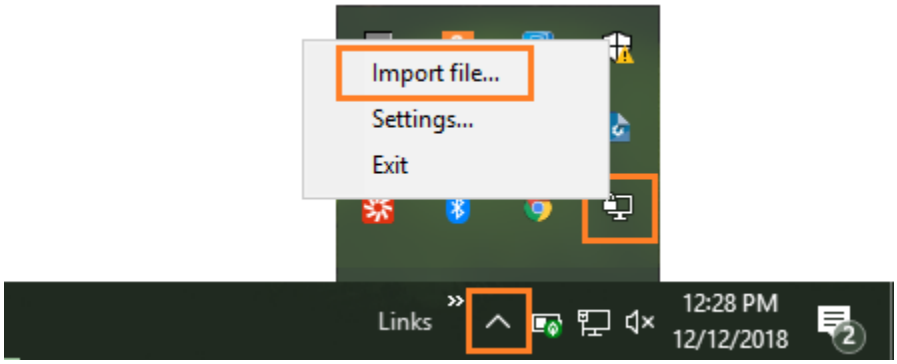
OpenVPN GUI

Prosedur berikut menunjukkan cara untuk membuat koneksi VPN menggunakan aplikasi klien OpenVPN GUI pada komputer Windows.

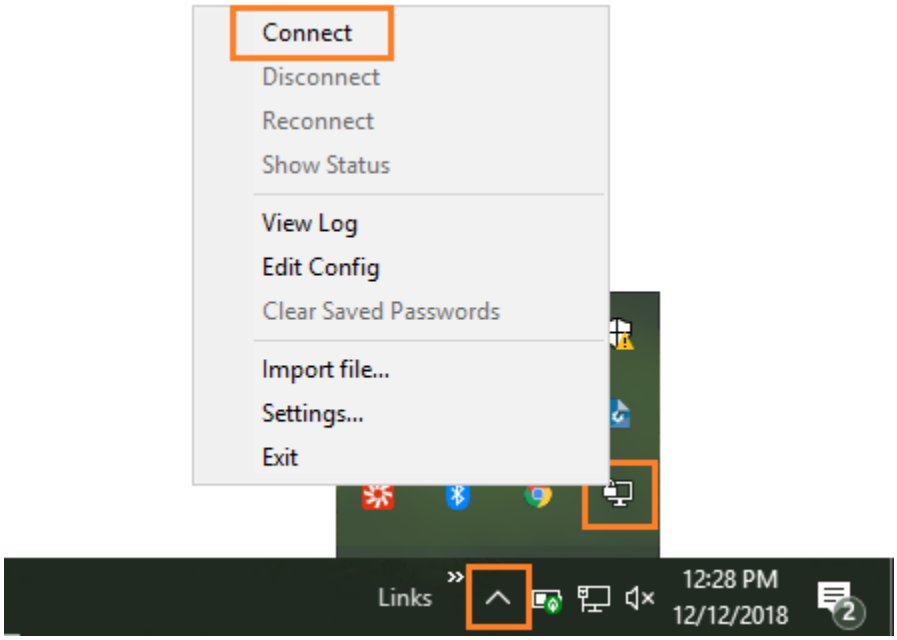
> **Note**
>
> Untuk informasi tentang aplikasi klien OpenVPN, lihat Unduhan Komunitas di situs web OpenVPN.

Untuk membuat koneksi VPN

1. Mulai aplikasi klien OpenVPN.
2. Pada taskbar Windows, pilih Tampilkan/Sembunyikan ikon, klik kanan GUI OpenVPN, dan pilih Impor file.



3. Di kotak dialog Buka, pilih file konfigurasi yang Anda terima dari administrator Client VPN dan pilih Buka.
4. Pada taskbar Windows, pilih Tampilkan/Sembunyikan ikon, klik kanan GUI OpenVPN, dan pilih Hubungkan.



OpenVPN Connect Client

Prosedur berikut menunjukkan cara untuk membuat koneksi VPN menggunakan aplikasi OpenVPN Connect Client pada komputer Windows.

> **Note**
>
> Untuk informasi selengkapnya, lihat Terhubung ke Server Akses dengan Windows di situs web OpenVPN.

Untuk membuat koneksi VPN

1. Mulai aplikasi OpenVPN Connect Client.
2. Pada taskbar Windows, pilih Tampilkan/Sembunyikan ikon, klik kanan OpenVPN, dan pilih Impor profil.
3. Pilih Impor dari File lalu pilih file konfigurasi yang Anda terima dari administrator Client VPN Anda.
4. Untuk memulai koneksi, pilih profil koneksi.

Terhubung menggunakan aplikasi klien Android atau iOS VPN

Informasi berikut menunjukkan cara membuat koneksi VPN menggunakan aplikasi klien OpenVPN pada perangkat seluler Android atau iOS. Langkah-langkah untuk Android dan iOS sama.

> **Note**
>
> Untuk informasi selengkapnya tentang aplikasi klien OpenVPN untuk Android, lihat FAQ mengenai OpenVPN Connect Android di situs web OpenVPN.

Sebelum memulai, pastikan administrator Client VPN Anda membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Untuk membuat koneksi, jalankan aplikasi klien OpenVPN, dan kemudian impor file yang Anda terima dari administrator Client VPN Anda.

Hubungkan menggunakan aplikasi klien macOS

Prosedur berikut menunjukkan cara membuat koneksi VPN menggunakan koneksi VPN berbasis macOS.

Sebelum memulai, pastikan administrator Client VPN Anda telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Untuk informasi pemecahan masalah, lihat Pemecahan masalah macOS.

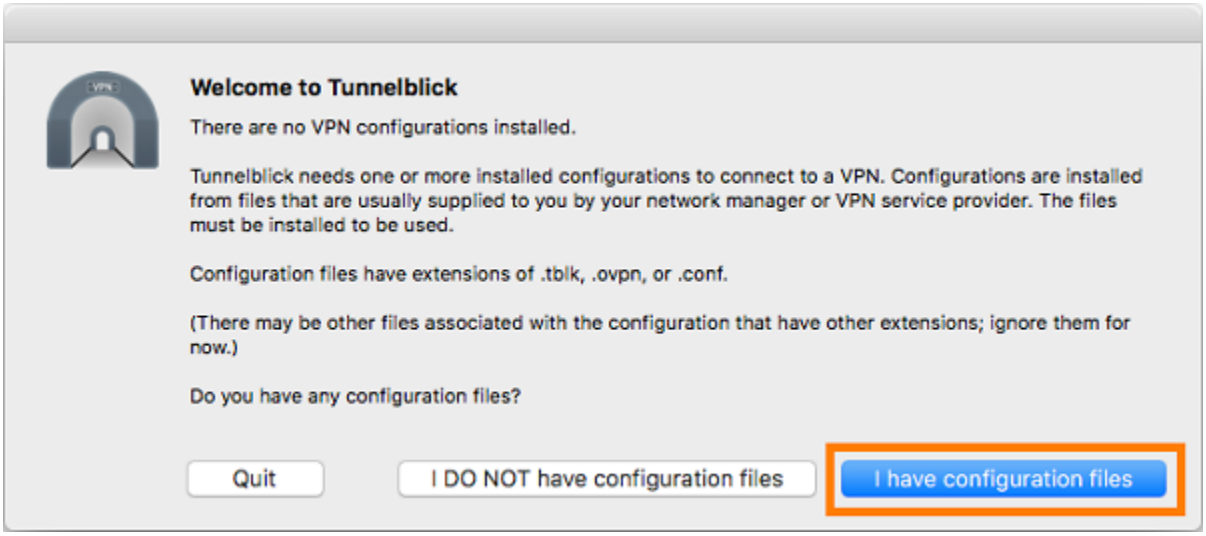
Tunnelblick

Prosedur berikut menunjukkan cara untuk membuat koneksi VPN menggunakan aplikasi klien Tunnelblick pada komputer macOS.

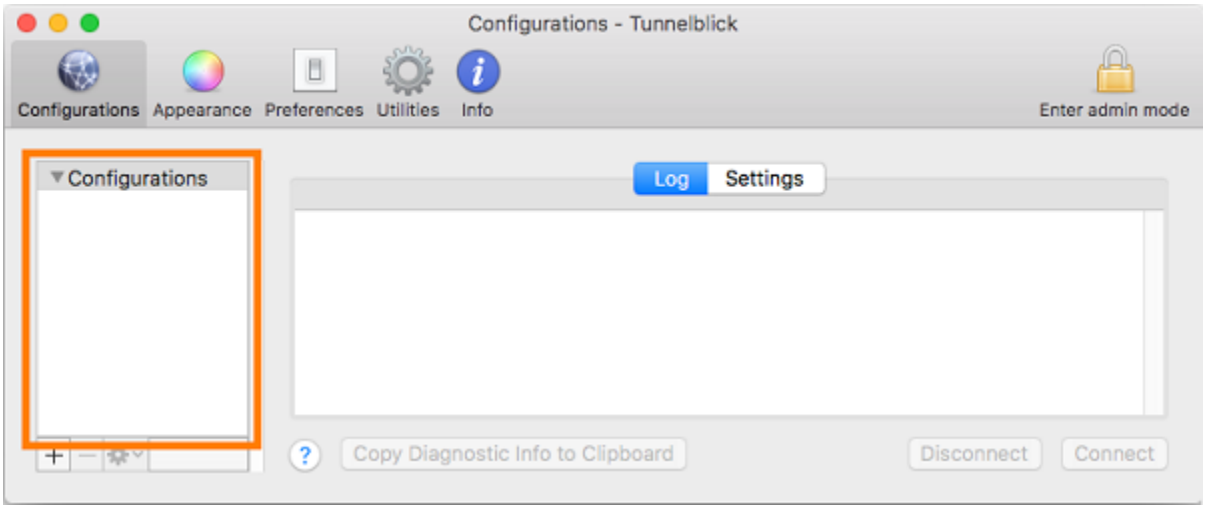
> **Note**
>
> Untuk informasi selengkapnya tentang aplikasi klien Tunnelblick untuk macOS, lihat dokumentasi Tunnelblick di situs web Tunnelblick.

Untuk membuat koneksi VPN

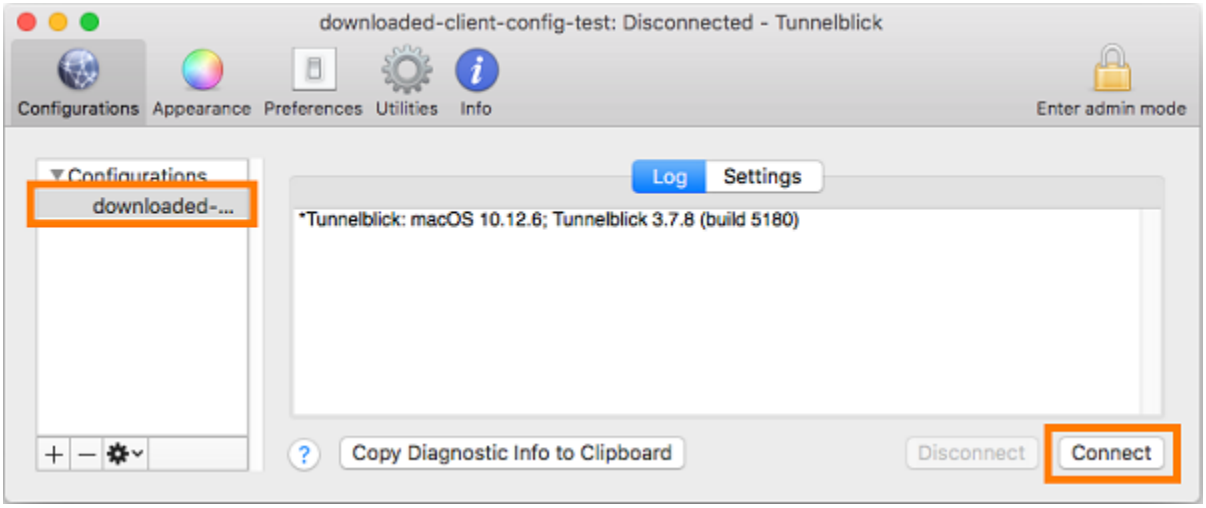
1. Mulai aplikasi klien Tunnelblick dan pilih Saya memiliki file konfigurasi.



2. Seret dan jatuhkan file konfigurasi yang Anda terima dari administrator VPN Anda di panel Konfigurasi.



3. Pilih file konfigurasi dalam panel Konfigurasi dan pilih Hubungkan.



OpenVPN Connect Client

Prosedur berikut menunjukkan bagaimana untuk membuat koneksi VPN menggunakan aplikasi OpenVPN Connect Client pada komputer macOS.

> **Note**
>
> Untuk informasi selengkapnya, lihat Terhubung ke Server Akses dengan macOS di situs web OpenVPN.

Untuk membuat koneksi VPN

1. Mulai aplikasi OpenVPN, dan pilih Impor, Dari file lokal....
2. Navigasikan ke file konfigurasi yang Anda terima dari administrator VPN Anda dan pilih Buka.

Hubungkan menggunakan aplikasi klien OpenVPN

Prosedur berikut menunjukkan cara membuat koneksi VPN menggunakan koneksi VPN berbasis OpenVPN.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN.

Untuk informasi pemecahan masalah, lihat Pemecahan masalah Linux.

> **Important**
>
> Jika titik akhir Client VPN telah dikonfigurasi untuk menggunakan autentikasi gabungan berbasis SAML, Anda tidak dapat menggunakan klien VPN berbasis OpenVPN untuk terhubung ke titik akhir Client VPN.

OpenVPN - Network Manager

Prosedur berikut menunjukkan cara untuk membuat koneksi VPN menggunakan aplikasi OpenVPN melalui GUI Network Manager Jaringan pada komputer Ubuntu.

Untuk membuat koneksi VPN

1. Instal modul network manager menggunakan perintah berikut.

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

2. Buka Pengaturan, Jaringan.
3. Pilih tanda tambah (+) di sebelah VPN, lalu pilih Impor dari file....
4. Navigasikan ke file konfigurasi yang Anda terima dari administrator VPN Anda dan pilih Buka.
5. Di jendela Tambahkan VPN, pilih Tambahkan.

6. Mulai hubungan dengan mengaktifkan tombol toggle di samping profil VPN yang Anda tambahkan.

OpenVPN

Prosedur berikut menunjukkan cara untuk membuat koneksi VPN menggunakan aplikasi OpenVPN pada komputer Ubuntu.

Untuk membuat koneksi VPN

1. Instal OpenVPN menggunakan perintah berikut.

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

2. Mulai hubungan dengan memuat file konfigurasi yang Anda terima dari administrator VPN Anda.

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

Pemecahan masalah koneksi Client VPN Anda

Gunakan topik berikut untuk memecahkan masalah yang mungkin Anda alami saat menggunakan aplikasi client untuk terkoneksi dengan titik akhir Client VPN.

Topik

Pemecahan masalah titik akhir Client VPN untuk administrator

Beberapa langkah dalam panduan ini dapat dilakukan oleh Anda. Langkah-langkah lain harus dilakukan oleh administrator Client VPN Anda pada titik akhir Client VPN itu sendiri. Bagian berikut memberi tahu kapan Anda perlu menghubungi administrator Anda.

Untuk informasi tambahan tentang pemecahan masalah titik akhir Client VPN, lihat Pemecahan masalah Client VPN dalam Panduan Administrator AWS Client VPN .

Kirim log diagnostik ke AWS Support klien yang AWS disediakan

Jika Anda memiliki masalah dengan klien yang AWS disediakan dan Anda perlu menghubungi AWS Support untuk membantu memecahkan masalah, klien memiliki opsi untuk mengirim log diagnostik ke. AWS Support Opsi ini tersedia pada aplikasi Windows, MacOS dan Linux client.

Sebelum Anda mengirim file, Anda harus setuju untuk mengizinkan AWS Support untuk mengakses log diagnostik Anda. Setelah Anda setuju, kami memberi Anda nomor referensi yang dapat Anda berikan AWS Support sehingga mereka dapat segera mengakses file.

Mengirim log diagnostik

Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk Windows

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Ya.
4. Di dalam jendela Kirim Log Diagnostik, lakukan salah satu operasi berikut:
   - Untuk menyalin nomor referensi ke clipboard, pilih Ya, dan kemudian pilih OKE.
   - Untuk melacak nomor referensi secara manual, pilih Tidak.

   Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk macOS

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Ya.
4. Perhatikan nomor referensi dari jendela konfirmasi, dan kemudian pilih OKE.

   Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk Ubuntu

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Kirim.
4. Perhatikan nomor referensi dari jendela konfirmasi. Anda diberi sebuah pilihan untuk menyalin informasi ke clipboard jika Anda mau.

   Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Pemecahan masalah Windows

Bagian berikut berisi informasi tentang masalah yang mungkin Anda alami saat menggunakan client berbasis Windows untuk terkoneksi ke titik akhir Client VPN.

Topik

AWS klien yang disediakan

AWS klien yang disediakan

Klien yang AWS disediakan membuat log peristiwa dan menyimpannya di lokasi berikut di komputer Anda.

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

Jenis-jenis log berikut tersedia:

- Log aplikasi: Berisi informasi tentang aplikasi. Log-log ini diawali dengan 'aws_vpn_client_'.
- Log OpenVPN: Berisi informasi tentang proses OpenVPN. Log-log ini diawali dengan 'ovpn_aws_vpn_client_'.

Klien yang AWS disediakan menggunakan layanan Windows untuk melakukan operasi root. Log layanan Windows disimpan di dalam lokasi berikut di komputer Anda.

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

Topik

- VPN terputus dengan pesan pop up

Client tidak dapat mengoneksikan

Masalah

Klien yang AWS disediakan tidak dapat terhubung ke titik akhir Client VPN.

Penyebab

Penyebab dari masalah berikut mungkin adalah salah satu dari hal-hal berikut:

- Proses OpenVPN lainnya sudah berjalan di komputer Anda, sehingga mencegah client untuk terkoneksi.
- File (.ovpn) konfigurasi milik Anda tidak valid.

Solusi

Periksa apakah ada aplikasi OpenVPN lain yang berjalan di komputer Anda. Jika ada, berhenti atau keluar dari proses-proses tersebut dan coba terkoneksi kembali ke titik akhir Client VPN. Periksa apakah terdapat galat log OpenVPN, dan minta administrator Client VPN Anda untuk memverifikasi informasi berikut:

- Bahwa file konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat Ekspor Konfigurasi client dalam Panduan administrator AWS Client VPN .
- CRL masih valid. Untuk informasi selengkapnya, lihat Klien Tidak Dapat Terhubung dengan Titik Akhir Client VPN dalam Panduan Administrator AWS Client VPN .

Klien tidak dapat terhubung dengan pesan log “tidak ada adaptor TAP-Windows”

Masalah

Klien yang AWS disediakan tidak dapat terhubung ke titik akhir Client VPN dan pesan kesalahan berikut muncul di log aplikasi: “Tidak ada adaptor TAP-Windows pada sistem ini. Anda harus dapat membuat adaptor TAP-Windows dengan membuka Start -> All Programs -> TAP-Windows -> Utilities -> Tambahkan adaptor ethernet virtual TAP-Windows baru”.

Solusi

Anda dapat mengatasi masalah ini dengan mengambil satu atau lebih tindakan berikut:

- Mulai ulang adaptor TAP-Windows.
- Instal ulang driver TAP-Windows.
- Buat adaptor TAP-Windows baru.

Client berada dalam status mengoneksikan ulang.

Masalah

Klien yang AWS disediakan mencoba untuk terhubung ke titik akhir Client VPN, tetapi terjebak dalam keadaan menyambung kembali.

Penyebab

Penyebab dari masalah berikut mungkin adalah sah satu dari hal-hal berikut:

- Komputer Anda tidak terkoneksi ke internet.
- DNS hostname tidak terhubung ke alamat IP.
- Proses OpenVPN merupakan upaya tanpa batas untuk terkoneksi dengan titik akhir.

Solusi

Verifikasi bahwa komputer Anda terkoneksi ke internet. Minta kepada administrator Client VPN Anda untuk memverifikasi bahwa direktif `remote` dalam file konfigurasi me-resolve ke alamat IP yang valid. Anda juga dapat memutuskan sambungan sesi VPN dengan memilih Putuskan sambungan di jendela Klien AWS VPN, dan coba sambungkan lagi.

Proses koneksi VPN berhenti secara tiba-tiba

Masalah

Saat mengoneksikan ke titik akhir Client VPN, client terhenti secara tiba-tiba.

Penyebab

TAP-Windows tidak diinstal di komputer anda. Perangkat lunak ini diperlukan untuk dapat menjalankan client.

Solusi

Jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

Aplikasi gagal diluncurkan

Masalah

Pada Windows 7, klien yang AWS disediakan tidak diluncurkan ketika Anda mencoba membukanya.

Penyebab

.NET Framework 4.7.2 atau versi yang lebih tinggi masih belum diinstal pada komputer Anda. Ini diperlukan untuk menjalankan client.

Solusi

Jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

Client tidak dapat membuat profil

Masalah

Anda akan menemukan kesalahan berikut ketika Anda mencoba untuk membuat profil menggunakan klien yang disediakan oleh AWS .

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

Penyebab

Jika titik akhir Client VPN menggunakan autentikasi bersama, file (.ovpn) konfigurasi tidak berisi sertifikat dan kunci client.

Solusi

Pastikan bahwa administrator Client VPN Anda menambahkan sertifikat dan kunci client ke dalam file konfigurasi. Untuk informasi selengkapnya, lihat Ekspor Konfigurasi client dalam Panduan administrator AWS Client VPN .

Kecelakaan klien terjadi pada PC Dell menggunakan Windows 10 atau 11

Masalah

Pada PC Dell tertentu (desktop dan laptop) yang menjalankan Windows 10 atau 11, crash dapat terjadi ketika Anda menjelajahi sistem file Anda untuk mengimpor file konfigurasi VPN. Jika masalah ini terjadi, Anda akan melihat pesan seperti berikut di log klien yang AWS disediakan:

```
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()
```

Penyebab

Sistem Pencadangan dan Pemulihan Dell di Windows 10 dan 11 dapat menyebabkan konflik dengan klien yang AWS disediakan, terutama dengan tiga DLL berikut:

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

Solusi

Untuk menghindari masalah ini, pertama-tama pastikan bahwa klien Anda up to date dengan versi terbaru dari klien yang AWS disediakan. Buka unduhan AWS Client VPN dan jika versi yang lebih baru tersedia, tingkatkan ke versi terbaru.

Selain itu, lakukan salah satu hal berikut:

- Jika Anda menggunakan aplikasi Backup and Recovery Dell, pastikan itu up to date. Posting forum Dell menyatakan bahwa masalah ini diselesaikan di versi aplikasi yang lebih baru.
- Jika Anda tidak menggunakan aplikasi Backup and Recovery Dell, beberapa tindakan masih perlu diambil jika Anda mengalami masalah ini. Jika Anda tidak ingin memutakhirkan aplikasi, sebagai

alternatif, Anda dapat menghapus atau mengganti nama file DLL. Namun, perhatikan bahwa ini akan mencegah aplikasi Backup and Recovery Dell berfungsi sepenuhnya.

Hapus atau ganti nama file DLL

1. Buka Windows Explorer dan telusuri ke lokasi di mana Dell Backup and Recovery diinstal. Biasanya dipasang di lokasi berikut, tetapi Anda mungkin perlu mencari untuk menemukannya.

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

2. Hapus file DLL berikut secara manual dari direktori instalasi, atau ganti namanya. Tindakan apa pun akan mencegahnya dimuat.

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

   Anda dapat mengganti nama file dengan menambahkan “.bak” ke akhir nama file, misalnya, DBR OverlayIconBackuped .dll.bak.

VPN terputus dengan pesan pop up

Masalah

VPN terputus dengan pesan pop up yang mengatakan: “Koneksi VPN sedang dihentikan karena ruang alamat jaringan lokal yang terhubung dengan perangkat Anda telah berubah. Silakan buat koneksi VPN baru.”

Penyebab

Adaptor tap-Windows tidak berisi deskripsi yang diperlukan.

Solusi

Jika `Description` bidang tidak cocok di bawah ini, pertama-tama hapus adaptor TAP-Windows, lalu jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

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

```
Ethernet adapter Ethernet 2:

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

OpenVPN GUI

Informasi pemecahan masalah berikut diuji pada perangkat lunak OpenVPN GUI versi 11.10.0.0 dan 11.11.0.0 di Windows 10 Home (64-bit) dan Windows Server 2016 (64-bit).

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

OpenVPN mengoneksikan client

Informasi pemecahan masalah berikut diuji pada perangkat lunak OpenVPN Connect Client versi 2.6.0.100 dan 2.7.1.101 di Windows 10 Home (64-bit) dan Windows Server 2016 (64-bit).

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Tidak dapat me-resolve DNS

Masalah

Koneksi gagal dengan galat berikut.

```
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.
```

Penyebab

Nama DNS tidak dapat di-resolve. Cient harus menambahkan string acak ke nama DNS untuk mencegah caching DNS; namun, beberapa client tidak melakukan hal ini.

Solusi

Lihat solusi untuk masalah Tidak Dapat Me-resolve Nama DNS Titik Akhir Client VPN dalam Panduan administrator AWS Client VPN .

Alias PKI tidak ditemukan

Masalah

Koneksi ke titik akhir Client VPN yang tidak menggunakan autentikasi bersama gagal dikarenakan kesalahan berikut.

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

Penyebab

Terjadi masalah yang dikenali saat Perangkat lunak Klien OpenVPN Connect mencoba mengautentikasi menggunakan autentikasi bersama. Jika file konfigurasi tidak berisi kunci dan sertifikat client, autentikasi akan gagal.

Solusi

Tentukan kunci serta sertifikat client acak di dalam file konfigurasi Client VPN, dan impor konfigurasi baru ke dalam perangkat lunak OpenVPN Connect Client. Atau, gunakan klien yang berbeda, seperti OpenVPN GUI client (v11.12.0.0) atau Viscosity client (v.1.7.14).

Pemecahan masalah macOS

Bagian berikut berisi informasi tentang pencatatan log serta masalah yang mungkin Anda hadapi saat menggunakan macOS client. Pastikan bahwa Anda menjalankan versi terbaru client-client tersebut.

Topik

- AWS klien yang disediakan
- Tunnelblick
- OpenVPN

AWS klien yang disediakan

Klien yang AWS disediakan membuat log peristiwa dan menyimpannya di lokasi berikut di komputer Anda.

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

Jenis-jenis log berikut tersedia:

- Log aplikasi: Berisi informasi tentang aplikasi. Log-log ini diawali dengan 'aws_vpn_client_'.
- Log OpenVPN: Berisi informasi tentang proses OpenVPN. Log-log ini diawali dengan 'ovpn_aws_vpn_client_'.

Klien AWS yang disediakan menggunakan daemon klien untuk melakukan operasi root. Log-log daemon disimpan di dalam lokasi berikut di komputer Anda.

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

Klien yang AWS disediakan menyimpan file konfigurasi di lokasi berikut di komputer Anda.

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

Topik

- Client tidak dapat mengoneksikan
- Client berada dalam status mengoneksikan ulang.
- Client tidak dapat membuat profil

Client tidak dapat mengoneksikan

Masalah

Klien yang AWS disediakan tidak dapat terhubung ke titik akhir Client VPN.

Penyebab

Penyebab dari masalah berikut mungkin adalah salah satu dari hal-hal berikut:

- Proses OpenVPN lainnya sudah berjalan di komputer Anda, sehingga mencegah client untuk terkoneksi.
- File (.ovpn) konfigurasi milik Anda tidak valid.

Solusi

Periksa apakah ada aplikasi OpenVPN lain yang berjalan di komputer Anda. Jika ada, berhenti atau keluar dari proses-proses tersebut dan coba terkoneksi kembali ke titik akhir Client VPN. Periksa apakah terdapat galat log OpenVPN, dan minta administrator Client VPN Anda untuk memverifikasi informasi berikut:

- Bahwa file konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat Ekspor Konfigurasi client dalam Panduan administrator AWS Client VPN .
- CRL masih valid. Untuk informasi selengkapnya, lihat Klien Tidak Dapat Terhubung dengan Titik Akhir Client VPN dalam Panduan Administrator AWS Client VPN .

Client berada dalam status mengoneksikan ulang.

Masalah

Klien yang AWS disediakan mencoba untuk terhubung ke titik akhir Client VPN, tetapi terjebak dalam keadaan menyambung kembali.

Penyebab

Penyebab dari masalah berikut mungkin adalah sah satu dari hal-hal berikut:

- Komputer Anda tidak terkoneksi ke internet.
- DNS hostname tidak terhubung ke alamat IP.
- Proses OpenVPN merupakan upaya tanpa batas untuk terkoneksi dengan titik akhir.

Solusi

Verifikasi bahwa komputer Anda terkoneksi ke internet. Minta kepada administrator Client VPN Anda untuk memverifikasi bahwa direktif `remote` dalam file konfigurasi me-resolve ke alamat IP yang valid. Anda juga dapat memutuskan sambungan sesi VPN dengan memilih Putuskan sambungan di jendela Klien AWS VPN, dan coba sambungkan lagi.

Client tidak dapat membuat profil

Masalah

Anda akan menemukan kesalahan berikut ketika Anda mencoba untuk membuat profil menggunakan klien yang disediakan oleh AWS .

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

Penyebab

Jika titik akhir Client VPN menggunakan autentikasi bersama, file (.ovpn) konfigurasi tidak berisi sertifikat dan kunci client.

Solusi

Pastikan bahwa administrator Client VPN Anda menambahkan sertifikat dan kunci client ke dalam file konfigurasi. Untuk informasi selengkapnya, lihat Ekspor Konfigurasi client dalam Panduan administrator AWS Client VPN .

Tunnelblick

Informasi pemecahan masalah berikut telah diuji pada perangkat lunak Tunnelblick versi 3.7.8 (build 5180) di macOS High Sierra 10.13.6.

File konfigurasi untuk konfigurasi privat telah disimpan di dalam lokasi berikut di komputer Anda.

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

File konfigurasi untuk konfigurasi bersama disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Untuk meningkatkan log yang bertele-tele, buka aplikasi Tunnelblick, pilih Pengaturan, dan sesuaikan nilai untuk Tingkat log VPN.

Algoritme sandi 'AES-256-GCM' tidak dapat ditemukan

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam 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
```

Penyebab

Aplikasi ini menggunakan versi OpenVPN yang tidak dapat mendukung algoritme sandi AES-256-GCM.

Solusi

Pilih versi OpenVPN yang kompatibel dengan melakukan hal berikut:

1. Buka aplikasi Tunnelblick.
2. Pilih Pengaturan.
3. Untuk Versi OpenVPN, pilih 2.4.6 - Versi OpenSSL adalah v1.0.2q.

Koneksi berhenti merespons dan mengatur ulang

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam 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
```

Penyebab

Sertifikat client telah dicabut. Koneksi berhenti merespons setelah berupaya untuk mengautentikasi dan mengatur ulang dari sisi server.

Solusi

Ajukan permintaan untuk file konfigurasi baru dari administrator Client VPN Anda.

Penggunaan kunci yang diperpanjang (EKU)

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam 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,,,,,
```

Penyebab

Autentikasi server telah berhasil. Namun, autentikasi client gagal karena sertifikat client memuat bidang penggunaan kunci yang diperpanjang (EKU) yang diaktifkan untuk autentikasi server.

Solusi

Verifikasi bahwa Anda sedang menggunakan sertifikat dan kunci klien yang benar. Jika diperlukan, verifikasi dengan administrator Client VPN milik Anda. Galat ini dapat terjadi jika Anda menggunakan sertifikat server dan bukan sertifikat client untuk mengoneksikan jaringan ke titik akhir Client VPN.

Sertifikat sudah kedaluwarsa

Masalah

Autentikasi server berhasil, namun autentikasi client gagal dengan galat berikut.

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

Penyebab

Validitas sertifikat client telah kedaluwarsa.

Solusi

Ajukan permintaan untuk sertifikat klien yang baru dari administrator Client VPN Anda.

OpenVPN

Informasi pemecahan masalah berikut telah diuji pada perangkat lunak OpenVPN Connect Client versi 2.7.1.100 di macOS High Sierra 10.13.6.

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

DNS tidak dapat di-resolve

Masalah

Koneksi gagal dengan galat berikut.

```
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
```

Penyebab

OpenVPN Connect tidak dapat me-resolve nama DNS Client VPN.

Solusi

Lihat solusi untuk Tidak Dapat Me-resolve Nama DNS Titik Akhir Client VPN dalam Panduan administrator AWS Client VPN .

Pemecahan masalah Linux

Bagian berikut berisi informasi tentang pencatatan, dan masalah yang mungkin Anda temui saat menggunakan client berbasis Linux. Pastikan bahwa Anda menjalankan client versi terbaru.

Topik

- AWS klien yang disediakan
- OpenVPN (baris perintah)
- OpenVPN melalui Pengelola Jaringan (GUI)

AWS klien yang disediakan

Klien yang AWS disediakan menyimpan file log dan file konfigurasi di lokasi berikut di sistem Anda:

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

Proses daemon klien yang AWS disediakan menyimpan file log di lokasi berikut di sistem Anda:

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

Masalah

Di beberapa situasi setelah koneksi VPN dibuat, kueri DNS akan tetap masuk ke dalam nameserver sistem default, bukan nameserver yang dikonfigurasi untuk titik akhir ClientVPN.

Penyebab

Klien berinteraksi dengan systemd-resolved, layanan yang tersedia pada sistem Linux, yang berfungsi sebagai bagian utama dari manajemen DNS. Ini digunakan untuk mengonfigurasi server DNS yang telah didorong dari titik akhir ClientVPN. Masalah ini terjadi karena systemd-resolved tidak dapat menetapkan prioritas tertinggi ke server DNS yang disediakan oleh titik akhir ClientVPN. Sebaliknya, ia menambahkan server ke daftar server DNS yang sudah ada yang dikonfigurasi pada sistem lokal. Akibatnya, server DNS asli mungkin masih memiliki prioritas tertinggi, dan karena itu digunakan untuk me-resolve kueri DNS.

Solusi

1. Tambahkan arahan berikut pada baris pertama file konfigurasi OpenVPN, untuk memastikan bahwa semua kueri DNS dikirim ke terowongan VPN.

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

2. Gunakan stub resolver yang disediakan oleh systemd-resolved. Untuk dapat melakukannya, symlink `/etc/resolv.conf` ke `/run/systemd/resolve/stub-resolv.conf` dengan menjalankan perintah berikut pada sistem.

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

3. (Opsional) Jika Anda tidak ingin systemd-resolved menjalankan proxy kueri DNS, dan sebagai gantinya ingin kueri dikirim ke server nama DNS asli secara langsung, symlink `/etc/resolv.conf` ke `/run/systemd/resolve/resolv.conf` sebagai gantinya.

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

   Anda mungkin ingin melakukan prosedur ini untuk melewati konfigurasi systemd-resolved, misalnya untuk caching jawaban DNS, konfigurasi DNS per-antarmuka, pelaksanaan DNSSec, dan sebagainya. Opsi ini sangat berguna ketika Anda memiliki kebutuhan untuk meng-override catatan DNS publik dengan catatan privat saat terkoneksi ke VPN. Misalnya, mungkin Anda memiliki DNS resolver privat di VPC privat Anda dengan sebuah catatan untuk www.example.com, yang dapat me-resolve ke IP privat. Opsi ini dapat digunakan untuk meng-override catatan publik www.example.com, yang me-resolve ke IP publik.

OpenVPN (baris perintah)

Masalah

Koneksi tidak berfungsi dengan benar karena resolusi DNS tidak bekerja.

Penyebab

Server DNS tidak dikonfigurasikan pada titik akhir Client VPN, atau tidak dianggap oleh perangkat lunak klien.

Solusi

Gunakan langkah-langkah berikut untuk memeriksa bahwa server DNS telah dikonfigurasi dan bekerja dengan benar.

1. Pastikan bahwa entri server DNS muncul di dalam log. Pada contoh berikut, `192.168.0.2` server DNS (dikonfigurasi di dalam titik akhir Client VPN) telah dikembalikan di baris terakhir.

   ```
   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
   ```

   Jika tidak ada server DNS yang ditentukan, minta kepada administrator Client VPN Anda untuk mengubah titik akhir Client VPN serta pastikan bahwa server DNS (misalnya, server VPC DNS) telah ditentukan untuk titik akhir Client VPN. Untuk informasi selengkapnya, lihat Titik akhir Client VPN dalam Panduan administrator AWS Client VPN .
2. Pastikan bahwa paket `resolvconf` telah diinstal dengan menjalankan perintah berikut.

   ```
   sudo apt list resolvconf
   ```

   Output akan mengembalikan hal-hal berikut.

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

   Jika tidak diinstal, instal paket dengan menggunakan perintah berikut.

```
sudo apt install resolvconf
```

3. Buka file konfigurasi Client VPN (file .ovpn) di teks editor dan tambahkan Anda baris berikut.

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

Periksa log untuk memverifikasi bahwa skrip `resolvconf` telah diminta. Log harus berisi baris yang serupa dengan baris berikut.

```
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 melalui Pengelola Jaringan (GUI)

Masalah

Ketika menggunakan client Pengelola Jaringan OpenVPN, koneksi gagal dengan galat berikut.

```
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
```

Penyebab

Tanda `remote-random-hostname` tidak diperhitungkan, dan klien tidak dapat membuat hubungan menggunakan paket `network-manager-gnome`.

Solusi

Lihat solusi untuk Tidak Dapat Me-resolve Nama DNS Titik Akhir Client VPN dalam Panduan administrator AWS Client VPN .

Permasalahan umum

Berikut ini adalah masalah umum yang mungkin Anda hadapi ketika menggunakan client untuk terkoneksi ke titik akhir Client VPN.

Negosiasi kunci TLS gagal

Masalah

Negosiasi TLS gagal dengan galat berikut.

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

Penyebab

Penyebab dari masalah ini mungkin adalah salah satu dari hal-hal berikut:

- Aturan firewall memblokir lalu lintas UDP atau TCP.
- Anda menggunakan kunci dan sertifikat klien yang salah di dalam file (.ovpn) konfigurasi.
- Daftar pencabutan sertifikat client (CRL) telah kedaluwarsa.

Solusi

Periksa apakah aturan firewall di komputer Anda telah memblokir lalu lintas masuk atau keluar TCP atau UDP pada port 443 atau 1194. Minta administrator Client VPN Anda untuk memverifikasi informasi berikut:

- Bahwa aturan firewall untuk titik akhir Client VPN tidak memblokir lalu lintas TCP atau UDP pada port 443 atau 1194.
- File konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat Ekspor Konfigurasi client dalam Panduan administrator AWS Client VPN .
- CRL masih valid. Untuk informasi selengkapnya, lihat Klien Tidak Dapat Terhubung dengan Titik Akhir Client VPN dalam Panduan Administrator AWS Client VPN .

Riwayat dokumen

Tabel berikut menjelaskan pembaruan Panduan Pengguna AWS Client VPN.

Perubahan	Deskripsi	Tanggal
AWS klien yang disediakan (3.13.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.12.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.10.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.9.2) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024
AWS klien yang disediakan (3.12.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024
AWS klien yang disediakan (3.11.2) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024
AWS klien yang disediakan (3.9.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.12.1) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.11.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.12.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Desember 19, 2023
AWS klien yang disediakan (3.9.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023

AWS klien yang disediakan (3.11.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.11.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.10.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.9.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023
AWS klien yang disediakan (3.10.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023
AWS klien yang disediakan (3.9.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.7.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.7.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.7.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.6.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023

AWS klien yang disediakan (3.6.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.5.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.6.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.5.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.4.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.3.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	27 April 2023
AWS klien yang disediakan (3.5.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 April 2023
AWS klien yang disediakan (3.4.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Maret 28, 2023
AWS klien yang disediakan (3.3.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Maret 17, 2023
AWS klien yang disediakan (3.4.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	14 Februari 2023
AWS klien yang disediakan (3.2.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	23 Januari 2023
AWS klien yang disediakan (3.2.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	23 Januari 2023
AWS klien yang disediakan (3.1.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022

AWS klien yang disediakan (3.1.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022
AWS klien yang disediakan (3.1.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022
AWS klien yang disediakan (3.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (3.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (3.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (2.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022
AWS klien yang disediakan (2.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022
AWS klien yang disediakan (2.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022
AWS klien yang disediakan (1.4.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	November 9, 2021
AWS klien yang disediakan untuk Windows (1.3.7) dirilis	Lihat catatan rilis untuk detailnya.	November 8, 2021
AWS klien yang disediakan (1.0.3) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	November 8, 2021
AWS klien yang disediakan (1.0.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2021
AWS klien yang disediakan untuk Windows (1.3.6) dan macOS (1.3.5) dirilis	Lihat catatan rilis untuk detailnya.	September 20, 2021

AWS klien yang disediakan untuk Ubuntu 18.04 LTS dan Ubuntu 20.04 LTS dirilis	Anda dapat menggunakan klien yang AWS disediakan di Ubuntu 18.04 LTS dan Ubuntu 20.04 LTS.	11 Juni 2021
Support untuk OpenVPN menggunakan sertifikat dari Windows Certificate System Store	Anda dapat menggunakan OpenVPN dengan sertifikat dari Penyimpanan Sistem Sertifikat Windows.	25 Februari 2021
Portal swalayan	Anda dapat mengakses portal swalayan untuk mendapatkan klien dan file konfigurasi terbaru yang AWS disediakan.	29 Oktober 2020
AWS klien yang disediakan	Anda dapat menggunakan klien yang AWS disediakan untuk terhubung ke titik akhir Client VPN.	4 Februari 2020
Rilis awal	Rilis ini memperkenalkan AWS Client VPN.	18 Desember 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.