Panduan Pengguna

AWS Client VPN

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Client VPN: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS VPN klien? 1
Komponen VPN klien 1
Sumber daya tambahan untuk mengonfigurasi VPN Klien 2
Memulai dengan Client VPN 3
Prasyarat untuk menggunakan Client VPN 3
Langkah 1: Dapatkan aplikasi klien VPN 4
Langkah 2: Dapatkan file konfigurasi titik akhir Client VPN 4
Langkah 3: Hubungkan ke VPN 4
Unduh Client VPN 5
Hubungkan menggunakan AWS klien yang disediakan 7
Keamanan 7
Pembaruan 8
Perintah CLI 8
Kontrol admin 8
Sintaks perintah CLI 9
hubungkan 10
memutuskan 11
import-profil 12
hapus profil 13
list-profil 14
get-config 15
dapatkan status koneksi 16
daftar koneksi 18
put-preferensi 19
daftar preferensi 21
kirim log-diagnostik 21
Kode keluar 22
Dukungan untuk koneksi bersamaan 22
Menghubungkan dengan postur perangkat 23
Pengaturan penyedia kepercayaan perangkat 24
Prasyarat 24
CrowdStrike 24
Jamf 25
JumpCloud 25

Apa yang diharapkan 25
Arahan OpenVPN 26
Windows 27
Persyaratan 27
Catatan Rilis 29
macOS 45
Persyaratan 45
Catatan Rilis 46
Linux 62
Persyaratan untuk menghubungkan ke VPN Klien dengan AWS disediakan klien untuk Linux 62
Instal klien 63
Catatan Rilis 64
Hubungkan menggunakan klien 70
Versi 6.0 dan yang lebih baru 70
Versi sebelumnya 72
Kompatibilitas keamanan titik akhir 73
AWS Jalur yang dapat dieksekusi VPN klien 73
Persyaratan jaringan 77
Mengkonfigurasi pengecualian keamanan titik akhir 77
Hubungkan menggunakan klien OpenVPN 79
Windows 80
Buat koneksi VPN menggunakan sertifikat di Windows 80
macOS 82
Buat koneksi VPN di macOS 83
Linux 83
Buat koneksi VPN di Linux 84
Koneksi VPN klien di Android dan iOS 85
Pemecahan Masalah 86
Pemecahan masalah titik akhir Client VPN untuk administrator 86
Kirim log diagnostik ke AWS Dukungan di AWS klien yang disediakan 86
Kirim log diagnostik (versi 6.0 dan yang lebih baru) 87
Mengirim log diagnostik (versi lebih awal dari 6.0) 87
Pemecahan masalah Windows 88
AWS menyediakan log peristiwa klien 88
Profil atau preferensi hilang setelah upgrade ke versi 6.0 90

Koneksi tetap aktif saat rute VPN tumpang tindih dengan IP titik akhir 90
Client tidak dapat mengoneksikan 91
Klien tidak dapat terhubung dengan “tidak TAP-Windows adaptor” pesan log 92
Client berada dalam status mengoneksikan ulang. 92
Proses koneksi VPN berhenti secara tiba-tiba 93
Aplikasi gagal diluncurkan 93
Client tidak dapat membuat profil 93
VPN terputus dengan pesan pop up 94
Kerusakan klien terjadi pada PC Dell menggunakan Windows 10 atau 11 94
OpenVPN GUI 96
OpenVPN mengoneksikan client 96
Tidak dapat me-resolve DNS 97
Alias PKI tidak ditemukan 97
Pemecahan masalah macOS 98
AWS menyediakan log peristiwa klien 98
Profil atau preferensi hilang setelah upgrade ke versi 6.0 99
Instalasi gagal saat menurunkan versi dari versi 6.0 atau yang lebih baru 100
Client tidak dapat mengoneksikan 100
Client berada dalam status mengoneksikan ulang. 101
Client tidak dapat membuat profil 102
Alat pembantu diperlukan kesalahan 102
Pemandangan terowongan 102
Algoritma cipher 'AES-256-GCM'tidak ditemukan 103
Koneksi berhenti merespons dan mengatur ulang 103
Penggunaan kunci yang diperpanjang (EKU) 104
Sertifikat sudah kedaluwarsa 105
OpenVPN 105
DNS tidak dapat di-resolve 105
Pemecahan masalah Linux 106
AWS menyediakan log peristiwa klien 88
Profil atau preferensi hilang setelah upgrade ke versi 6.0 107
Kueri DNS masuk ke server nama default 108
OpenVPN (baris perintah) 109
OpenVPN melalui Pengelola Jaringan (GUI) 110
Permasalahan umum 111
Negosiasi kunci TLS gagal 111

Riwayat dokumen 113
..... cxxvi

Apa itu AWS VPN klien?

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

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

> **Note**
>
> Beberapa titik akhir VPN Klien memerlukan postur perangkat, yang memeriksa kesehatan perangkat Anda sebelum dan selama sesi. Untuk terhubung ke titik akhir berpintu postur, Anda harus menggunakan AWS klien yang disediakan, versi 6.2.0 atau yang lebih baru, dan penyedia kepercayaan perangkat organisasi Anda — seperti CrowdStrike, Jamf, atau JumpCloud — harus diatur pada perangkat Anda.

Komponen VPN klien

Berikut ini adalah komponen kunci untuk menggunakan AWS VPN klien.

- 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 VPN Klien dan sertifikat yang diperlukan untuk membuat koneksi VPN. Anda memuat file ini ke aplikasi klien VPN pilihan Anda. The AWS klien yang disediakan memungkinkan Anda untuk terhubung ke lima sesi bersamaan, setiap sesi dengan file konfigurasi sendiri yang disediakan oleh administrator VPN Klien. Untuk informasi selengkapnya tentang sesi bersamaan, lihat Dukungan untuk koneksi bersamaan.

Sumber daya tambahan untuk mengonfigurasi VPN Klien

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

Memulai dengan AWS 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 menggunakan Client VPN
- Langkah 1: Dapatkan aplikasi klien VPN
- Langkah 2: Dapatkan file konfigurasi titik akhir Client VPN
- Langkah 3: Hubungkan ke VPN
- Unduh AWS Client VPN dari portal swalayan

Prasyarat untuk menggunakan Client VPN

Untuk membuat koneksi VPN, Anda harus melakukan hal berikut:

- Mengakses ke internet
- Perangkat yang didukung
- Versi Windows, macOS, atau Linux 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.

Anda dapat mengunduh aplikasi Client VPN melalui salah satu dari dua metode, tergantung pada apakah administrator membuat file konfigurasi titik akhir untuk aplikasi:

- Jika administrator Anda tidak menyiapkan file konfigurasi titik akhir, unduh dan instal klien dari unduhan AWS Client VPN. Setelah mengunduh dan menginstal aplikasi, lanjutkan the section called “Langkah 2: Dapatkan file konfigurasi titik akhir Client VPN” untuk mendapatkan file konfigurasi titik akhir dari administrator Anda. Jika Anda terhubung ke beberapa profil, Anda memerlukan file konfigurasi untuk setiap profil.
- Jika administrator Anda telah mengkonfigurasi file konfigurasi titik akhir, Anda dapat mengunduh aplikasi Client VPN, bersama dengan file konfigurasi, dari portal swalayan. Untuk langkah-langkah mengunduh file klien dan konfigurasi dari portal swalayan, lihatthe section called “Unduh Client VPN”. Setelah mengunduh dan menginstal aplikasi dan file, bukathe section called “Langkah 3: Hubungkan ke 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 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.

Atau, jika administrator Client VPN Anda telah mengonfigurasi portal swalayan untuk titik akhir Client VPN, Anda dapat mengunduh versi terbaru dari klien yang AWS disediakan dan versi terbaru dari file konfigurasi titik akhir Client VPN sendiri. Untuk informasi selengkapnya, lihat Unduh AWS Client VPN dari portal swalayan.

Langkah 3: Hubungkan ke VPN

Impor file konfigurasi titik akhir Client VPN ke klien yang AWS disediakan atau ke aplikasi klien OpenVPN Anda dan sambungkan ke VPN. Untuk langkah-langkah untuk terhubung ke VPN,

termasuk mengimpor satu atau beberapa file konfigurasi titik akhir untuk klien yang AWS disediakan, lihat topik berikut:

- Hubungkan ke AWS Client VPN titik akhir menggunakan AWS klien yang disediakan
- Hubungkan ke AWS Client VPN titik akhir 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 otentikasi federasi berbasis SAML (single sign-on), klien yang AWS disediakan membuka jendela browser di komputer Anda. Anda akan diminta untuk memasukkan kredensial perusahaan Anda sebelum terhubung ke titik akhir Client VPN.

Unduh AWS Client VPN dari portal swalayan

Portal swalayan adalah halaman web yang memungkinkan Anda mengunduh versi terbaru dari klien yang AWS disediakan dan versi terbaru dari file konfigurasi titik akhir Client VPN. Jika administrator titik akhir Client VPN Anda telah mengkonfigurasi satu atau lebih file konfigurasi untuk klien Client VPN, Anda dapat mengunduh dan menginstal aplikasi Client VPN itu bersama dengan file konfigurasi tersebut, dari portal ini.

> **Note**
>
> Jika Anda seorang administrator dan ingin mengonfigurasi portal layanan mandiri, lihat Titik akhir Client VPN di Panduan AWS Client VPN Administrator.

Sebelum memulai, Anda harus memiliki ID dari setiap titik akhir Client VPN yang ingin Anda unduh Administrator endpoint VPN Klien Anda dapat memberi Anda ID, atau dapat memberi Anda URL portal swalayan yang menyertakan ID. Untuk beberapa koneksi titik akhir, Anda memerlukan ID titik akhir untuk setiap profil yang ingin Anda sambungkan.

Untuk mengakses portal layanan mandiri

1. Buka portal swalayan di https://self-service.clientvpn.amazonaws.com/, atau gunakan URL yang diberikan kepada Anda 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. Jika Anda ingin terhubung ke beberapa titik akhir, Anda harus mengunduh file konfigurasi untuk setiap titik akhir.
   - Unduh versi terbaru dari klien yang AWS disediakan untuk platform Anda.
5. Ulangi langkah-langkah ini untuk setiap file konfigurasi titik akhir yang ingin Anda buat profil koneksi.

Hubungkan ke AWS Client VPN titik akhir menggunakan AWS klien yang disediakan

Anda dapat terhubung ke titik akhir VPN Klien menggunakan AWS disediakan klien, yang didukung pada Windows, macOS, dan Ubuntu. Anda dapat menggunakan klien dalam dua cara — melalui antarmuka pengguna grafis (GUI) atau antarmuka baris perintah (CLI). Yang AWS klien yang disediakan juga mendukung hingga lima koneksi bersamaan serta arahan OpenVPN.

Topik

- Pembaruan
- Perintah CLI
- Kontrol admin
- Dukungan untuk koneksi bersamaan
- Menghubungkan dengan postur perangkat
- Arahan OpenVPN

Keamanan

Keamanan adalah prioritas tertinggi di AWS klien yang disediakan. Kami secara teratur merilis patch untuk meningkatkan postur keamanan aplikasi. Klien yang disediakan AWS mencakup beberapa fitur keamanan unik dibandingkan dengan klien OpenVPN lainnya, termasuk otentikasi SAML, Penegakan Rute Klien, dan pemantauan pengaturan perangkat.

Sementara AWS asalkan klien dirancang untuk mengurangi ancaman yang berasal dari lingkungan jaringan yang salah konfigurasi atau terganggu, tidak bertanggung jawab untuk memodifikasi lingkungan atau menghilangkan ancaman eksternal pada sumbernya. Yang AWS asalkan klien bergantung pada pelanggan untuk mempertahankan lingkungan yang aman dan terkonfigurasi dengan baik. Hal ini mencakup:

- Mencegah modifikasi atau penyalahgunaan yang tidak sah oleh pengguna lokal
- Membatasi hak administratif untuk pengguna tepercaya
- Mempertahankan patch keamanan terkini

Pembaruan perangkat lunak

Kami menyarankan Anda selalu menjalankan versi terbaru dari AWS menyediakan klien untuk menerima fitur terbaru dan patch keamanan.

Pada Windows dan macOS, AWS klien disediakan secara otomatis memeriksa versi yang lebih baru dan, ketika tersedia, menampilkan pemberitahuan yang meminta Anda untuk memperbarui. Ikuti prompt untuk menginstal pembaruan.

Di Ubuntu, AWS klien yang disediakan untuk Linux tidak secara otomatis memeriksa pembaruan. Kami menyarankan Anda menginstal klien melalui repositori paket dan memperbaruinya dari sana. Untuk informasi selengkapnya, lihat the section called “Instal klien”.

Hubungkan menggunakan antarmuka baris perintah

Yang AWS Client VPN Command Line Interface (CLI) menyediakan antarmuka yang ringan dan dapat ditulis untuk mengelola profil dan koneksi VPN. CLI tersedia di Windows, macOS, dan Linux, dan memungkinkan administrator perusahaan untuk mengotomatiskan penerapan VPN, mengelola profil dalam skala besar, dan mengintegrasikan VPN Klien dengan infrastruktur manajemen yang ada.

Alat CLI diberi nama `aws-vpn-client` dan dipasang di samping AWS disediakan klien dari versi 6.0 dan seterusnya.

CLI menyediakan akses ke semua fitur aplikasi klien, termasuk manajemen profil, manajemen koneksi, dan konfigurasi administratif.

Untuk detail tentang perintah dan sintaks CLI, lihat Sintaks perintah CLI.

Kontrol administratif

AWS Kontrol administratif VPN klien menyediakan pengaturan konfigurasi global dan kemampuan manajemen profil yang memungkinkan administrator mengelola penerapan klien VPN dalam skala besar.

Dengan kontrol administratif, administrator dapat:

- Kontrol izin manajemen profil untuk pengguna akhir
- Tetapkan jumlah maksimum koneksi bersamaan

- Impor profil secara global untuk semua pengguna di perangkat
- Kelola pengaturan telemetri

Untuk menjalankan perintah administratif, Anda memerlukan hak istimewa yang ditingkatkan (sudo on macOS/Linux, administrator di Windows).

Anda dapat menggunakan pengaturan preferensi berikut dengan `aws-vpn-client put-preference`:

Kelola preferensi

> Gunakan `aws-vpn-client put-preference` dengan hak istimewa yang ditingkatkan untuk mengatur nilai konfigurasi global seperti `max-connections`, `enable-user-profile-management`, dan `enable-telemetry`.

Selain itu, Anda dapat mengimpor profil secara global untuk semua pengguna di perangkat dengan menggunakan `aws-vpn-client import-profile` dengan `--global` bendera dan hak istimewa yang ditinggikan.

Untuk daftar lengkap perintah dan sintaks CLI, lihat Sintaks perintah CLI.

Sintaks perintah CLI

Anda dapat menggunakan perintah CLI dengan menggunakan sintaks berikut:

```
aws-vpn-client <COMMAND> [OPTIONS]
```

Alat CLI mendukung perintah berikut.

```
Usage: aws-vpn-client <COMMAND>

Commands:
  connect               Connect a profile through the AWS VPN Client
  disconnect            Disconnect a profile from the AWS VPN Client
  delete-profile        Delete a profile from the AWS VPN Client
  import-profile        Import a VPN connection profile
  list-profiles         List all VPN profiles
  get-config            Get configuration for a profile
  put-preference        Put a preference value
```

```
  list-preferences       List all preferences
  get-connection-status  Get the current connection status for a VPN profile
  list-connections       List all active VPN connections
  send-diagnostic-logs   Send diagnostic logs to AWS for troubleshooting
  help                   Print this message or the help of the given subcommand(s)

Options:
  -h, --help     Print help
  -V, --version  Print version
```

hubungkan

Deskripsi

Buat koneksi VPN ke profil.

Sinopsis

```
aws-vpn-client connect
  --profile-name <PROFILE>
  [--auth-user-pass <AUTH_USER_PASS>]
```

Opsi

`--profile-name`(string)

Nama profil untuk terhubung. Opsi ini diperlukan.

`--auth-user-pass`(string)

Jalur ke file yang berisi nama pengguna (baris 1), kata sandi (baris 2), dan kode MFA opsional (baris 3). Opsi ini tidak diperlukan.

Contoh

Contoh: Sambungkan ke profil VPN

`connect`Contoh berikut membuat koneksi VPN ke profil.

```
aws-vpn-client connect --profile-name "Production-VPN"
```

Output:

```
{
  "status": "Connected"
}
```

memutuskan

Deskripsi

Hentikan koneksi VPN aktif.

Sinopsis

```
aws-vpn-client disconnect
  --profile-name <PROFILE_NAME>
```

Opsi

`--profile-name`(string)

Nama profil yang terhubung untuk memutuskan sambungan. Opsi ini diperlukan.

Contoh

Contoh: Putuskan sambungan dari profil VPN

`disconnect`Contoh berikut mengakhiri koneksi VPN. Tidak ada output dari kesuksesan.

```
aws-vpn-client disconnect --profile-name "Production-VPN"
```

Contoh: Kesalahan pemutusan

`disconnect`Contoh berikut menunjukkan kesalahan saat profil tidak terhubung.

```
aws-vpn-client disconnect --profile-name "Production-VPN"
```

Output:

```
{
```

```
  "status": "Error",
  "message": "Profile is not connected"
}
```

import-profil

Deskripsi

Impor profil koneksi VPN.

Sinopsis

```
aws-vpn-client import-profile
  --profile-name <PROFILE_NAME>
  --config-path <CONFIG_PATH>
  [--global]
```

Opsi

`--profile-name`(string)

Nama khusus untuk profil yang diimpor. Opsi ini diperlukan.

`--config-path`(string)

Jalur ke file konfigurasi OpenVPN (.ovpn). Opsi ini diperlukan.

`--global`(boolean)

Impor sebagai profil global yang tersedia untuk semua pengguna. Opsi ini memerlukan hak administrator.

Contoh

Contoh: Mengimpor profil

`import-profile`Contoh berikut mengimpor profil koneksi VPN.

```
aws-vpn-client import-profile --profile-name "Production-VPN" --config-path /path/to/
vpn-config.ovpn
```

Output:

```
{
  "status": "Success"
}
```

Contoh: Mengimpor profil global

`import-profile`Contoh berikut mengimpor profil global. Ini membutuhkan hak administrator.

```
sudo aws-vpn-client import-profile --profile-name "Company-VPN" --config-path /path/to/
config.ovpn --global
```

Output:

```
{
  "status": "Success"
}
```

Contoh: Kesalahan impor dengan jalur file yang tidak valid

`import-profile`Contoh berikut menunjukkan kesalahan ketika file konfigurasi tidak ditemukan.

```
aws-vpn-client import-profile --profile-name "test" --config-path /invalid/path.ovpn
```

Output:

```
{
  "status": "Error",
  "message": "Failed to read OpenVPN config file: No such file or directory (os error
 2)"
}
```

hapus profil

Deskripsi

Hapus profil dari klien.

Sinopsis

```
aws-vpn-client delete-profile
```

```
  --profile-name <PROFILE_NAME>
```

Opsi

`--profile-name`(string)

Nama profil yang akan dihapus. Opsi ini diperlukan.

Contoh

Contoh: Menghapus profil

`delete-profile`Contoh berikut menghapus profil VPN. Tidak ada output dari kesuksesan.

```
aws-vpn-client delete-profile --profile-name "Production-VPN"
```

Contoh: Hapus kesalahan dengan profil yang tidak ada

`delete-profile`Contoh berikut menunjukkan kesalahan ketika profil tidak ada.

```
aws-vpn-client delete-profile --profile-name "nonexistent"
```

Output:

```
{
  "status": "Error",
  "message": "Profile not found"
}
```

list-profil

Deskripsi

Daftar semua profil VPN.

Sinopsis

```
aws-vpn-client list-profiles
```

Contoh

Contoh: Daftar semua profil VPN

`list-profiles`Contoh berikut mencantumkan semua profil VPN yang diimpor.

```
aws-vpn-client list-profiles
```

Output:

```
[
  {
    "profile-name": "Production-VPN",
    "owned-by": "jdoe",
    "auth-type": "saml",
    "imported-at": "2026-07-21T13:04:42-07:00"
  },
  {
    "profile-name": "Staging-VPN",
    "owned-by": "jdoe",
    "auth-type": "ma",
    "imported-at": "2026-07-22T10:30:00-07:00"
  }
]
```

> **Note**
>
> Profil global (diimpor dengan`--global`) tidak memiliki `owned-by` bidang.

get-config

Deskripsi

Ambil konfigurasi OpenVPN untuk profil.

Sinopsis

```
aws-vpn-client get-config
```

```
  --profile-name <PROFILE_NAME>
```

Opsi

`--profile-name`(string)

Nama profil untuk mengambil konfigurasi. Opsi ini diperlukan.

Contoh

Contoh: Ambil konfigurasi OpenVPN

`get-config`Contoh berikut mengambil konfigurasi OpenVPN untuk profil.

```
aws-vpn-client get-config --profile-name "Production-VPN"
```

Output:

```
client
dev tun
proto udp
remote cvpn-endpoint-0123456789abcdef0.prod.clientvpn.us-east-1.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3
<ca>
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
</ca>
auth-user-pass
reneg-sec 0
```

dapatkan status koneksi

Deskripsi

Dapatkan status koneksi saat ini untuk profil VPN.

Sinopsis

```
aws-vpn-client get-connection-status
  --profile-name <PROFILE_NAME>
  [--show-details]
```

Opsi

`--profile-name`(string)

Nama profil untuk mengambil status koneksi. Opsi ini diperlukan.

`--show-details`(boolean)

Sertakan statistik byte koneksi dalam output.

Contoh

Contoh: Dapatkan status koneksi

`get-connection-status`Contoh berikut mengambil status koneksi untuk profil.

```
aws-vpn-client get-connection-status --profile-name "Production-VPN"
```

Output:

```
{
  "connection-status": "Connected",
  "latest-connection-attempt": {
    "initiated-by": "jdoe",
    "updated-at": "2026-07-24T15:50:36-07:00"
  }
}
```

Contoh: Dapatkan status koneksi dengan detail

`get-connection-status`Contoh berikut mencakup statistik byte dengan menggunakan `--show-details` opsi.

```
aws-vpn-client get-connection-status --profile-name "Production-VPN" --show-details
```

Output:

```
{
  "connection-status": "Connected",
  "latest-connection-attempt": {
    "initiated-by": "jdoe",
    "updated-at": "2026-07-24T15:50:36-07:00",
    "details": {
      "tunnel-bytes-in": 0,
      "tunnel-bytes-out": 0,
      "transport-bytes-in": 9674,
      "transport-bytes-out": 11413
    }
  }
}
```

daftar koneksi

Deskripsi

Daftar semua koneksi VPN aktif.

Sinopsis

```
aws-vpn-client list-connections
```

Contoh

Contoh: Daftar koneksi aktif

`list-connections`Contoh berikut mencantumkan semua koneksi VPN aktif.

```
aws-vpn-client list-connections
```

Output:

```
[
  {
    "profile-name": "Production-VPN",
    "initiated-by": "jdoe",
    "connection-status": "Connected",
```

```
    "last-updated-at": "2026-07-24T15:50:36-07:00"
  }
]
```

Contoh: Tidak ada koneksi aktif

`list-connections`Contoh berikut menunjukkan output ketika tidak ada koneksi aktif.

```
aws-vpn-client list-connections
```

Output:

```
[]
```

put-preferensi

Deskripsi

Tetapkan preferensi konfigurasi global. Sebagian besar pengaturan memerlukan hak administrator.

Sinopsis

```
aws-vpn-client put-preference
  --key <PREFERENCE_KEY>
  --value <PREFERENCE_VALUE>
```

Opsi

`--key`(string)

Nama kunci preferensi untuk disetel. Opsi ini diperlukan.

`--value`(string)

Nilai yang akan ditetapkan untuk kunci preferensi. Opsi ini diperlukan.

Kunci preferensi berikut tersedia:

`enable-telemetry`

Mengaktifkan atau menonaktifkan telemetri (true/false).

`enable-user-profile-management`

Mengizinkan atau melarang pengguna akhir untuk mengimpor atau menghapus profil (true/false).

`max-connections`

Jumlah maksimum koneksi bersamaan (integer, 1-5).

Contoh

Contoh: Tetapkan preferensi

`put-preference`Contoh berikut menetapkan jumlah koneksi maksimum. Ini membutuhkan hak administrator. Tidak ada output dari kesuksesan.

```
sudo aws-vpn-client put-preference --key max-connections --value 4
```

Contoh: Kesalahan tanpa hak administrator

`put-preference`Contoh berikut menunjukkan kesalahan saat Anda menjalankan perintah tanpa hak administrator.

```
aws-vpn-client put-preference --key max-connections --value 4
```

Output:

```
{
  "status": "Error",
  "message": "Permission denied: admin privileges required"
}
```

Contoh: Kesalahan dengan nilai tidak valid

`put-preference`Contoh berikut menunjukkan kesalahan saat Anda memberikan nilai yang tidak valid.

```
sudo aws-vpn-client put-preference --key max-connections --value 8
```

Output:

```
{
```

```
  "status": "Error",
  "message": "Preference value is invalid"
}
```

daftar preferensi

Deskripsi

Tampilkan semua preferensi konfigurasi global dan nilai saat ini.

Sinopsis

```
aws-vpn-client list-preferences
```

Contoh

Contoh: Daftar semua preferensi

`list-preferences`Contoh berikut menampilkan semua preferensi konfigurasi global dan nilainya saat ini.

```
aws-vpn-client list-preferences
```

Output:

```
{
  "enable-telemetry": true,
  "enable-user-profile-management": true,
  "max-connections": 1
}
```

kirim log-diagnostik

Deskripsi

Kumpulkan dan kirimkan log diagnostik AWS untuk pemecahan masalah.

Sinopsis

```
aws-vpn-client send-diagnostic-logs
```

Contoh

Contoh: Mengirim log diagnostik

`send-diagnostic-logs`Contoh berikut mengumpulkan dan mengirimkan log diagnostik ke AWS.

```
aws-vpn-client send-diagnostic-logs
```

Output:

```
{
  "reference-id": "us-west-2:78ff6531-5dc4-c706-7149-
e6cfd8adadc7/2026-07-24-16-03-55.zip"
}
```

> **Note**
>
> Bagikan `reference-id` nilai dengan AWS Dukungan saat melaporkan masalah.

Kode keluar

Alat AWS Client VPN CLI mengembalikan kode keluar berikut.

Kode keluar	Arti
0	Berhasil
1	Kesalahan umum
2	Sintaks perintah tidak valid

Dukungan untuk koneksi bersamaan menggunakan AWS klien yang disediakan

Yang AWS asalkan klien mendukung menghubungkan ke beberapa sesi bersamaan. Ini sangat membantu jika Anda memerlukan akses ke sumber daya di beberapa AWS lingkungan dan memiliki

titik akhir yang berbeda untuk sumber daya tersebut. Misalnya, Anda mungkin memerlukan akses ke database di lingkungan di titik akhir yang berbeda dari titik akhir yang saat ini terhubung, tetapi Anda tidak ingin memutuskan koneksi saat ini. Untuk mengaktifkan AWS menyediakan klien untuk terhubung ke beberapa sesi, unduh file konfigurasi yang dibuat administrator Anda untuk setiap titik akhir, lalu buat profil koneksi untuk setiap file. Menggunakan AWS disediakan klien, Anda kemudian dapat terhubung ke beberapa sesi tanpa memutuskan koneksi dari sesi apa pun yang saat ini terbuka. Hal ini didukung untuk AWS disediakan klien saja. Untuk langkah-langkah menyambung ke sesi bersamaan, lihat the section called “Hubungkan menggunakan klien”.

Saat menghubungkan ke beberapa titik akhir, VPN Klien memeriksa konflik dengan koneksi titik akhir terbuka lainnya — misalnya, jika dua sesi memiliki blok CIDR yang bertentangan atau kebijakan perutean, atau jika Anda sudah terhubung dengan koneksi terowongan penuh. Jika pemeriksaan menemukan konflik, koneksi gagal. Anda harus memilih koneksi lain yang tidak bertentangan dengan koneksi terbuka, atau memutuskan sambungan dari sesi terbuka yang menyebabkan konflik.

Koneksi DNS bersamaan diperbolehkan. Server DNS dari salah satu DNS-enabled koneksi diterapkan. Tergantung pada server DNS, Anda mungkin diminta untuk otentikasi selama koneksi ulang tersebut.

> **Note**
>
> Jumlah maksimum sesi bersamaan yang diizinkan adalah lima.

Menghubungkan ke titik akhir yang membutuhkan postur perangkat

Jika administrator Anda telah mengaktifkan postur perangkat pada titik akhir, AWS asalkan klien mengumpulkan data postur perangkat dari penyedia kepercayaan perangkat Anda saat Anda terhubung dan mengirimkannya ke titik akhir untuk dievaluasi. Untuk menyambung ke titik akhir yang memerlukan postur perangkat, Anda harus memenuhi persyaratan berikut:

- Gunakan AWS disediakan klien, versi 6.2.0 atau yang lebih baru. Postur perangkat tidak didukung dengan klien OpenVPN lainnya.
- Penyedia kepercayaan perangkat Anda harus diatur di perangkat Anda. Penyedia berikut didukung oleh sistem operasi: CrowdStrike (macOS, Windows), Jamf (macOS), dan JumpCloud (MacOS, Windows, Ubuntu).
- Profil yang Anda impor menyertakan `aws-auth-device-posture <provider>` direktif dalam konfigurasinya. Jangan hapus baris ini.

Jika perangkat Anda tidak memenuhi kebijakan, koneksi ditolak. Sesi Anda juga dapat berakhir di tengah sesi jika perangkat Anda nantinya tidak sesuai. Jika Anda ditolak secara tidak terduga, konfirmasikan penyedia kepercayaan perangkat Anda telah diatur dan perangkat Anda sesuai dengan persyaratan organisasi Anda, lalu coba lagi.

Menyiapkan penyedia kepercayaan perangkat

Jika administrator Anda telah mengaktifkan postur perangkat pada titik akhir VPN Klien, perangkat Anda harus memiliki penyedia kepercayaan perangkat yang didukung yang dikonfigurasi. Penyedia kepercayaan perangkat membuat token postur perangkat tersedia di perangkat Anda, yang AWS asalkan klien membaca saat Anda terhubung.

Halaman ini menjelaskan prasyarat untuk postur perangkat dan cara mengatur setiap penyedia yang didukung di perangkat Anda.

Prasyarat

Sebelum Anda mengatur penyedia kepercayaan perangkat, pastikan Anda memiliki yang berikut ini.

- The AWS disediakan klien, versi 6.2.0 atau yang lebih baru.
- Administrator yang telah mengaktifkan postur perangkat pada titik akhir VPN Klien yang Anda sambungkan.
- Konfigurasi klien (`.ovpn`) file yang berisi arahan postur perangkat. Administrator Anda menyediakan file ini.

CrowdStrike

Platform yang didukung

MacOS, Windows

Instal CrowdStrike Sensor Falcon pada perangkat Anda. Administrator TI organisasi Anda biasanya menerapkan ini.

Untuk informasi lebih lanjut, lihat CrowdStrike Penilaian Nol Kepercayaan di situs web penyedia.

Jamf

Platform yang didukung

macOS

Versi agen minimum

Jamf Trust 2.26.0

Daftarkan perangkat macOS Anda di Jamf Pro. Administrator TI organisasi Anda biasanya menangani pendaftaran.

Untuk informasi lebih lanjut, lihat Akses Terpercaya Jamf di situs web penyedia.

JumpCloud

Platform yang didukung

MacOS, Windows, Ubuntu

Versi agen minimum

JumpCloud Agen 2.144.3

Instal JumpCloud agen di perangkat Anda. Administrator TI organisasi Anda biasanya menerapkan ini.

Untuk informasi lebih lanjut, lihat JumpCloud Kepercayaan Perangkat di situs web penyedia.

Apa yang diharapkan saat menghubungkan

Saat Anda terhubung ke titik akhir VPN Klien yang mengaktifkan postur perangkat, AWS asalkan klien membaca token postur perangkat dari penyedia kepercayaan perangkat Anda dan mengirimkannya ke VPN Klien untuk evaluasi. Jika perangkat Anda memenuhi persyaratan dalam kebijakan otorisasi administrator, koneksi berjalan normal.

Jika perangkat Anda tidak memenuhi persyaratan, Client VPN menolak koneksi dan AWS asalkan klien menampilkan pesan `Authorization policy evaluation failed`. Jika Anda melihat pesan ini, hubungi administrator Anda.

Arahan OpenVPN

Yang AWS klien yang disediakan mendukung arahan OpenVPN berikut. Untuk informasi lebih lanjut tentang arahan ini, lihat dokumentasi di Situs OpenVPN.

- aut-federasi
- auth-nocache
- autentikasi coba lagi
- auth-user-pass
- aws-auth-device email
- blok-outside-dns
- ca
- sertifikat
- sandi
- klien
- hubung-coba lagi
- sambungkan retry-max
- cryptoapicert
- dev
- tipe pengembang
- opsi dhcp
- ifconfig-ipv6
- tidak aktif
- tetap hidup
- kunci
- mssfix
- nobind
- tombol persisten
- persistent
- ping
- ping-exit
- ping-restart

- proto
- tarik
- tarik-filter
- terpencil
- remote cert-tls
- nama host random-jarak jauh
- pemberontak detik
- penyelesaian-coba lagi
- rute
- rute-ipv6
- batas waktu poll-server
- tantangan statis
- tun-mtu
- kata kerja
- verifikasix509 nama-nama

> **Note**
>
> Dimulai dengan versi 6.0, AWS asalkan klien tidak lagi mendukung `rcvbuf`, `tap-sleep`, dan `tun-mtu-extra` arahan. Saat Anda memutakhirkan dari versi sebelumnya, arahan ini secara otomatis dihapus dari profil Anda yang ada. Jangan sertakan mereka dalam profil yang Anda impor di versi 6.0 atau yang lebih baru; jika tidak, impor gagal.

AWS Client VPN untuk Windows

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan AWS menyediakan klien untuk sistem Windows x64 dan Windows Arm64. Anda dapat mengunduh dan menginstal klien di mengunduh AWS Client VPN.

Persyaratan

Yang AWS klien yang disediakan mendukung sistem Windows x64 dan Arm64. Berikut ini diperlukan untuk setiap sistem operasi:

Sistem operasi Windows Arm64

- Windows 11 (sistem operasi 64-bit, prosesor Arm64)
- .NET Framework 4.8.1 atau lebih tinggi

> **Note**
>
> Aplikasi ini mencakup proses latar belakang yang memanfaatkan emulasi Arm64. Ini sepenuhnya didukung dan diaktifkan secara default pada perangkat Windows 11 Arm64, memastikan pengoperasian yang mulus tanpa diperlukan pengaturan tambahan. Untuk informasi lebih lanjut, lihat Bagaimana emulasi bekerja di Arm.

Sistem operasi Windows x64

- Windows 11 (sistem operasi 64-bit, prosesor x64)
- .NET Framework 4.7.2 atau lebih tinggi
- Perangkat lunak keamanan titik akhir mungkin memerlukan pengecualian untuk memungkinkan AWS menyediakan klien untuk berfungsi. Untuk informasi selengkapnya, lihat the section called “Kompatibilitas keamanan titik akhir”.

> **Note**
>
> Untuk sistem operasi Windows x64 dan Arm64, titik akhir VPN Klien yang menggunakan SAML-based otentikasi federasi (single sign-on), klien menyimpan port TCP 8096-8115 di komputer Anda.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Untuk petunjuk penggunaan klien, lihat the section called “Hubungkan menggunakan klien”.

Topik

- AWS Client VPN untuk catatan rilis Windows

AWS Client VPN untuk catatan rilis Windows

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi saat ini dan sebelumnya AWS Client VPN untuk Windows berbasis x64 dan Windows Arm64-based sistem.

> **Note**
>
> Kami terus memberikan perbaikan kegunaan dan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin terpengaruh oleh masalah kegunaan atau keamanan. Lihat entri versi individual di bawah ini untuk detailnya.

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.2.2	Rilis ini mencakup penyempurnaan kecil dan memperbaiki masalah berikut yang ada di versi 6.x sebelumnya: • Profil terdaftar dalam urutan yang berbeda dari pada 5.x • Pemilihan profil berubah saat koneksi sedang dibuat atau setelah terputus • Profil dan preferensi tidak bermigrasi dari 5.x ketika folder data 5.x adalah sambungan atau tautan simbolik • Koneksi terputus segera setelah terhubung ketika beberapa perangkat lunak keamanan jaringan berjalan • Split-tunnel koneksi kehilangan jaringan lokal dan akses internet pada mesin dengan beberapa jenis adaptor jaringan • Tombol Tutup spanduk panjang bergerak di luar layar saat jendela diubah ukurannya	5 November 2026	• Unduh Windows x64 versi 6.2.2 sha256:4f56da7857c6533cdeaa1cee8234b0782ec0604e3a2bc51193d90fcaf4f0e756 • Unduh Windows Arm64 versi 6.2.2 sha256:d62f7137f56ae256b246d63cbaf48678dbb471a9fdf67

Versi	Perubahan	Date	Tautan unduh dan SHA256
			1f44f96d5 e5e1608bd8

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.2.1	Rilis ini mencakup penyempurnaan kecil dan memperbaiki masalah berikut yang ada di versi 6.x sebelumnya: • Kehilangan akses jaringan setelah melanjutkan dari hibernasi saat terhubung • Nama host pendek gagal diselesaikan saat titik akhir VPN Klien mendorong alamat server DNS duplikat • Resolusi nama internal gagal ketika adaptor jaringan fisik menggunak an akhiran DNS yang sama dengan domain internal • Hilang `platform-version` nilai dalam peristiwa handler koneksi klien, yang dapat menyebabkan koneksi ditolak oleh penangan otorisasi yang secara eksplisit mengandalkan bidang ini • Kegagalan impor untuk `.ovpn` profil yang sertifikat atau jalur kuncinya menggunakan pemisah garis miring ganda • GUI dan CLI crash yang terjadi ketika direktori konfigurasi pengguna adalah tautan simbolis • Pesan kesalahan khusus dari otorisasi Lambda tidak ditampilkan dalam beberapa skenario • Kegagalan instalasi pada mesin tanpa pustaka Microsoft Visual C++ Runtime	Oktober 16, 2026	• Unduh Windows x64 versi 6.2.1 sha256:89 b9522c723 b2be6d436 6ab78a592 a60f7b862 43edfa67b bb4977d0c 4a5215ba • Unduh Windows Arm64 versi 6.2.1 sha256:32 54a883276 0373dab5a c0958d4bc 23145434e 50d675c75 95f8b2b26 5f41e8a9

Versi	Perubahan	Date	Tautan unduh dan SHA256
	• Menambahkan dukungan untuk `remote` kata kunci host di `route` Arahan OpenVPN		
6.2.0	• Dukungan untuk Postur Perangkat • Perbaikan bug minor dan peningkatan	September 28, 2026	• Unduh Windows x64 versi 6.2.0 sha256:729d438555bf2ff671ea078c4325de7475718bee8b7b8acdf3f669bf2fb74641 • Unduh Windows Arm64 versi 6.2.0 sha256:6bc448d8ef61ea274fa9167654a65e60b3b580642405aef81f52224d1a6d7bca

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.1.1	• Memperbaiki bug yang memblokir peningkatan otomatis di versi 6.0.3	September 25, 2026	• Unduh Windows x64 versi 6.1.1 sha256:8f57525c843ea94cbd835b45298f2ce3cbdb62fc331b40139c4785af4e8ba51b • Unduh Windows Arm64 versi 6.1.1 sha256:1fa1e6d2b5f9914d93bd0898b32c3b36692772dd4c65a52a49d231c8d4ce05b6
6.1.0	• Perbaikan bug minor dan peningkatan	September 24, 2026	Tidak lagi didukung.
6.0.3	• Pemberitahuan peningkatan yang diaktifkan meminta pengguna pra-6.x untuk pindah ke 6.x • Minta untuk memutuskan sambungan saat aplikasi GUI berhenti • Peningkatan postur keamanan • Perbaikan bug minor dan peningkatan	September 14, 2026	Tidak lagi didukung.

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.0.2	• Memperbaiki masalah pemasangan adaptor TAP karena konflik nama • Memperbaiki nama profil duplikat selama migrasi dengan menambahkan akhiran • Perbaikan bug minor dan peningkatan	Agustus 12, 2026	• Unduh Windows x64 versi 6.0.2 sha256:519e5d3e62dbe438f501f0da226ec386216df54be4a31f9d349731d7d7dda080aa • Unduh Windows Arm64 versi 6.0.2 sha256:4e8466dafd71f3a16e56a6caa316942f1c4320fc50912fb0091441f0bb7ffc7d

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.0.1	• Memperbaiki masalah otentikasi SAML yang menyebabkan kesalahan koneksi VPN sporadis di versi 6.0.0 • Perbaikan bug minor dan peningkatan	Agustus 7, 2026	• Unduh Windows x64 versi 6.0.1 sha256:23 a008656f1 0f3af2895 1fe3ae69d a46117f0f 50e86cbc2 5490a4f50 374f3b5b • Unduh Windows Arm64 versi 6.0.1 sha256:2a 531aa5c7a 525be24b6 361127df6 6e8d8bfce 2da8d5cb3 2bc333ec2 7cd228a6

Versi	Perubahan	Date	Tautan unduh dan SHA256
6.0.0	• Ditambahkan dukungan untuk antarmuka baris perintah (CLI) • Menambahkan dukungan untuk kontrol administratif perusahaan • Antarmuka pengguna grafis (GUI) AWS Client VPN yang didesain ulang • Arsitektur konektivitas modern dan postur keamanan yang ditingkatkan • Peningkatan waktu pembentukan koneksi • Memindahkan file konfigurasi ke lokasi yang dilindungi admin di seluruh sistem. Jika profil atau preferensi hilang setelah pemutakhiran, lihat the section called “Profil atau preferensi hilang setelah upgrade ke versi 6.0” untuk langkah-langkah resolusi.	Agustus 4, 2026	• Unduh Windows x64 versi 6.0.0 sha256:76 a4d2b76e9 5a5b43b6f 0d0e212ef 7bba20660 ac9390766 555414abc 30fe4cb3 • Unduh Windows Arm64 versi 6.0.0 sha256: a8f47e401 0de34dd72 0f22e8c75 4c98e45ea 1c1c63b00 bbb002598 04069314ea

Versi	Perubahan	Date	Tautan unduh dan SHA256
5.4.3	• Peningkatan kecil	Juli 23, 2026	• Unduh Windows x64 versi 5.4.3 sha256: eaa60ff88 478745604 c500020d8 24bfdd361 a739b5021 db0378ece 4c3f4d60b1 • Unduh Windows Arm64 versi 5.4.3 sha256: bdcb1a5ac ff49770df f48d2aa8d ce3ca6053 1cd04c1d7 49c518ef5 567e0231b0
5.4.2	• Peningkatan kecil.	Juli 20, 2026	Tidak lagi didukung.
5.4.1	• Peningkatan kecil.	Juli 9, 2026	Tidak lagi didukung.
5.4.0	• Peningkatan postur keamanan.	Juni 22, 2026	Tidak lagi didukung.
5.3.7	• Perbaikan bug minor dan peningkatan.	Juni 15, 2026	Tidak lagi didukung.

Versi	Perubahan	Date	Tautan unduh dan SHA256
5.3.6	• Mengembalikan perubahan dari 5.3.5	Mei 28, 2026	Tidak lagi didukung.
5.3.5	• Perbaikan bug minor dan peningkatan. • Peningkatan postur keamanan.	27 Mei 2026	Tidak lagi didukung.
5.3.4	• Perbaikan bug minor dan peningkatan. • Peningkatan postur keamanan.	Maret 27, 2026	Tidak lagi didukung.
5.3.3	• Kegagalan koneksi tetap di versi 5.3.2	Februari 28, 2026	Tidak lagi didukung.
5.3.2	• Perbaikan bug minor dan peningkatan. • Peningkatan postur keamanan.	Februari 17, 2026	Tidak lagi didukung.
5.3.1	Perbaikan bug minor dan peningkatan.	30. September 2025	Tidak lagi didukung.
5.3.0 (Tangan6)	Baru AWS Client VPN dukungan untuk Windows Arm64-based sistem operasi. Rilis ini mencakup semua pembaruan dari rilis Windows (x64) 5.3.0.	Agustus 26, 2025	Tidak lagi didukung.
5.3.0	• Peningkatan kecil. • Menambahkan dukungan untuk koneksi IPv6	Agustus 14, 2025	Tidak lagi didukung.
5.2.2	Peningkatan postur keamanan.	Juni 2, 2025	Tidak lagi didukung.
5.2.1	• Menambahkan dukungan untuk `ping-exit` Bendera OpenVPN. • Memperbarui pustaka OpenSSL. • Perbaikan bug minor dan peningkatan.	April 21, 2025	Tidak lagi didukung.

Versi	Perubahan	Date	Tautan unduh dan SHA256
5.2.0	• Peningkatan kecil. • Menambahkan dukungan untuk Penegakan Rute Klien.	8 April 2025	Tidak lagi didukung.
5.1.0	• Memperbaiki masalah yang menyebabkan AWS Client VPN versi 5.0.x untuk secara otomatis terhubung kembali ke VPN setelah pemutusan batas waktu tidak aktif. • Perbaikan bug minor dan peningkatan.	Maret 17, 2025	Tidak lagi didukung.
5.0.2	• Memperbaiki masalah DNS untuk koneksi bersamaan. • Memperbaiki masalah sporadis saat memasang adaptor TAP baru.	Februari 24, 2025	Tidak lagi didukung.
5.0.1	Memperbaiki masalah yang menyebabkan kesalahan koneksi VPN sporadis pada klien Windows versi 5.0.0.	Januari 30, 2025	Tidak lagi didukung.
5.0.0	• Menambahkan dukungan untuk koneksi bersamaan. • Memperbarui versi driver TAP. • Memperbarui antarmuka pengguna grafis. • Perbaikan bug minor dan peningkatan.	Januari 21, 2025	Tidak lagi didukung.
4.1.0	Perbaikan bug minor dan peningkatan.	November 12, 2024	Tidak lagi didukung.
4.0.0	Peningkatan kecil.	September 25, 2024	Tidak lagi didukung.

Versi	Perubahan	Date	Tautan unduh dan SHA256
3.14.2	Menambahkan dukungan untuk `mssfix` Bendera OpenVPN.	September 4, 2024	Tidak lagi didukung.
3.14.1	Perbaikan bug minor dan peningkatan.	Agustus 22, 2024	Tidak lagi didukung.
3.14.0	• Menambahkan dukungan untuk `tap-sleep` Bendera OpenVPN. • Memperbarui pustaka OpenVPN dan OpenSSL.	Agustus 12, 2024	Tidak lagi didukung.
3.13.0	Memperbarui pustaka OpenVPN dan OpenSSL.	Juli 29, 2024	Tidak lagi didukung.
3.12.1	Memperbaiki masalah yang mencegah klien Windows versi 3.12.0 membuat koneksi VPN untuk beberapa pengguna.	Juli 18, 2024	Tidak lagi didukung.
3.12.0	• Secara otomatis menyambung kembali saat rentang jaringan area lokal berubah. • Menghapus fokus aplikasi otomatis saat terhubung dengan titik akhir SAML.	Mei 21, 2024	Tidak lagi didukung
3.11.2	Menyelesaikan masalah otentikasi SAML dengan Chromium-based browser sejak versi 123.	April 11, 2024	Tidak lagi didukung.
3.11	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal untuk mengeksekusi perintah arbitrer dengan izin yang ditingkatkan. • Peningkatan postur keamanan.	Februari 16, 2024	Tidak lagi didukung.

Versi	Perubahan	Date	Tautan unduh dan SHA256
3.11.0	• Memperbaiki masalah konektivitas yang disebabkan oleh VM Windows. • Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Tidak lagi didukung.
3.0.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Memperbaiki masalah konektivitas saat Hyper-V adaptor jaringan diinstal pada mesin klien. • Perbaikan bug minor dan peningkatan.	24 Agustus 2023	Tidak lagi didukung.
3.9.0	Peningkatan postur keamanan.	3 Agustus 2023	Tidak lagi didukung.
3.8.0	Peningkatan postur keamanan.	15 Juli 2023	Tidak lagi didukung
3.7.0	Mengembalikan perubahan dari 3.6.0.	15 Juli 2023	Tidak lagi didukung
3.6.0	Peningkatan postur keamanan.	14 Juli 2023	Tidak lagi didukung
3.5.0	Perbaikan bug minor dan peningkatan.	3 April 2023	Tidak lagi didukung
3.4.0	Mengembalikan 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	Date	Tautan unduh dan SHA256
3.2.0	• Menambahkan dukungan untuk bendera OpenVPN “verify-x509-name”. • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Menambahkan kemampuan untuk menginstal versi klien baru secara otomatis bila tersedia.	23 Januari 2023	Tidak lagi didukung
3.1.0	Peningkatan postur keamanan.	23 Mei 2022	Tidak lagi didukung
3.0.0	• Menambahkan dukungan Windows 11. • Memperbaiki penamaan driver TAP Windows yang menyebabkan nama driver lain terpengaruh. • Memperbaiki pesan spanduk yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks spanduk tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan.	3 Maret 2022	Tidak lagi didukung
2.0.0	• Menambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Dihapus kemampuan untuk menggunakan filter tarik dalam kaitannya dengan gema. yaitu 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.	8 November 2021	Tidak lagi didukung

Versi	Perubahan	Date	Tautan unduh dan SHA256
1.3.6	• Menambahkan dukungan untuk bendera 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	• Menambahkan dukungan untuk bendera OpenVPN: opsi dhcp. • 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	Date	Tautan unduh 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	Date	Tautan unduh 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

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan AWS disediakan klien untuk MacOS. Anda dapat mengunduh dan menginstal klien di mengunduh AWS Client VPN.

Persyaratan

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

- macOS Sonoma (14.0), Sequoia (15.0), Tahoe (26.0), atau Golden Gate (27.0)
- Prosesor x86_64 atau ARM64 kompatibel.

- Untuk VPN Klien, titik akhir yang menggunakan SAML-based otentikasi federasi (single sign-on), Klien menyimpan port TCP 8096-8115 di komputer Anda.
- Perangkat lunak keamanan titik akhir mungkin memerlukan pengecualian untuk memungkinkan AWS menyediakan klien untuk berfungsi. Untuk informasi selengkapnya, lihat the section called "Kompatibilitas keamanan titik akhir".

Untuk petunjuk penggunaan klien, lihat the section called "Hubungkan menggunakan klien".

Topik

- AWS Client VPN untuk catatan rilis macOS

AWS Client VPN untuk catatan rilis macOS

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

> **Note**
>
> Kami terus memberikan perbaikan kegunaan dan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin dipengaruhi oleh kegunaan and/or masalah keamanan. Lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
6.2.2	Memperbaiki masalah yang ada di versi 6.x sebelumnya: • Profil terdaftar dalam urutan yang berbeda dari pada 5.x • Pemilihan profil berubah saat koneksi sedang dibuat atau setelah terputus • Profil dan preferensi tidak bermigrasi dari 5.x ketika folder data 5.x adalah tautan simbolis	5 November 2026	• Unduh macOS ARM64 versi 6.2.2 sha256:01de5a76eeda2b8ac822ed6f37a8bafd582069fae45f57bd910be786330f0ff8 • Unduh macOS x64 versi 6.2.2

Versi	Perubahan	Tanggal	Tautan unduh
	• Split-tunnel koneksi kehilangan akses internet di Mac dengan antarmuka jaringan yang tidak memiliki subnet mask, atau dengan alamat loopback alias • Pengaturan DNS VPN tidak dipulihkan setelah macOS mengubah konfigurasi jaringan • Log perbaikan DNS hilang dari Kirim Log Diagnostik • Tombol Tutup spanduk panjang bergerak di luar layar saat jendela diubah ukurannya		sha256:138f5de11a65fdf23b78ef2b33684780bcc9efd5b7dc3f6173dd69cbf9dad8b0
6.2.1	Memperbaiki masalah yang ada di versi 6.x sebelumnya: • Pemutusan tak terduga saat mencoba menginstal versi aplikasi saat ini atau versi sebelumnya • GUI dan CLI crash yang terjadi ketika direktori konfigurasi pengguna adalah tautan simbolis • Masalah yang mencegah aplikasi menampilkan pesan kesalahan khusus dari otorisasi Lambda dalam beberapa skenario • Menambahkan dukungan untuk `remote` kata kunci host di `route` Arahan OpenVPN	Oktober 9, 2026	• Unduh macOS ARM64 versi 6.2.1 sha256:45e08aebe669854afd7851e46298b7baa2dec8793927422656ba8e149cd85826 • Unduh macOS x64 versi 6.2.1 sha256:12e0159c0e0192c79d09c33f46c9554b9c9168061991832f2efbbf904d3b0b95

Versi	Perubahan	Tanggal	Tautan unduh
6.2.0	• Dukungan untuk Postur Perangkat • Perbaikan bug minor dan peningkatan	September 28, 2026	• Unduh macOS ARM64 versi 6.2.0 sha256:25a753dc9e24d0abba3ee4aa0118209c352d64059ece2827e33cfb523e50a36a • Unduh macOS x64 versi 6.2.0 sha256:0c1894f50af8a0255888718bdf384d89f7d3dea208d7d0146f187e4315f76cd1
6.1.1	• Memperbaiki bug yang memblokir peningkatan otomatis di versi 6.0.3	September 25, 2026	• Unduh macOS ARM64 versi 6.1.1 sha256: e7a804b6172cec9507eb497729cd001f7acb269e58080aa7ba941f1513cc53b0 • Unduh macOS x64 versi 6.1.1 sha256:0500fcc9daef464cde2f59dfbb8dc08f19801d486e291031529d2d0e1bf2e68b
6.1.0	• Perbaikan bug minor dan peningkatan	September 24, 2026	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
6.0.3	• Pemberitahuan peningkatan yang diaktifkan meminta pengguna pra-6.x untuk pindah ke 6.x • Minta untuk memutuskan sambungan saat aplikasi GUI berhenti • Peningkatan postur keamanan • Perbaikan bug minor dan peningkatan	Agustus 27, 2026	Tidak lagi didukung.
6.0.2	• Memperbaiki masalah migrasi profil yang memengaruhi beberapa pengguna yang memutakhirkan dari pra-6.x ke 6.x • Perbaikan bug minor dan peningkatan	Agustus 18, 2026	• Unduh macOS ARM64 versi 6.0.2 sha256:0188775963a86946c17e90f102e39b1ac45e1e2df49d4e4d6aa44ca92c0f3116 • Unduh macOS x64 versi 6.0.2 sha256:8e2d7a2fd3ce62c0109d93cff6a6099defdabb668d8069cb27e56e4861a84ff5

Versi	Perubahan	Tanggal	Tautan unduh
6.0.1	• Memperbaiki masalah otentikasi SAML yang menyebabkan kesalahan koneksi VPN sporadis di versi 6.0.0 • Perbaikan bug minor dan peningkatan	Agustus 7, 2026	• Unduh macOS ARM64 versi 6.0.1 sha256:74783fe5ddbcc5924e491b4df1a90fb6a6ba246fc188e7d235629652f28a0958 • Unduh macOS x64 versi 6.0.1 sha256:0e630f52e90e257866c2bbbbe506d291400fb3cfa666be17572cbdd5e47f3da2

Versi	Perubahan	Tanggal	Tautan unduh
6.0.0	• Ditambahkan dukungan untuk antarmuka baris perintah (CLI) • Menambahkan dukungan untuk kontrol administratif perusahaan • Antarmuka pengguna grafis yang didesain ulang (GUI) • Arsitektur konektivitas modern dan postur keamanan yang ditingkatkan • Perangkat lunak keamanan titik akhir mungkin memerlukan pengecualian untuk memungkinkan AWS menyediakan klien untuk berfungsi. Untuk informasi selengkapnya, lihat the section called “Kompatibilitas keamanan titik akhir”. • Peningkatan waktu pembentukan koneksi • Memindahkan file konfigurasi ke lokasi yang dilindungi admin di seluruh sistem. Jika profil atau preferensi hilang setelah pemutakhiran, lihat the section called “Profil atau preferensi hilang setelah upgrade ke versi 6.0” untuk langkah-langkah resolusi.	Agustus 4, 2026	• Unduh macOS ARM64 versi 6.0.0 sha256:0c0d26b6d8677281ef0eed4ac481abd3fdee1df096c451a26a38dd245b5577da • Unduh macOS x64 versi 6.0.0 sha256:147b7235e2b040a2e63630d48e2b071b4a0d2ee4edad83756eb6a0e8235ba256

Versi	Perubahan	Tanggal	Tautan unduh
5.4.3	• Peningkatan kecil	Juli 23, 2026	• Unduh macOS ARM64 versi 5.4.3 sha256:9c783f3e5a28f74a75b1229336a6f3c03dcf4f97a7ee2303a24f864f922fc3c0 • Unduh macOS x64 versi 5.4.3 sha256:3fdcfc14cc30c790258a71581410898faf7e8a21d838c766ab220f2d2f13139c
5.4.2	• Peningkatan kecil	Juli 20, 2026	Tidak lagi didukung.
5.4.1	• Peningkatan kecil	Juli 6, 2026	Tidak lagi didukung.
5.4.0	• Peningkatan postur keamanan	Juni 22, 2026	Tidak lagi didukung.
5.3.5	• Perbaikan bug minor dan peningkatan • Peningkatan postur keamanan • Mengaktifkan peningkatan otomatis ke klien ARM64 asli untuk ARM-based Pengguna Mac dalam pembaruan mendatang, menghilangkan kebutuhan untuk migrasi manual dari Intel-based klien berjalan di bawah lapisan terjemahan Rosetta	14 Mei 2026	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
5.3.4	• Menghapus persyaratan lapisan kompatibilitas Intel (Rosetta) pada mesin ARM • Perbaikan bug minor dan peningkatan	Februari 17, 2026	Tidak lagi didukung.
5.3.3	• Perbaikan bug minor dan peningkat an. • Peningkatan postur keamanan.	Desember 26, 2025	Tidak lagi didukung.
5.3.2	• Menambahkan dukungan asli untuk arsitektur Apple Silicon dan penginstal macOS ARM64 baru. • Perbaikan bug minor dan peningkat an.	Oktober 27, 2025	Tidak lagi didukung.
5.3.1	• Perbaikan bug minor dan peningkat an.	September 9, 2025	Tidak lagi didukung.
5.3.0	• Peningkatan kecil. • Menambahkan dukungan untuk koneksi IPv6.	Agustus 14, 2025	Tidak lagi didukung.
5.2.1	• Menambahkan dukungan untuk flag ping-exit OpenVPN. • Memperbarui pustaka OpenSSL. • Peningkatan postur keamanan. • Perbaikan bug minor dan peningkat an.	Juni 18, 2025	Tidak lagi didukung.
5.2.0	• Peningkatan kecil. • Menambahkan dukungan untuk Penegakan Rute Klien.	8 April 2025	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
5.1.0	• Memperbaiki masalah yang menyebabkan AWS Client VPN versi 5.0.x untuk secara otomatis terhubung kembali ke VPN setelah pemutusan batas waktu tidak aktif. • Memperbaiki masalah yang mencegah AWS Client VPN dari membuat koneksi VPN untuk file konfigurasi dengan Windows-style akhir baris. • Perbaikan bug minor dan peningkat an.	Maret 17, 2025	Tidak lagi didukung.
5.0.3	Perbaikan bug minor dan peningkatan.	Maret 6, 2025	Tidak lagi didukung.
5.0.2	Memperbaiki masalah yang menyebabk an kesalahan sporadis saat memilih Menghubungkan.	Februari 17, 2025	Tidak lagi didukung.
5.0.1	Memperbaiki masalah yang mencegah klien versi 5.0.0 membuat koneksi VPN untuk nama profil yang berisi spasi.	Januari 22, 2025	Tidak lagi didukung.
5.0.0	• Menambahkan dukungan untuk koneksi bersamaan. • Memperbarui antarmuka pengguna grafis. • Perbaikan bug minor dan peningkat an.	Januari 21, 2025	Tidak lagi didukung.
4.1.0	Perbaikan bug minor dan peningkatan.	November 12, 2024	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
4.0.0	Peningkatan kecil.	September 25, 2024	Tidak lagi didukung.
3.12.1	Menambahkan dukungan untuk `mssfix` Bendera OpenVPN.	September 4, 2024	Tidak lagi didukung.
3.12.0	• Menambahkan dukungan untuk `tap-sleep` Bendera OpenVPN. • Memperbarui pustaka OpenVPN dan OpenSSL.	Agustus 12, 2024	Tidak lagi didukung.
3.11.0	• Memperbarui pustaka OpenVPN dan OpenSSL.	Juli 29, 2024	Tidak lagi didukung.
3.0.0	• Secara otomatis menyambung kembali saat rentang jaringan area lokal berubah. • Memperbaiki masalah pemulihan DNS selama peralihan jaringan. • Menghapus fokus aplikasi otomatis saat terhubung dengan titik akhir SAML.	Mei 21, 2024	Tidak lagi didukung.
3.9.2	• Menyelesaikan masalah otentikasi SAML dengan Chromium-based browser sejak versi 123. • Menambahkan dukungan untuk macOS Sonoma. Hentikan dukungan untuk macOS Big Sur. • Peningkatan postur keamanan.	April 11, 2024	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
3.9.1	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal untuk mengeksekusi perintah arbitrer dengan izin yang ditingkatkan. • Bilah kemajuan unduhan pembaruan aplikasi tetap. • Peningkatan postur keamanan.	Februari 16, 2024	Tidak lagi didukung.
3.9.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Tidak lagi didukung.
3.8.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Perbaikan bug minor dan peningkat an.	24 Agustus 2023	Tidak lagi didukung.
3.7.0	• Peningkatan postur keamanan.	3 Agustus 2023	Tidak lagi didukung.
3.6.0	• Peningkatan postur keamanan.	15 Juli 2023	Tidak lagi didukung.
3.5.0	• Mengembalikan perubahan dari 3.4.0.	15 Juli 2023	Tidak lagi didukung.
3.4.0	• Peningkatan postur keamanan.	14 Juli 2023	Tidak lagi didukung.
3.3.0	• Menambahkan dukungan untuk macOS Ventura (13.0). • Perbaikan bug minor dan peningkat an.	27 April 2023	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
3.2.0	• Menambahkan dukungan untuk bendera OpenVPN “verify-x509-name”. • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Menambahkan kemampuan untuk menginstal versi klien baru secara otomatis bila tersedia.	23 Januari 2023	Tidak lagi didukung.
3.1.0	• Menambahkan dukungan untuk macOS Monterey. • Memperbaiki masalah untuk deteksi jenis drive. • Peningkatan postur keamanan.	23 Mei 2022	Tidak lagi didukung.
3.0.0	• Memperbaiki pesan spanduk yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks spanduk tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan.	3 Maret 2022	Tidak lagi didukung.
2.0.0	• Menambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Dihapus kemampuan untuk menggunakan filter tarik dalam kaitannya dengan gema. yaitu pull-filter * echo • Perbaikan bug minor dan peningkatan.	20 Januari 2022	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
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.	9 November 2021	Tidak lagi didukung.
1.3.5	• Menambahkan dukungan untuk bendera 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	• Menambahkan dukungan untuk bendera OpenVPN: opsi dhcp. • 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 autentika si 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.

Versi	Perubahan	Tanggal	Tautan unduh
1.2.2	Perbaikan bug minor dan penyempurnaan.	12 Agustus 2020	Tidak lagi didukung.
1.2.1	• Penambahan dukungan untuk menghapus aplikasi. • Perbaikan bug minor dan penyempurnaan.	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 penyempurnaan.	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 penyempurnaan.	9 Maret 2020	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.0.0	Rilis awal.	4 Februari 2020	Tidak lagi didukung.

AWS Client VPN untuk Linux

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan AWS menyediakan klien untuk Linux. Untuk pembaruan dan unduhan terbaru, lihat the section called “Catatan Rilis”.

Persyaratan untuk menghubungkan ke VPN Klien dengan AWS disediakan klien untuk Linux

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

- Ubuntu 22.04 LTS (AMD64), Ubuntu 24.04 LTS (hanya AMD64), atau Ubuntu 26.04 LTS (hanya AMD64)
- Perangkat lunak keamanan titik akhir mungkin memerlukan pengecualian untuk memungkinkan AWS menyediakan klien untuk berfungsi. Untuk informasi selengkapnya, lihat the section called “Kompatibilitas keamanan titik akhir”.

Untuk titik akhir VPN Klien yang menggunakan SAML-based otentikasi federasi (single sign-on) klien menyimpan port TCP 8096-8115 di komputer Anda.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Untuk petunjuk penggunaan klien, lihat the section called “Hubungkan menggunakan klien”.

Topik

- Instal yang disediakan AWS Client VPN untuk Linux
- AWS Client VPN untuk catatan rilis Linux

Instal yang disediakan AWS Client VPN untuk Linux

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 Klien AWS VPN 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 berikut untuk menambahkan repositori ke OS Ubuntu Anda (versi 22.04 ke atas):

```
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. 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 file paket.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.

AWS Client VPN untuk catatan rilis Linux

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

> **Note**
>
> Kami terus memberikan perbaikan kegunaan dan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin dipengaruhi oleh kegunaan and/or masalah keamanan. Lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
6.2.0	• Dukungan untuk Postur Perangkat • Perbaikan bug minor dan peningkatan	September 28, 2026	Unduh versi 6.2.0 sha256:27 79a8af748 addc2e6f5 061c8ea89 ec9f7cb00 a6f455af3 a3da17dcf 8b40abb7
6.0.2	• Minta untuk memutuskan sambungan saat aplikasi GUI berhenti • Peningkatan postur keamanan • Perbaikan bug minor dan peningkatan	September 22, 2026	Unduh versi 6.0.2 sha256:90 74a16d111

Versi	Perubahan	Tanggal	Tautan unduh
			27fcc0dd0 bc9e12e0b 7709fe852 814ddcf9a a65c7360b 312c85c6
6.0.1	• Ditambahkan dukungan untuk antarmuka baris perintah (CLI) • Menambahkan dukungan untuk kontrol administratif perusahaan • Antarmuka pengguna grafis yang didesain ulang (GUI) • Arsitektur konektivitas modern dan postur keamanan yang ditingkatkan • Peningkatan waktu pembentukan koneksi • Memindahkan file konfigurasi ke lokasi yang dilindungi admin di seluruh sistem. Jika profil atau preferensi hilang setelah pemutakhiran, lihat the section called “Profil atau preferensi hilang setelah upgrade ke versi 6.0” untuk langkah-langkah resolusi.	Agustus 12, 2026	Unduh versi 6.0.1 sha256: c3c10d916 93efa2800 c4812afa7 cdb0be221 81fa9a2d5 51030fa6f 4c819e8cc9

Versi	Perubahan	Tanggal	Tautan unduh
5.4.1	• Perbaikan bug minor dan peningkatan	Agustus 25, 2026	Unduh versi 5.4.1 sha256: e5d847366 0be6429c8 6bfd554f4 97849aa94 725225e2d 42a105933 759155e804
5.4.0	• Peningkatan postur keamanan	Juni 22, 2026	Tidak lagi didukung.
5.3.3	• Perbaikan bug minor dan peningkatan • Peningkatan postur keamanan	18 Mei 2026	Tidak lagi didukung.
5.3.2	• Perbaikan bug minor dan peningkatan. • Peningkatan postur keamanan.	Desember 17, 2025	Tidak lagi didukung.
5.3.1	• Peningkatan kecil.	25 September 2025	Tidak lagi didukung.
5.3.0	• Peningkatan kecil. • Menambahkan dukungan untuk koneksi IPv6.	Agustus 14, 2025	Tidak lagi didukung.
5.2.0	• Peningkatan kecil. • Menambahkan dukungan untuk Penegakan Rute Klien.	8 April 2025	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
5.1.0	• Memperbaiki masalah yang menyebabkan AWS Client VPN versi 5.0.x untuk secara otomatis terhubung kembali ke VPN setelah pemutusan batas waktu tidak aktif. • Perbaikan bug minor dan peningkatan.	Maret 17, 2025	Tidak lagi didukung.
5.0.0	• Menambahkan dukungan untuk beberapa koneksi bersamaan. • Memperbarui antarmuka pengguna grafis. • Perbaikan bug minor dan peningkatan.	Januari 21, 2025	Tidak lagi didukung.
4.1.0	• Menambahkan dukungan untuk Ubuntu 22.04 dan 24.04. • Perbaikan bug.	12 November 2024	Tidak lagi didukung.
4.0.0	Peningkatan kecil.	25 September 2024	Tidak lagi didukung.
3.15.1	Menambahkan dukungan untuk `mssfix` Bendera OpenVPN.	4 September 2024	Tidak lagi didukung.
3.15.0	• Menambahkan dukungan untuk `tap-sleep` Bendera OpenVPN. • Memperbarui pustaka OpenVPN dan OpenSSL.	Agustus 12, 2024	Tidak lagi didukung.
3.14.0	• Memperbarui pustaka OpenVPN dan OpenSSL.	Juli 29, 2024	Tidak lagi didukung.
3.13.0	• Secara otomatis terhubung kembali saat rentang jaringan area lokal berubah.	Mei 21, 2024	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
3.12.2	• Menyelesaikan masalah otentikasi SAML dengan Chromium-based browser sejak versi 123.	April 11, 2024	Tidak lagi didukung.
3.12.1	• Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal untuk menjalankan perintah arbitrer dengan izin yang ditingkatkan. • Peningkatan postur keamanan.	Februari 16, 2024	Tidak lagi didukung.
3.12.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN.	Desember 19, 2023	Tidak lagi didukung.
3.11.0	• Kembalikan untuk “Masalah konektivitas tetap untuk beberapa konfigurasi LAN”. • Peningkatan aksesibilitas.	6 Desember 2023	Tidak lagi didukung.
3.0.0	• Memperbaiki masalah konektivitas untuk beberapa konfigurasi LAN. • Peningkatan aksesibilitas.	6 Desember 2023	Tidak lagi didukung.
3.9.0	• Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Perbaikan bug minor dan peningkatan.	24 Agustus 2023	Tidak lagi didukung.
3.8.0	• Peningkatan postur keamanan.	3 Agustus 2023	Tidak lagi didukung.
3.7.0	• Peningkatan postur keamanan.	15 Juli 2023	Tidak lagi didukung.
3.6.0	• Mengembalikan perubahan dari 3.5.0.	15 Juli 2023	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
3.5.0	• Peningkatan postur keamanan.	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 jenis drive. • Peningkatan postur keamanan.	23 Mei 2022	Tidak lagi didukung.
3.0.0	• Memperbaiki pesan spanduk 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.
2.0.0	• Menambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Dihapus kemampuan untuk menggunak an filter tarik dalam kaitannya dengan gema. yaitu 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.	8 November 2021	Tidak lagi didukung.
1.0.2	• Menambahkan dukungan untuk bendera 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.

Versi	Perubahan	Tanggal	Tautan unduh
1.0.1	• Opsi diaktifkan untuk keluar 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 AWS klien yang disediakan

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Sebelum Anda mulai, pastikan bahwa Anda telah membaca persyaratan untuk platform Anda (the section called “Persyaratan”, the section called “Persyaratan”, atau the section called “Persyaratan untuk menghubungkan ke VPN Klien dengan AWS disediakan klien untuk Linux”). AWS Pelanggan yang disediakan juga disebut sebagai AWS Klien VPN dalam langkah-langkah berikut.

Versi 6.0 dan yang lebih baru

Menambahkan profil koneksi

Untuk menambahkan satu atau lebih profil koneksi, gunakan file konfigurasi yang disediakan oleh administrator VPN Klien Anda untuk setiap profil.

1. Buka AWS Klien VPN aplikasi.
2. Jika tidak ada profil, pilih Tambah profil tombol ditampilkan di jendela utama. Jika tidak, pilih Tindakan lain tombol, pilih Profil, dan kemudian memilih Tambah.
3. Untuk Nama profil, masukkan nama untuk profil.
4. Untuk File konfigurasi VPN, pilih Pilih berkas, telusuri ke dan kemudian pilih file konfigurasi, dan pilih Tambah profil.
5. Untuk membuat beberapa koneksi, ulangi langkah sebelumnya untuk setiap file konfigurasi yang ingin Anda tambahkan.

Hubungkan ke profil

Untuk menyambung ke profil

1. Buka AWS Klien VPN aplikasi.
2. Pilih profil dari Pilih profil dropdown, lalu pilih Menghubungkan.
3. Jika titik akhir VPN Klien menggunakan otentikasi berbasis kredensi, masukkan nama pengguna dan kata sandi saat diminta. Jika menggunakan SAML-based otentikasi federasi (single sign-on), otentikasi lengkap di jendela browser yang terbuka.
4. Setelah Anda terhubung, profil muncul di daftar profil yang terhubung dengan status Terhubung.

> **Note**
>
> Anda dapat terhubung ke beberapa profil secara bersamaan.

> **Note**
>
> Jika ada profil yang Anda sambungkan ke bertentangan dengan sesi yang sedang terbuka, Anda tidak akan dapat membuat koneksi. Pilih koneksi baru atau putuskan sambungan dari sesi yang menyebabkan konflik.

Putuskan sambungan

Untuk memutuskan sambungan dari profil, pilih Putuskan sambungan tombol di sebelah profil yang terhubung. Pada Windows dan macOS, Anda juga dapat memilih AWS Ikon Klien VPN di baki sistem (atau bilah menu di macOS) dan pilih Putuskan sambungan. Jika Anda memiliki beberapa koneksi terbuka, Anda harus memutuskan setiap koneksi satu per satu.

Lihat statistik koneksi

Untuk melihat statistik untuk koneksi, pilih Tindakan lain tombol, lalu pilih Statistik.

Versi sebelumnya

Menambahkan profil koneksi

Untuk menambahkan satu atau lebih profil koneksi, gunakan file konfigurasi yang disediakan oleh administrator VPN Klien Anda untuk setiap profil.

1. Buka AWS Klien VPN aplikasi.
2. Pilih File, Mengelola Profil.
3. Pilih Tambah profil.
4. Untuk Nama tampilan, masukkan nama untuk profil.
5. Untuk File Konfigurasi VPN, telusuri ke dan kemudian pilih file konfigurasi, dan pilih Tambah Profil.
6. Untuk membuat beberapa koneksi, ulangi langkah sebelumnya untuk setiap file konfigurasi yang ingin Anda tambahkan. Anda dapat memiliki hingga lima koneksi terbuka.

Hubungkan ke profil

Untuk menyambung ke profil

1. Buka AWS Klien VPN aplikasi.
2. Di AWS Klien VPN jendela, pilih profil yang ingin Anda sambungkan, lalu pilih Menghubungkan.
3. Jika titik akhir VPN Klien menggunakan otentikasi berbasis kredensi, masukkan nama pengguna dan kata sandi saat diminta. Jika menggunakan SAML-based otentikasi federasi (single sign-on), otentikasi lengkap di jendela browser yang terbuka.

> **Note**
>
> Anda dapat terhubung ke beberapa profil secara bersamaan, hingga lima koneksi terbuka. Ulangi langkah sambungkan untuk setiap profil yang ingin Anda mulai.

> **Note**
>
> Jika ada profil yang Anda sambungkan ke bertentangan dengan sesi yang sedang terbuka, Anda tidak akan dapat membuat koneksi. Pilih koneksi baru atau putuskan sambungan dari sesi yang menyebabkan konflik.

Putuskan sambungan

Untuk memutuskan sambungan, pilih koneksi di AWS Klien VPN jendela, lalu pilih Putuskan sambungan. Pada Windows dan macOS, Anda juga dapat memilih ikon klien di baki sistem (atau bilah menu di macOS) dan memilih Putuskan sambungan. Jika Anda memiliki beberapa koneksi terbuka, Anda harus menutup setiap koneksi satu per satu.

Lihat statistik koneksi

Untuk melihat statistik untuk koneksi, pilih Koneksi di AWS Klien VPN jendela, pilih Tampilkan Rincian, lalu pilih koneksi yang ingin Anda lihat detailnya.

Kompatibilitas perangkat lunak keamanan titik akhir

Produk keamanan titik akhir perusahaan seperti firewall berbasis host, agen deteksi dan respons titik akhir (EDR), dan perangkat lunak antivirus terkadang dapat mengganggu AWS Koneksi VPN klien. Jika Anda mengalami masalah konektivitas saat menggunakan AWS disediakan klien, Anda mungkin perlu mengonfigurasi pengecualian di perangkat lunak keamanan titik akhir Anda.

AWS Jalur yang dapat dieksekusi VPN klien

Yang AWS asalkan klien menginstal kunci yang dapat dieksekusi berikut. Anda mungkin memerlukan jalur ini saat mengonfigurasi aturan firewall, daftar izin aplikasi, atau kebijakan keamanan titik akhir.

Windows

Versi 6.0 dan yang lebih baru

Antarmuka pengguna grafis

```
C:\Program Files\Amazon\AWS VPN Client\AWS VPN Client.exe
```

Antarmuka baris perintah

```
C:\Program Files\Amazon\AWS VPN Client\aws-vpn-client.exe
```

Layanan Windows

```
C:\Program Files\Amazon\AWS VPN Client\aws-client-vpn-daemon.exe
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Agen postur perangkat

```
C:\Program Files\Amazon\AWS VPN Client\aws-vpn-client-agent.exe
```

Saat Anda menyambung ke titik akhir yang mengaktifkan postur perangkat, proses ini membaca data postur perangkat dari penyedia kepercayaan perangkat Anda.

Sebelum versi 6.0

Aplikasi klien VPN

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

Proses OpenVPN

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Layanan Windows

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

macOS

Versi 6.0 dan yang lebih baru

Antarmuka pengguna grafis

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/MacOS/AWS VPN Client
```

Antarmuka baris perintah

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/MacOS/aws-vpn-client
```

Symlink kenyamanan juga dipasang di `/usr/local/bin/aws-vpn-client`.

Daemon

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/Helpers/aws-client-vpn-daemon
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Agen postur perangkat

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/Helpers/aws-vpn-client-agent
```

Saat Anda menyambung ke titik akhir yang mengaktifkan postur perangkat, proses ini membaca data postur perangkat dari penyedia kepercayaan perangkat Anda.

Sebelum versi 6.0

Aplikasi klien VPN

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/MacOS/AWS VPN Client
```

Proses OpenVPN

```
/Applications/AWS VPN Client/AWS VPN Client.app/Contents/Resources/openvpn/acvc-openvpn
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Pembantu istimewa

```
/Library/PrivilegedHelperTools/com.amazonaws.acvc.helper
```

Mengelola rute dan konfigurasi DNS atas nama aplikasi.

Linux

Versi 6.0 dan yang lebih baru

Antarmuka pengguna grafis

```
/opt/awsvpnclient/AWS VPN Client
```

Antarmuka baris perintah

```
/opt/awsvpnclient/aws-vpn-client
```

Daemon

```
/opt/awsvpnclient/aws-client-vpn-daemon
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Agen postur perangkat

```
/opt/awsvpnclient/aws-vpn-client-agent
```

Saat Anda menyambung ke titik akhir yang mengaktifkan postur perangkat, proses ini membaca data postur perangkat dari penyedia kepercayaan perangkat Anda.

Sebelum versi 6.0

Aplikasi klien VPN

```
/opt/awsvpnclient/AWS VPN Client
```

Proses OpenVPN

```
/opt/awsvpnclient/Resources/openvpn/acvc-openvpn
```

Ini adalah proses inti yang membangun dan memelihara koneksi terowongan VPN.

Layanan istimewa

```
/opt/awsvpnclient/Service/ACVC.GTK.Service
```

Mengelola koneksi dan rute VPN atas nama aplikasi.

Persyaratan jaringan

Yang AWS klien yang disediakan memerlukan akses jaringan keluar ke titik akhir VPN Klien untuk membuat koneksi VPN. Pastikan firewall atau perangkat lunak keamanan titik akhir Anda memungkinkan lalu lintas keluar dari proses terowongan VPN ke port dan protokol yang dikonfigurasi pada titik akhir VPN Klien Anda.

Versi 6.0 dan yang lebih baru

- Windows: `aws-client-vpn-daemon.exe`
- MacOS: `aws-client-vpn-daemon`
- Linux: `aws-client-vpn-daemon`

Sebelum versi 6.0

- Windows: `acvc-openvpn.exe`
- MacOS dan Linux: `acvc-openvpn`

Mengkonfigurasi pengecualian keamanan titik akhir

Jika produk keamanan titik akhir Anda mengganggu AWS disediakan konektivitas klien, tinjau kategori pengecualian berikut dengan administrator keamanan Anda:

Process-based pengecualian

Tambahkan file yang dapat dieksekusi yang tercantum di the section called “AWS Jalur yang dapat dieksekusi VPN klien” ke daftar izin atau daftar pengecualian proses produk keamanan titik akhir Anda.

Network-based pengecualian

Izinkan lalu lintas keluar dari proses terowongan VPN ke port dan protokol titik akhir VPN Klien Anda. Untuk versi 6.0 dan yang lebih baru, ini `aws-client-vpn-daemon` (atau `aws-client-vpn-daemon.exe` pada Windows). Untuk versi sebelumnya, ini adalah `acvc-openvpn` (atau `acvc-openvpn.exe` pada Windows).

Path-based pengecualian

Kecualikan AWS disediakan direktori instalasi klien dari pemindaian real-time atau analisis perilaku:

- Windows: `C:\Program Files\Amazon\AWS VPN Client\`
- MacOS: `/Applications/AWS VPN Client/`
- Linux: `/opt/awsvpnclient/`

> **Important**
>
> Instruksi konfigurasi preskriptif untuk produk keamanan titik akhir pihak ketiga tertentu berada di luar cakupan AWS dokumentasi karena variabilitas di seluruh versi produk dan konfigurasi. Konsultasikan dokumentasi vendor keamanan titik akhir Anda untuk petunjuk terperinci tentang mengonfigurasi pengecualian untuk produk spesifik Anda.

Hubungkan ke AWS Client VPN titik akhir menggunakan klien OpenVPN

Anda dapat membuat koneksi ke titik akhir VPN Klien menggunakan aplikasi klien Open VPN umum. Klien VPN didukung pada sistem operasi berikut:

- Windows

  Gunakan sertifikat dan kunci pribadi dari Windows Certificate Store. Setelah Anda membuat sertifikat dan kunci, Anda dapat membuat koneksi AWS Klien menggunakan aplikasi klien OpenVPN GUI atau OpenVPN GUI Connect Client. Untuk langkah-langkah untuk membuat sertifikat dan kunci, lihatBuat koneksi VPN menggunakan sertifikat di Windows.

- macOS

  Buat koneksi VPN menggunakan file konfigurasi untuk mac OS-based Tunnelblick atau untuk VPN AWS Klien. Untuk informasi selengkapnya, lihat Buat koneksi VPN di macOS.

- Linux

  Buat koneksi VPN di Linux menggunakan antarmuka OpenVPN - Network Manager atau aplikasi OpenVPN. Untuk menggunakan antarmuka OpenVPN - Network Manager Anda harus terlebih dahulu menginstal modul manajer jaringan jika belum diinstal. Untuk informasi selengkapnya, lihat Buat koneksi VPN di Linux.

- Android dan iOS

  Buat koneksi VPN menggunakan aplikasi klien OpenVPN di perangkat Android atau iOS. Untuk mengetahui informasi selengkapnya, lihat Koneksi VPN klien di Android dan iOS.

Important

Jika titik akhir VPN Klien telah dikonfigurasi untuk menggunakan otentikasi SAML-based federasi, Anda tidak dapat menggunakan klien OpenVPN-based VPN untuk menyambung ke titik akhir VPN Klien. Ini termasuk ARM-based arsitektur apa pun. Jika Anda menggunakan perangkat dengan prosesor ARM (seperti Apple Silicon Mac atau perangkat ARM-based Windows), Anda harus menggunakan titik akhir SAML-based VPN dengan klien yang AWS disediakan alih-alih klien OpenVPN.

Aplikasi klien

- Hubungkan ke AWS Client VPN titik akhir menggunakan aplikasi klien Windows
- Hubungkan ke AWS Client VPN titik akhir menggunakan aplikasi klien macOS
- Hubungkan ke AWS Client VPN titik akhir menggunakan aplikasi klien OpenVPN
- AWS Client VPN koneksi pada aplikasi Android dan iOS

Hubungkan ke AWS Client VPN titik akhir menggunakan aplikasi klien Windows

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan klien Windows-based VPN.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Untuk informasi pemecahan masalah, lihat Pemecahan Masalah AWS Koneksi VPN klien dengan Windows-based klien.

> **Important**
>
> Jika titik akhir VPN Klien telah dikonfigurasi untuk menggunakan otentikasi SAML-based federasi, Anda tidak dapat menggunakan klien OpenVPN-based VPN untuk menyambung ke titik akhir VPN Klien. Ini termasuk ARM-based arsitektur apa pun. Jika Anda menggunakan perangkat dengan prosesor ARM (seperti Apple Silicon Mac atau perangkat ARM-based Windows), Anda harus menggunakan titik akhir SAML-based VPN dengan klien yang AWS disediakan alih-alih klien OpenVPN.

Tugas

- Gunakan sertifikat dan buat AWS Koneksi VPN klien pada Windows

Gunakan sertifikat dan buat AWS Koneksi VPN klien pada Windows

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 sertifikat dan membuat koneksi

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, lihat Cara: Melihat sertifikat dengan snap-in MMC di 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 H ak untuk melihat penyimpanan sertifikat komputer lokal di situs web Microsoft.
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, lihat Cara: Mengambil Tanda Jempol Sertifikat di situs web Microsoft.

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```
5. Setelah Anda menyelesaikan konfigurasi, gunakan OpenVPN untuk membuat koneksi VPN dengan melakukan salah satu hal berikut:

   - Gunakan aplikasi klien OpenVPN GUI
     1. Mulai aplikasi klien OpenVPN.
     2. Pada bilah tugas Windows, pilih Show/Hide ikon. Right-click OpenVPN GUI, lalu pilih Impor file.

3. Di kotak dialog Buka, pilih file konfigurasi yang Anda terima dari administrator Client VPN dan pilih Buka.
4. Pada bilah tugas Windows, pilih Show/Hide ikon. Right-click OpenVPN GUI, lalu pilih Connect.

- Gunakan OpenVPN GUI Connect Client
  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 ke AWS Client VPN titik akhir menggunakan aplikasi klien macOS

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan klien Mac OS-based VPN, Tunnelblick atau AWS Klien VPN.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Untuk informasi pemecahan masalah, lihat Pemecahan Masalah AWS Koneksi VPN klien dengan klien macOS.

> **Important**
>
> Jika titik akhir VPN Klien telah dikonfigurasi untuk menggunakan otentikasi SAML-based federasi, Anda tidak dapat menggunakan klien OpenVPN-based VPN untuk menyambung ke titik akhir VPN Klien. Ini termasuk ARM-based arsitektur apa pun. Jika Anda menggunakan perangkat dengan prosesor ARM (seperti Apple Silicon Mac atau perangkat ARM-based Windows), Anda harus menggunakan titik akhir SAML-based VPN dengan klien yang AWS disediakan alih-alih klien OpenVPN.

Topik

- Menetapkan AWS Client VPN koneksi pada macOS

Menetapkan AWS Client VPN koneksi pada macOS

Anda dapat membuat koneksi VPN menggunakan aplikasi klien Tunnelblick di komputer macOS.

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

Untuk membuat koneksi VPN menggunakan Tunnelblick

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.

Untuk membuat koneksi VPN menggunakan AWS VPN klien.

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 ke AWS Client VPN titik akhir menggunakan aplikasi klien OpenVPN

Bagian ini menjelaskan cara membuat koneksi VPN menggunakan OpenVPN - Network Manager atau OpenVPN.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

Untuk informasi pemecahan masalah, lihat Pemecahan Masalah AWS Koneksi VPN klien dengan Linux-based klien.

> **Important**
>
> Jika titik akhir VPN Klien telah dikonfigurasi untuk menggunakan otentikasi SAML-based federasi, Anda tidak dapat menggunakan klien OpenVPN-based VPN untuk menyambung ke titik akhir VPN Klien. Ini termasuk ARM-based arsitektur apa pun. Jika Anda menggunakan perangkat dengan prosesor ARM (seperti Apple Silicon Mac atau perangkat ARM-based Windows), Anda harus menggunakan titik akhir SAML-based VPN dengan klien yang AWS disediakan alih-alih klien OpenVPN.

Topik

- Menetapkan AWS Client VPN koneksi di Linux

Menetapkan AWS Client VPN koneksi di Linux

Buat koneksi VPN menggunakan GUI Network Manager pada komputer Ubuntu atau aplikasi OpenVPN.

Untuk membuat koneksi VPN menggunakan OpenVPN - Network Manager

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.

Untuk membuat koneksi VPN menggunakan OpenVPN

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
```

AWS Client VPN koneksi pada aplikasi Android dan iOS

Important

Jika titik akhir VPN Klien telah dikonfigurasi untuk menggunakan otentikasi SAML-based federasi, Anda tidak dapat menggunakan klien OpenVPN-based VPN untuk menyambung ke titik akhir VPN Klien. Ini termasuk ARM-based arsitektur apa pun. Jika Anda menggunakan perangkat dengan prosesor ARM (seperti Apple Silicon Mac atau perangkat ARM-based Windows), Anda harus menggunakan titik akhir SAML-based VPN dengan klien yang AWS disediakan alih-alih klien OpenVPN.

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 lebih lanjut tentang mengunduh dan menggunakan aplikasi klien OpenVPN untuk iOS atau Android, lihat Panduan Pengguna OpenVPN Connect di situs web OpenVPN.

Sebelum memulai, pastikan administrator Client VPN telah membuat titik akhir Client VPN dan memberi Anda file konfigurasi titik akhir Client VPN. Jika Anda ingin terhubung ke beberapa profil secara bersamaan, Anda memerlukan file konfigurasi untuk setiap profil.

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

Pemecahan Masalah AWS Koneksi VPN klien

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
- Kirim log diagnostik ke AWS Dukungan di AWS klien yang disediakan
- Pemecahan Masalah AWS Koneksi VPN klien dengan Windows-based klien
- Pemecahan Masalah AWS Koneksi VPN klien dengan klien macOS
- Pemecahan Masalah AWS Koneksi VPN klien dengan Linux-based klien
- Pemecahan masalah umum AWS Masalah VPN klien

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 Dukungan di AWS klien yang disediakan

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

Setelah Anda mengirim file, kami memberi Anda nomor referensi yang dapat Anda berikan AWS Dukungan sehingga mereka dapat langsung mengakses file.

Langkah-langkahnya tergantung pada versi AWS disediakan klien yang Anda gunakan. Untuk memeriksa versi Anda, buka Tentang jendela. Di Windows dan Linux, pilih Bantuan, Tentang AWS Klien VPN. Di macOS, pilih AWS Klien VPN, Tentang AWS Klien VPN.

Kirim log diagnostik (versi 6.0 dan yang lebih baru)

Langkah-langkah berikut adalah sama untuk Windows, macOS, dan Linux.

Untuk mengirim log diagnostik menggunakan AWS disediakan klien versi 6.0 atau yang lebih baru

1. Buka AWS Klien VPN aplikasi.
2. Memilih Tindakan lain, Kirim log diagnostik.
3. Pada Log Diagnostik halaman, pilih Kirim log diagnostik.
4. Perhatikan nomor referensi dari jendela konfirmasi. Anda dapat menyalinnya ke clipboard Anda dari jendela konfirmasi.

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

Anda juga dapat mengirim log diagnostik dengan menggunakan `aws-vpn-client send-diagnostic-logs` perintah. Untuk informasi selengkapnya, lihat kirim log-diagnostik.

Mengirim log diagnostik (versi lebih awal dari 6.0)

Sebelum Anda mengirim file, Anda harus setuju untuk mengizinkan AWS Dukungan untuk mengakses log diagnostik Anda.

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

Untuk mengirim log diagnostik menggunakan AWS disediakan klien untuk Windows

1. Buka AWS Klien VPN aplikasi.
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 Dukungan, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan AWS disediakan klien untuk macOS

1. Buka AWS Klien VPN aplikasi.
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 Dukungan, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan AWS menyediakan klien untuk Ubuntu

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

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

Pemecahan Masalah AWS Koneksi VPN klien dengan Windows-based klien

Bagian berikut berisi informasi tentang masalah yang mungkin Anda miliki saat menggunakan Windows-based klien untuk terhubung ke titik akhir VPN Klien.

AWS menyediakan log peristiwa klien

Yang AWS klien disediakan membuat log peristiwa dan menyimpannya di lokasi berikut di komputer Anda.

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

> **Note**
>
> Untuk versi 6.0 dan yang lebih baru, log disimpan di lokasi berikut.

```
%USERPROFILE%\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_'.

Yang AWS asalkan klien 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
```

Note

Untuk versi 6.0 dan yang lebih baru, log layanan disimpan di lokasi berikut.

```
C:\ProgramData\Amazon\AWSVPNClient\logs\
```

Topik-topik penyelesaian masalah

- Profil atau preferensi hilang setelah upgrade ke versi 6.0
- Koneksi tetap aktif saat rute VPN tumpang tindih dengan IP titik akhir
- Client tidak dapat mengoneksikan
- Klien tidak dapat terhubung dengan “tidak TAP-Windows adaptor” pesan log
- Client berada dalam status mengoneksikan ulang.
- Proses koneksi VPN berhenti secara tiba-tiba
- Aplikasi gagal diluncurkan
- Client tidak dapat membuat profil
- VPN terputus dengan pesan pop up
- Kerusakan klien terjadi pada PC Dell menggunakan Windows 10 atau 11

- OpenVPN GUI
- OpenVPN mengoneksikan client
- Tidak dapat me-resolve DNS
- Alias PKI tidak ditemukan

Profil atau preferensi hilang setelah upgrade ke versi 6.0

Masalah

Setelah memutakhirkan AWS disediakan klien ke versi 6.0 atau yang lebih baru, satu atau lebih profil VPN yang dikonfigurasi sebelumnya tidak muncul di klien, dan preferensi mungkin diatur ulang ke defaultnya.

Penyebab

Versi 6.0 memperkenalkan arsitektur baru yang menyimpan data konfigurasi di lokasi baru di seluruh sistem. Pada peluncuran pertama, klien secara otomatis memigrasikan profil dan preferensi dari lokasi sebelumnya. Migrasi adalah upaya terbaik: jika profil individu tidak dapat dimigrasi, profil tersebut dilewati dan profil yang tersisa masih dimigrasi. Klien tidak menghapus asli Anda `.ovpn` file konfigurasi.

Untuk menemukan profil mana yang tidak dimigrasi dan mengapa, cari entri berikut di log layanan.

```
Skipping profile due to migration error (partial migration)
```

Solusi

Unduh file konfigurasi titik akhir baru dari titik akhir VPN Klien Anda dan impor ulang. Untuk petunjuk tentang cara mengunduh file konfigurasi, lihat Konfigurasi Klien Ekspor di AWS Client VPN Panduan Administrator. Untuk petunjuk tentang cara menambahkan profil, lihat the section called “Hubungkan menggunakan klien”.

Jika Anda tidak dapat menemukan titik akhir atau tidak memiliki akses ke portal layanan mandiri, hubungi administrator VPN Anda untuk mendapatkan file konfigurasi baru.

Koneksi tetap aktif saat rute VPN tumpang tindih dengan IP titik akhir

Masalah

Ketika rute VPN tumpang tindih dengan alamat IPv4 publik dari titik akhir VPN Klien, koneksi tetap berjalan dengan versi 6.0 dan yang lebih baru pada titik akhir UDP dan TCP. Dengan versi 5.x, koneksi tetap aktif di titik akhir TCP tetapi turun dan terhubung kembali pada titik akhir UDP. Di platform lain, koneksi terputus dan terhubung kembali.

Penyebab

Secara default, Windows menyimpan lalu lintas untuk koneksi yang ada pada antarmuka jaringan tempat koneksi dibuat. Perilaku ini dikenal sebagai model host yang kuat. Versi 5.x mengatur koneksi UDP secara berbeda, sehingga lalu lintas mengikuti rute VPN.

Solusi

Ini adalah perbedaan yang diharapkan antara 5.x dan 6.x, dan tidak ada tindakan yang diperlukan.

Client tidak dapat mengoneksikan

Masalah

Yang AWS asalkan klien tidak dapat terhubung ke titik akhir VPN Klien.

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 “tidak TAP-Windows adaptor” pesan log

Masalah

Yang AWS asalkan klien tidak dapat terhubung ke titik akhir VPN Klien dan pesan kesalahan berikut muncul di log aplikasi: “Tidak ada TAP-Windows adaptor pada sistem ini. Anda harus dapat membuat TAP-Windows adaptor dengan pergi ke Mulai -> Semua Program -> TAP-Windows -> Utilitas -> Tambahkan yang baru TAP-Windows adaptor ethernet virtual”.

Solusi

Anda dapat memperbaiki masalah ini dengan mengambil satu atau beberapa tindakan berikut:

- Mulai ulang TAP-Windows adaptor.
- Instal ulang TAP-Windows pengemudi.
- Buat yang baru TAP-Windows adaptor.

Client berada dalam status mengoneksikan ulang.

Masalah

Yang AWS asalkan klien mencoba terhubung ke titik akhir VPN Klien, 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 sesi VPN dengan memilih Putuskan sambungan di AWS Jendela VPN Client, 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 pada komputer Anda. Perangkat lunak ini diperlukan untuk dapat menjalankan client.

Solusi

Jalankan kembali AWS menyediakan installer klien untuk menginstal semua dependensi yang diperlukan.

Aplikasi gagal diluncurkan

Masalah

Pada Windows 7, AWS asalkan klien tidak diluncurkan saat 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 AWS menyediakan installer klien 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 .

VPN terputus dengan pesan pop up

Masalah

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

Penyebab

TAP-Windows adaptor tidak berisi deskripsi yang diperlukan.

Solusi

Jika `Description` bidang tidak cocok di bawah ini, pertama-tama hapus TAP-Windows adaptor, lalu jalankan kembali AWS menyediakan installer klien 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
```

Kerusakan klien terjadi pada PC Dell menggunakan Windows 10 atau 11

Masalah

Pada PC Dell tertentu (desktop dan laptop) yang menjalankan Windows 10 atau 11, kerusakan dapat terjadi saat Anda menjelajahi sistem file Anda untuk mengimpor file konfigurasi VPN. Jika masalah ini terjadi, Anda akan melihat pesan seperti berikut ini di log AWS klien yang 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 Cadangan dan Pemulihan Dell di Windows 10 dan 11 dapat menyebabkan konflik dengan AWS menyediakan klien, terutama dengan tiga DLL berikut:

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

Solusi

Untuk menghindari masalah ini, pertama-tama pastikan klien Anda sudah up to date dengan versi terbaru AWS klien yang disediakan. Pergi ke AWS Unduhan VPN Klien dan jika versi yang lebih baru tersedia, tingkatkan ke versi terbaru.

Selain itu, lakukan salah satu hal berikut:

- Jika Anda menggunakan aplikasi Dell Backup and Recovery, pastikan aplikasi tersebut sudah mutakhir. SEBUAH Postingan forum Dell menyatakan bahwa masalah ini diselesaikan di versi aplikasi yang lebih baru.
- Jika Anda tidak menggunakan aplikasi Dell Backup and Recovery, beberapa tindakan masih perlu dilakukan 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 Dell Backup and Recovery berfungsi sepenuhnya.

Hapus atau ganti nama file DLL

1. Buka Windows Explorer dan telusuri ke lokasi di mana Dell Backup and Recovery diinstal. Biasanya diinstal 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 mana pun akan mencegahnya dimuat.

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

   Anda dapat mengganti nama file dengan menambahkan ".bak" ke akhir nama file, misalnya, DBROverlayIconBackuped.dll.bak.

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 AWS Koneksi VPN klien dengan klien 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.

AWS menyediakan log peristiwa klien

The AWS klien 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_'.

The AWS asalkan klien menggunakan daemon klien untuk melakukan operasi root. Log daemon disimpan di lokasi berikut di komputer Anda.

```
/var/log/AWSVPNClient/
```

The AWS klien disediakan menyimpan file konfigurasi di lokasi berikut di komputer Anda.

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

Topik-topik penyelesaian masalah

- Profil atau preferensi hilang setelah upgrade ke versi 6.0
- Instalasi gagal saat menurunkan versi dari versi 6.0 atau yang lebih baru
- Client tidak dapat mengoneksikan
- Client berada dalam status mengoneksikan ulang.
- Client tidak dapat membuat profil
- Alat pembantu diperlukan kesalahan
- Pemandangan terowongan
- Algoritma cipher 'AES-256-GCM'tidak ditemukan
- Koneksi berhenti merespons dan mengatur ulang
- Penggunaan kunci yang diperpanjang (EKU)
- Sertifikat sudah kedaluwarsa
- OpenVPN
- DNS tidak dapat di-resolve

Profil atau preferensi hilang setelah upgrade ke versi 6.0

Masalah

Setelah memutakhirkan AWS disediakan klien ke versi 6.0 atau yang lebih baru, satu atau lebih profil VPN yang dikonfigurasi sebelumnya tidak muncul di klien, dan preferensi mungkin diatur ulang ke defaultnya.

Penyebab

Versi 6.0 memperkenalkan arsitektur baru yang menyimpan data konfigurasi di lokasi baru di seluruh sistem. Pada peluncuran pertama, klien secara otomatis memigrasikan profil dan preferensi dari lokasi sebelumnya. Migrasi adalah upaya terbaik: jika profil individu tidak dapat dimigrasi, profil tersebut dilewati dan profil yang tersisa masih dimigrasi. Klien tidak menghapus asli Anda `.ovpn` file konfigurasi.

Untuk menemukan profil mana yang tidak dimigrasi dan mengapa, cari entri berikut di log daemon.

```
Skipping profile due to migration error (partial migration)
```

Solusi

Unduh file konfigurasi titik akhir baru dari titik akhir VPN Klien Anda dan impor ulang. Untuk petunjuk tentang cara mengunduh file konfigurasi, lihat Konfigurasi Klien Ekspor di AWS Client VPN Panduan Administrator. Untuk petunjuk tentang cara menambahkan profil, lihat the section called “Hubungkan menggunakan klien”.

Jika Anda tidak dapat menemukan titik akhir atau tidak memiliki akses ke portal layanan mandiri, hubungi administrator VPN Anda untuk mendapatkan file konfigurasi baru.

Instalasi gagal saat menurunkan versi dari versi 6.0 atau yang lebih baru

Masalah

Anda memiliki versi 6.0 atau yang lebih baru dari AWS asalkan klien diinstal, dan Anda mencoba menginstal versi sebelumnya (misalnya, 5.x) di atasnya. Penginstal menampilkan pesan berikut dan instalasi tidak selesai.

```
The Installer encountered an error that caused the installation to fail. Contact the
 software manufacturer for assistance.
```

Penyebab

The AWS asalkan klien tidak mendukung menginstal versi sebelumnya di atas yang lebih baru (downgrade), dan melakukannya dapat membuat klien dalam keadaan yang tidak terduga.

Solusi

Instal versi terbaru dari AWS menyediakan klien lagi untuk memulihkan klien yang berfungsi. Untuk pindah ke versi sebelumnya, pertama-tama gunakan aplikasi Uninstall AWS VPN Client untuk menghapus klien. Kemudian instal versi lama yang Anda inginkan.

Client tidak dapat mengoneksikan

Masalah

The AWS asalkan klien tidak dapat terhubung ke titik akhir VPN Klien.

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

The AWS asalkan klien mencoba terhubung ke titik akhir VPN Klien, 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 sesi VPN dengan memilih Putuskan sambungan di AWS Jendela VPN Client, 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 .

Alat pembantu diperlukan kesalahan

Masalah

Anda mendapatkan kesalahan berikut ketika Anda mencoba menghubungkan VPN.

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

Solusi

Lihat artikel berikut tentang AWS Re: posting. Klien AWS VPN - Alat pembantu diperlukan kesalahan

Pemandangan terowongan

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.

Algoritma cipher 'AES-256-GCM'tidak 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 mendukung algoritma cipher 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 masalah Tidak Dapat Me-resolve Nama DNS Titik Akhir Client VPN dalam Panduan administrator AWS Client VPN .

Pemecahan Masalah AWS Koneksi VPN klien dengan Linux-based klien

Bagian berikut berisi informasi tentang logging, dan tentang masalah yang mungkin Anda alami saat menggunakan Linux-based klien. Pastikan bahwa Anda menjalankan versi terbaru client-client tersebut.

Topik

- AWS menyediakan log peristiwa klien
- Profil atau preferensi hilang setelah upgrade ke versi 6.0
- Kueri DNS masuk ke server nama default
- OpenVPN (baris perintah)
- OpenVPN melalui Pengelola Jaringan (GUI)

AWS menyediakan log peristiwa klien

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

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

The AWS proses daemon klien yang disediakan menyimpan file log di lokasi berikut pada sistem Anda:

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

> **Note**
>
> Untuk versi 6.0 dan yang lebih baru, log daemon disimpan di lokasi berikut.
>
> ```
> /var/log/awsvpnclient/
> ```

Misalnya, Anda dapat memeriksa file log berikut untuk menemukan kesalahan di DNS up/down skrip yang menyebabkan koneksi gagal:

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

Profil atau preferensi hilang setelah upgrade ke versi 6.0

Masalah

Setelah memutakhirkan AWS disediakan klien ke versi 6.0 atau yang lebih baru, satu atau lebih profil VPN yang dikonfigurasi sebelumnya tidak muncul di klien, dan preferensi mungkin diatur ulang ke defaultnya.

Penyebab

Versi 6.0 memperkenalkan arsitektur baru yang menyimpan data konfigurasi di lokasi baru di seluruh sistem. Pada peluncuran pertama, klien secara otomatis memigrasikan profil dan preferensi dari lokasi sebelumnya. Migrasi adalah upaya terbaik: jika profil individu tidak dapat dimigrasi, profil tersebut dilewati dan profil yang tersisa masih dimigrasi. Klien tidak menghapus asli Anda `.ovpn` file konfigurasi.

Untuk menemukan profil mana yang tidak dimigrasi dan mengapa, cari entri berikut di log daemon.

```
Skipping profile due to migration error (partial migration)
```

Solusi

Unduh file konfigurasi titik akhir baru dari titik akhir VPN Klien Anda dan impor ulang. Untuk petunjuk tentang cara mengunduh file konfigurasi, lihat Konfigurasi Klien Ekspor di AWS Client VPN Panduan Administrator. Untuk petunjuk tentang cara menambahkan profil, lihat the section called “Hubungkan menggunakan klien”.

Jika Anda tidak dapat menemukan titik akhir atau tidak memiliki akses ke portal layanan mandiri, hubungi administrator VPN Anda untuk mendapatkan file konfigurasi baru.

Kueri DNS masuk ke server nama default

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 diselesaikan dengan sistem, layanan yang tersedia pada sistem Linux, yang berfungsi sebagai bagian sentral 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 masalah Tidak Dapat Me-resolve Nama DNS Titik Akhir Client VPN dalam Panduan administrator AWS Client VPN .

Pemecahan masalah umum AWS Masalah VPN klien

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 AWS Pembaruan Panduan Pengguna VPN Klien.

Perubahan	Deskripsi	Tanggal
AWS klien yang disediakan (6.2.2) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	5 November 2026
AWS klien yang disediakan (6.2.2) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	5 November 2026
AWS klien yang disediakan (6.2.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Oktober 9, 2026
AWS klien yang disediakan (6.2.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2026
AWS klien yang disediakan (6.2.0) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2026
AWS klien yang disediakan (6.2.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2026
AWS klien yang disediakan (6.1.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	25 September 2026
AWS klien yang disediakan (6.1.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	25 September 2026
AWS klien yang disediakan (6.1.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	September 24, 2026
AWS klien yang disediakan (6.1.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	September 24, 2026

AWS klien yang disediakan (6.0.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 22, 2026
AWS klien yang disediakan untuk macOS sekarang mendukung macOS 27 Golden Gate	Untuk informasi selengkapnya tentang persyaratan macOS, lihat Persyaratan VPN Klien untuk macOS.	September 14, 2026
AWS klien yang disediakan (6.0.3) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	September 14, 2026
AWS klien yang disediakan (6.0.3) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 27, 2026
AWS klien yang disediakan (5.4.1) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Agustus 25, 2026
AWS klien yang disediakan (6.0.2) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 18, 2026
AWS klien yang disediakan (6.0.2) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2026
AWS klien yang disediakan (6.0.1) untuk Linux dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2026
AWS klien yang disediakan (6.0.1) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 7, 2026
AWS klien yang disediakan (6.0.1) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 7, 2026

AWS klien yang disediakan (6.0.0) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 4, 2026
AWS klien yang disediakan (6.0.0) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Agustus 4, 2026
AWS klien yang disediakan (5.4.3) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 23, 2026
AWS klien yang disediakan (5.4.3) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 23, 2026
AWS klien yang disediakan (5.4.2) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 20, 2026
AWS klien yang disediakan (5.4.2) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 20, 2026
AWS klien yang disediakan (5.4.1) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 9, 2026
AWS klien yang disediakan (5.4.1) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juli 6, 2026
AWS klien yang disediakan (5.4.0) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juni 22, 2026
AWS klien yang disediakan (5.4.0) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juni 22, 2026

AWS klien yang disediakan (5.4.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Juni 22, 2026
AWS klien yang disediakan (5.3.7) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Juni 15, 2026
AWS klien yang disediakan (5.3.6) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Mei 28, 2026
AWS klien yang disediakan (5.3.5) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	27 Mei 2026
AWS klien yang disediakan (5.3.3) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	18 Mei 2026
AWS klien yang disediakan (5.3.5) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	14 Mei 2026
AWS klien yang disediakan (5.3.4) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Maret 26, 2026
AWS klien yang disediakan (5.3.3) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Februari 28, 2026
AWS klien yang disediakan (5.3.4) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Februari 17, 2026
AWS klien yang disediakan (5.3.2) untuk Windows ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Februari 17, 2026

AWS klien yang disediakan (5.3.3) untuk macOS ARM64 dan x64 dirilis	Lihat catatan rilis untuk detailnya.	Desember 26, 2025
AWS klien yang disediakan (5.3.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Desember 17, 2025
AWS klien yang disediakan (5.3.2) untuk macOS x64 dirilis	Lihat catatan rilis untuk detailnya.	Oktober 27, 2025
AWS klien yang disediakan (5.3.2) untuk sistem macOS ARM64 dirilis	Dukungan sekarang ditambahkan untuk macOS ARM64-based sistem operasi. Ini termasuk yang baru AWS Client VPN versi 5.3.2 unduh khusus untuk sistem macOS ARM64. Lihat Persyaratan VPN Klien untuk macOS untuk detail lebih lanjut dan AWS Client VPN untuk catatan rilis macOS untuk tautan unduhan.	Oktober 27, 2025
AWS klien yang disediakan (5.3.1) untuk Windows x64 dan Arm64 dirilis	Lihat catatan rilis untuk detailnya.	30 September 2025
AWS klien yang disediakan untuk macOS sekarang mendukung Tahoe (26.0)	Lihat Persyaratan untuk detailnya.	25 September 2025
AWS klien yang disediakan (5.3.1) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	25 September 2025
AWS klien yang disediakan (5.3.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	September 9, 2025

AWS klien yang disediakan (5.3.0) untuk sistem Windows Arm64 dirilis	Dukungan sekarang ditambahkan untuk Windows Arm64-based sistem operasi. Ini termasuk yang baru AWS Client VPN versi 5.3.0 unduh khusus untuk sistem Windows Arm64. Lihat Klien VPN untuk Persyaratan Windows untuk detail lebih lanjut dan AWS Client VPN untuk catatan rilis Windows untuk tautan unduhan.	Agustus 26, 2025
AWS klien yang disediakan (5.3.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Agustus 14, 2025
AWS klien yang disediakan (5.3.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Agustus 14, 2025
AWS klien yang disediakan (5.3.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Agustus 14, 2025
AWS klien yang disediakan (5.2.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Juni 18, 2025
AWS klien yang disediakan (5.2.2) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Juni 2, 2025
AWS klien yang disediakan (5.2.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	April 21, 2025
AWS klien yang disediakan (5.2.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	8 April 2025
AWS klien yang disediakan (5.2.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	8 April 2025
AWS klien yang disediakan (5.2.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	8 April 2025

AWS klien yang disediakan (5.1.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Maret 17, 2025
AWS klien yang disediakan (5.1.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Maret 17, 2025
AWS klien yang disediakan (5.1.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Maret 17, 2025
Menghapus dukungan untuk macOS Monterey dan menambahkan dukungan untuk macOS Sonoma (14.0)	Lihat Persyaratan VPN Klien untuk macOS untuk detailnya.	Maret 12, 2025
Menghapus dukungan untuk Ubuntu 18.0.4 (LTS) dan Ubuntu 20.04 LTS (hanya AMD64)	Lihat Persyaratan VPN Klien untuk Linux untuk detailnya.	Maret 12, 2025
AWS klien yang disediakan (5.0.3) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Maret 6, 2025
AWS klien yang disediakan (5.0.2) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Februari 24, 2025
AWS klien yang disediakan (5.0.2) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Februari 17, 2025
AWS klien yang disediakan (5.0.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Januari 30, 2025
AWS klien yang disediakan (5.0.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Januari 22, 2025
The AWS klien yang disediakan sekarang mendukung hingga lima koneksi bersamaan	Lihat Dukungan untuk koneksi bersamaan menggunakan AWS klien yang disediakan untuk detailnya.	Januari 21, 2025

AWS klien yang disediakan (5.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Januari 21, 2025
AWS klien yang disediakan (5.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Januari 21, 2025
AWS klien yang disediakan (5.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	12 November 2024
AWS klien yang disediakan (4.1.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	12 November 2024
AWS klien yang disediakan (4.1.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	12 November 2024
AWS klien yang disediakan (4.1.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	12 November 2024
AWS klien yang disediakan (4.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	September 25, 2024
AWS klien yang disediakan (4.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	September 25, 2024
AWS klien yang disediakan (4.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 25, 2024
AWS klien yang disediakan (3.15.1) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	4 September 2024
AWS klien yang disediakan (3.14.2) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	4 September 2024
AWS klien yang disediakan (3.12.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	4 September 2024
AWS klien yang disediakan (3.14.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Agustus 22, 2024

AWS klien yang disediakan (3.15.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.14.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.12.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.14.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.13.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.11.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.12.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Juli 18, 2024
AWS klien yang disediakan (3.13.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Mei 21, 2024
AWS klien yang disediakan (3.12.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Mei 21, 2024
AWS klien yang disediakan (3.10.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Mei 21, 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.	9 November 2021
AWS klien yang disediakan untuk Windows (1.3.7) dirilis	Lihat catatan rilis untuk detailnya.	8 November 2021
AWS klien yang disediakan (1.0.3) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	8 November 2021
AWS klien yang disediakan (1.0.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2021
AWS disediakan klien untuk Windows (1.3.6) dan macOS (1.3.5) dirilis	Lihat catatan rilis untuk detailnya.	September 20, 2021
AWS disediakan klien untuk Ubuntu 18.04 LTS dan Ubuntu 20.04 LTS dirilis	Anda dapat menggunakan AWS-disediakan klien di Ubuntu 18.04 LTS dan Ubuntu 20.04 LTS.	11 Juni 2021
Dukungan untuk OpenVPN menggunakan sertifikat dari Windows Certificate System Store	Anda dapat menggunakan OpenVPN dengan sertifika t dari Penyimpanan Sistem Sertifikat Windows.	25 Februari 2021
Self-service pintu gerbang	Anda dapat mengakses portal layanan mandiri untuk mendapatkan yang terbaru AWS disediakan klien dan file konfigurasi.	29 Oktober 2020
AWS klien yang disediakan	Anda dapat menggunakan AWS menyediakan klien untuk terhubung ke titik akhir VPN Klien.	4 Februari 2020
Rilis awal	Rilis ini memperkenalkan AWS VPN klien.	18 Desember 2018

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