사용자 가이드

AWS Client VPN

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Client VPN: 사용자 가이드

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS Client VPN이란 무엇입니까? 1
Client VPN 구성 요소 1
Client VPN 구성을 위한 추가 리소스 1
Client VPN 시작하기 2
Client VPN을 사용하기 위한 사전 조건 2
1단계: VPN 클라이언트 애플리케이션 설치 2
2단계: Client VPN 엔드포인트 구성 파일 받기 3
3단계: VPN에 연결 3
Client VPN 다운로드 4
AWS 제공된 클라이언트를 사용하여 연결 5
동시 연결 지원 5
OpenVPN 지시문 6
Windows 7
요구 사항 8
클라이언트를 사용하여 연결 8
릴리스 정보 9
macOS 19
요구 사항 19
클라이언트를 사용하여 연결 20
릴리스 정보 21
Linux 32
Linux용 AWS 제공 클라이언트를 사용하여 Client VPN에 연결하기 위한 요구 사항 32
클라이언트 설치 32
클라이언트를 사용하여 연결 33
릴리스 정보 34
OpenVPN 클라이언트를 사용하여 연결 42
Windows 43
Windows에서 인증서를 사용하여 VPN 연결 설정 43
Android 및 iOS의 Client VPN 연결 45
macOS 46
macOS에서 VPN 연결 설정 46
Linux 47
Linux에서 VPN 연결 설정 48
문제 해결 49

관리자를 위한 Client VPN 엔드포인트 문제 해결 49
AWS 제공된 클라이언트 AWS Support 의에 진단 로그 전송 49
진단 로그 보내기 49
Windows 문제 해결 50
AWS 제공된 클라이언트 이벤트 로그 51
클라이언트가 연결할 수 없습니다. 52
클라이언트가 연결할 수 없고 "no TAP-Windows adapters" 로그 메시지가 표시됨 52
클라이언트가 다시 연결 중 상태로 멈췄습니다. 53
VPN 연결 프로세스가 예기치 않게 종료됩니다. 53
애플리케이션을 시작하지 못했습니다. 53
클라이언트가 프로필을 만들 수 없습니다. 54
팝업 메시지와 함께 VPN 연결 해제 54
Windows 10 또는 11을 사용하는 Dell PC에서 클라이언트 충돌 발생 55
OpenVPN GUI 56
OpenVPN 연결 클라이언트 57
DNS를 확인할 수 없습니다. 57
PKI 별칭 누락 58
macOS 문제 해결 58
AWS 제공된 클라이언트 이벤트 로그 58
클라이언트가 연결할 수 없습니다. 59
클라이언트가 다시 연결 중 상태로 멈췄습니다. 60
클라이언트가 프로필을 만들 수 없습니다. 60
Helper 도구 필요함 오류 61
Tunnelblick 61
암호 알고리즘 'AES-256-GCM'을 찾을 수 없습니다. 62
연결 응답이 중지되고 재설정됨 62
확장 키 사용(EKU) 63
만료된 인증서 64
OpenVPN 64
DNS를 확인할 수 없습니다. 64
Linux 문제 해결 65
AWS 제공된 클라이언트 이벤트 로그 51
DNS 쿼리는 기본 네임서버로 이동합니다. 66
OpenVPN(명령줄) 67
네트워크 관리자를 통한 OpenVPN(GUI) 68
공통 문제 69

TLS 키 협상 실패 69
문서 기록 70
..... lxxviii

AWS Client VPN이란 무엇입니까?

AWS Client VPN은 온프레미스 네트워크의 리소스와 리소스에 안전하게 액세스할 AWS 수 있는 관리형 클라이언트 기반 VPN 서비스입니다.

이 안내서에서는 디바이스의 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 대한 VPN 연결을 설정하는 단계를 제공합니다.

Client VPN 구성 요소

다음은 AWS Client VPN을 사용하기 위한 주요 구성 요소입니다.

- Client VPN 엔드포인트 - Client VPN 관리자가 AWS에서 Client VPN 엔드포인트를 생성하고 구성합니다. 관리자는 사용자가 VPN 연결을 설정할 때 사용자가 액세스할 수 있는 네트워크와 리소스를 제어합니다.
- VPN 클라이언트 애플리케이션 - Client VPN 엔드포인트에 연결하고 보안 VPN 연결을 설정하는 데 사용하는 소프트웨어 애플리케이션입니다.
- Client VPN 엔드포인트 구성 파일 - Client VPN 관리자가 제공한 구성 파일입니다. 파일에는 Client VPN 엔드포인트에 대한 정보와 VPN 연결을 설정하는 데 필요한 인증서가 포함되어 있습니다. 선택한 VPN 클라이언트 애플리케이션에 이 파일을 로드합니다. AWS 제공된 클라이언트를 사용하면 5개의 동시 세션에 연결할 수 있으며, 각 세션에는 Client VPN 관리자가 제공하는 자체 구성 파일이 있습니다. 동시 세션에 대한 자세한 내용은 섹션을 참조하세요동시 연결 지원.

Client VPN 구성을 위한 추가 리소스

Client VPN 관리자인 경우 Client VPN 엔드포인트 생성 및 구성에 대한 자세한 내용은 AWS Client VPN 관리자 안내서를 참조하세요.

시작하기 AWS Client VPN

VPN 세션을 설정하려면 먼저 Client VPN 관리자가 Client VPN 엔드포인트를 생성하고 구성해야 합니다. 관리자는 VPN 세션을 설정한 사용자가 액세스할 수 있는 네트워크와 리소스를 제어합니다. 그런 다음 VPN 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 연결하고 보안 VPN 연결을 설정합니다.

Client VPN 엔드포인트 생성이 필요한 관리자인 경우 AWS Client VPN 관리자 안내서를 참조하세요.

주제

- Client VPN을 사용하기 위한 사전 조건
- 1단계: VPN 클라이언트 애플리케이션 설치
- 2단계: Client VPN 엔드포인트 구성 파일 받기
- 3단계: VPN에 연결
- 셀프 서비스 포털 AWS Client VPN 에서 다운로드

Client VPN을 사용하기 위한 사전 조건

VPN 연결을 설정하려면 다음이 필요합니다.

- 인터넷 액세스
- 지원되는 디바이스
- 지원되는 Windows, macOS 또는 Linux 버전입니다.
- SAML 기반 연동 인증(Single Sign-On)을 사용하는 Client VPN 엔드포인트의 경우 다음 브라우저 중 하나를 사용합니다.
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

1단계: VPN 클라이언트 애플리케이션 설치

AWS 제공 클라이언트 또는 다른 OpenVPN 기반 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 연결하고 VPN 연결을 설정할 수 있습니다.

관리자가 애플리케이션에 대한 엔드포인트 구성 파일을 생성했는지 여부에 따라 두 가지 방법 중 하나를 통해 Client VPN 애플리케이션을 다운로드할 수 있습니다.

- 관리자가 엔드포인트 구성 파일을 설정하지 않은 경우 AWS Client VPN 다운로드에서 클라이언트를 다운로드하고 설치합니다. 애플리케이션을 다운로드하고 설치한 후 the section called "2단계: Client VPN 엔드포인트 구성 파일 받기"로 이동하여 관리자로부터 엔드포인트 구성 파일을 가져옵니다. 여러 프로필에 연결하는 경우 각 프로필에 대한 구성 파일이 필요합니다.
- 관리자가 엔드포인트 구성 파일을 이미 사전 구성한 경우 셀프 서비스 포털에서 구성 파일과 함께 Client VPN 애플리케이션을 다운로드할 수 있습니다. 셀프 서비스 포털에서 클라이언트 및 구성 파일을 다운로드하는 단계는 the section called "Client VPN 다운로드" 섹션을 참조하세요. 애플리케이션 및 파일을 다운로드하고 설치한 후 the section called "3단계: VPN에 연결"로 이동합니다.

또는 VPN 연결을 설정하려는 디바이스에서 OpenVPN 클라이언트 애플리케이션을 다운로드하여 설치합니다.

2단계: Client VPN 엔드포인트 구성 파일 받기

관리자로부터 Client VPN 엔드포인트 구성 파일을 가져옵니다. 구성 파일에는 Client VPN 엔드포인트에 대한 정보와 VPN 연결을 설정하는 데 필요한 인증서가 포함되어 있습니다.

또는 Client VPN 관리자가 Client VPN 엔드포인트에 대한 셀프 서비스 포털을 구성한 경우 AWS 제공된 클라이언트의 최신 버전과 Client VPN 엔드포인트 구성 파일의 최신 버전을 직접 다운로드할 수 있습니다. 자세한 내용은 셀프 서비스 포털 AWS Client VPN 에서 다운로드 단원을 참조하십시오.

3단계: VPN에 연결

Client VPN 엔드포인트 구성 파일을 AWS 제공된 클라이언트 또는 OpenVPN 클라이언트 애플리케이션으로 가져와 VPN에 연결합니다. AWS 제공된 클라이언트에 대한 하나 이상의 엔드포인트 구성 파일 가져오기를 포함하여 VPN에 연결하는 단계는 다음 주제를 참조하세요.

- AWS 제공된 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결
- OpenVPN 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결

Active Directory 인증을 사용하는 Client VPN 엔드포인트의 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 디렉터리에 대해 Multi-Factor Authentication(MFA)이 활성화된 경우 MFA 코드를 입력하라는 메시지도 표시됩니다.

SAML 기반 페더레이션 인증(Single Sign-On)을 사용하는 Client VPN 엔드포인트의 경우 AWS 제공된 클라이언트가 컴퓨터에서 브라우저 창을 엽니다. Client VPN 엔드포인트에 연결하기 전에 회사 자격 증명을 입력하라는 메시지가 표시됩니다.

셀프 서비스 포털 AWS Client VPN 에서 다운로드

셀프 서비스 포털은 AWS 제공된 클라이언트의 최신 버전과 Client VPN 엔드포인트 구성 파일의 최신 버전을 다운로드할 수 있는 웹 페이지입니다. Client VPN 엔드포인트 관리자가 Client VPN 클라이언트에 대해 하나 이상의 구성 파일을 미리 구성한 경우이 포털에서 해당 구성 파일과 함께 해당 Client VPN 애플리케이션을 다운로드하고 설치할 수 있습니다.

> **Note**
>
> 관리자가 셀프 서비스 포털을 구성하려는 경우 AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트를 참조하세요.

시작하기 전에 다운로드할 각 Client VPN 엔드포인트의 ID가 있어야 합니다. Client VPN 엔드포인트 관리자는 ID를 제공하거나 ID가 포함된 셀프 서비스 포털 URL을 제공할 수 있습니다. 여러 엔드포인트 연결의 경우 연결하려는 각 프로필에 대한 엔드포인트 ID가 필요합니다.

셀프 서비스 포털에 액세스하려면

1. https://self-service.clientvpn.amazonaws.com/에서 셀프 서비스 포털로 이동하거나 관리자가 제공한 URL을 사용합니다.
2. 필요한 경우 Client VPN 엔드포인트의 ID(예: `cvpn-endpoint-0123456abcd123456`)를 입력합니다. Next(다음)를 선택합니다.
3. 사용자 이름과 암호를 입력하고 로그인(Sign In)을 선택합니다. 이는 Client VPN 엔드포인트에 연결하는 데 사용하는 사용자 이름 및 암호와 동일합니다.
4. 셀프 서비스 포털에서 다음을 수행할 수 있습니다.
   - Client VPN 엔드포인트에 대한 최신 버전의 클라이언트 구성 파일을 다운로드합니다. 여러 엔드포인트에 연결하려면 각 엔드포인트에 대한 구성 파일을 다운로드해야 합니다.
   - 플랫폼에 AWS 제공된 클라이언트의 최신 버전을 다운로드합니다.
5. 연결 프로필을 생성하려는 각 엔드포인트 구성 파일에 대해이 단계를 반복합니다.

AWS 제공된 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결

Windows, macOS 및 Ubuntu에서 지원되는 AWS 제공된 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 있습니다. 또한 AWS 제공된 클라이언트는 최대 5개의 동시 연결과 OpenVPN 명령을 지원합니다.

주제

- 동시 연결 지원
- OpenVPN 지시문

제공된 클라이언트를 AWS 사용한 동시 연결 지원

AWS 제공된 클라이언트는가 여러 동시 세션에 연결할 수 있도록 허용합니다. 이는 여러 AWS 환경의 리소스에 액세스해야 하고 해당 리소스에 대한 엔드포인트가 다른 경우에 유용합니다. 예를 들어 현재 연결되어 있는 엔드포인트와 다른 엔드포인트의 환경에 있는 데이터베이스에 액세스해야 하지만 현재 연결을 끊고 싶지 않을 수 있습니다. AWS 제공된 클라이언트가 현재 세션에 연결할 수 있도록 하려면 관리자가 각 엔드포인트에 대해 생성한 구성 파일을 다운로드한 다음 각 파일에 대한 연결 프로파일을 생성합니다. 그런 다음 AWS 제공된 클라이언트를 사용하여 현재 열려 있는 세션과의 연결을 끊지 않고 여러 세션에 연결할 수 있습니다. 이는 AWS 제공된 클라이언트에서만 지원됩니다. 동시 세션에 연결하는 단계는 다음을 참조하세요.

- Windows용 AWS 제공 클라이언트를 사용하여 연결
- macOS용 AWS 제공 클라이언트를 사용하여 연결
- Linux용 AWS 제공 클라이언트를 사용하여 연결

여러 엔드포인트에 연결할 때 Client VPN은 검사를 구현하여 두 세션에 충돌하는 CIDR 블록 또는 라우팅 정책이 있거나 이미 전체 터널 연결에 연결되어 있는 경우와 같이 다른 열린 엔드포인트 연결과 충돌이 없는지 확인합니다. 검사에서 충돌이 발견되면 열린 연결과 충돌하지 않는 다른 연결을 선택하거나 충돌을 일으키는 열린 세션에서 연결을 끊을 때까지 연결이 설정되지 않습니다.

동시 DNS 연결이 허용됩니다. DNS 지원 연결 중 하나의 DNS 서버가 적용됩니다. DNS 서버에 따라 해당 재연결 중에 인증을 묻는 메시지가 표시될 수 있습니다.

> **Note**
> 허용되는 최대 동시 세션 수는 5개입니다.

OpenVPN 지시문

AWS 제공된 클라이언트는 다음 OpenVPN 명령을 지원합니다. 이러한 명령에 대한 자세한 내용은 OpenVPN 웹사이트의 설명서를 참조하세요.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- 암호
- 클라이언트
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb

  dhcp-option
- ifconfig-ipv6
- 비활성
- keepalive
- 키
- mssfix
- nobind

- persist-key
- persist-tun
- ping
- ping-exit
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- 원격
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- 라우팅
- route-ipv6
- server-poll-timeout
- static-challenge
- 탭-슬립
- tun-mtu
- tun-mtu-extra
- 동사
- verify-x509-name

AWS Client VPN Windows용

이 섹션에서는 Windows용 AWS 제공된 클라이언트를 사용하여 VPN 연결을 설정하는 방법을 설명합니다. AWS Client VPN 다운로드에서 클라이언트를 다운로드하여 설치할 수 있습니다. AWS 제공된 클라이언트는 자동 업데이트를 지원하지 않습니다.

요구 사항

Windows용 AWS 제공 클라이언트를 사용하려면 다음이 필요합니다.

- Windows 10 또는 Windows 11(64비트 운영 체제, x64 프로세서)
- .NET Framework 4.7.2 이상

SAML 기반 페더레이션 인증(Single Sign-On)을 사용하는 Client VPN 엔드포인트의 경우 클라이언트는 컴퓨터에 TCP 포트 8096-8115을 예약합니다.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

주제

- Windows용 AWS 제공된 클라이언트를 AWS Client VPN 사용하여에 연결
- AWS Client VPN Windows용 릴리스 정보

Windows용 AWS 제공된 클라이언트를 AWS Client VPN 사용하여에 연결

시작하기 전에 먼저 요구 사항을 읽으십시오. AWS 제공된 클라이언트는 다음 단계에서 AWS VPN 클라이언트라고도 합니다.

Windows용 AWS 제공된 클라이언트를 사용하여 연결하려면

1. [AWS VPN Client] 앱을 엽니다.
2. 파일, 프로파일 관리를 선택합니다.
3. 프로파일 추가를 선택합니다.
4. 표시 이름에 프로파일의 이름을 입력합니다.
5. VPN 구성 파일(VPN Configuration File)의 경우 Client VPN 관리자로부터 받은 구성 파일을 찾아 선택한 다음 프로파일 추가(Add Profile)를 선택합니다.
6. 여러 연결을 생성하려면 추가하려는 각 구성 파일에 대해 프로필 추가 단계를 반복합니다. 원하는 만큼 프로필을 추가할 수 있지만 최대 5개의 열린 연결만 가질 수 있습니다.
7. AWS VPN 클라이언트 창에서 연결할 프로필을 선택한 다음 연결을 선택합니다. Client VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시

지가 표시됩니다. 시작하려는 각 프로필 연결에 대해이 단계를 반복하여 최대 5개의 동시 엔드포인트를 연결합니다.

> **Note**
>
> 에 연결하는 프로필이 현재 열려 있는 세션과 충돌하는 경우 연결할 수 없습니다. 새 연결을 선택하거나 충돌을 일으키는 세션과의 연결을 해제합니다.

8. 연결에 대한 통계를 보려면 AWS VPN 클라이언트 창에서 연결을 선택하고 세부 정보 표시를 선택한 다음 세부 정보를 보려는 연결을 선택합니다.
9. 연결을 해제하려면 AWS VPN 클라이언트 창에서 연결을 선택한 다음 연결 해제를 선택합니다. 열린 연결이 여러 개 있는 경우 각 연결을 개별적으로 닫아야 합니다. 또는 Windows 작업 표시줄에서 클라이언트 아이콘을 선택한 다음 연결 해제를 선택합니다.

AWS Client VPN Windows용 릴리스 정보

다음 표에는 Windows용의 현재 및 이전 버전에 대한 릴리스 정보와 다운로드 링크가 나와 AWS Client VPN 있습니다.

> **Note**
>
> 모든 릴리스에서 사용성 및 보안 수정 사항을 지속적으로 제공합니다. 항상 모든 플랫폼의 최신 버전을 사용하는 것이 좋습니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크 및 SHA256
5.2.2	보안 태세가 개선되었습니다.	2025년 6월 2일	버전 5.2.2 다운로드 sha256: f27cb0eed7c9c5354caa5d7e37595eefbb048d7481bf6

버전	변경	날짜	다운로드 링크 및 SHA256
			98b2e5fb6 53b667c190
5.2.1	• `ping-exit` OpenVPN 플래그에 대한 지원이 추가되었습니다. • OpenSSL 라이브러리를 업데이트했습니다. • 사소한 버그 수정 및 개선	2025년 4월 21일	더 이상 지원되지 않습니다.
5.2.0	• 사소한 개선 사항. • 클라이언트 라우팅 적용에 대한 지원이 추가되었습니다.	2025년 4월 8일	더 이상 지원되지 않습니다.
5.1.0	• 비활성 제한 시간 연결 해제 후 AWS Client VPN 버전 5.0.x가 VPN에 자동으로 다시 연결하는 문제를 수정했습니다. • 사소한 버그 수정 및 개선	2025년 3월 17일	더 이상 지원되지 않습니다.
5.0.2	• 동시 연결에 대한 DNS 문제를 수정했습니다. • 새 TAP 어댑터를 설치할 때 발생하는 산발적인 문제를 수정했습니다.	2025년 2월 24일	더 이상 지원되지 않습니다.
5.0.1	Windows 클라이언트 버전 5.0.0에서 산발적인 VPN 연결 오류가 발생하는 문제를 수정했습니다.	2025년 1월 30일	더 이상 지원되지 않습니다.
5.0.0	• 동시 연결에 대한 지원이 추가되었습니다. • TAP 드라이버 버전을 업데이트했습니다. • 그래픽 사용자 인터페이스를 업데이트했습니다. • 사소한 버그 수정 및 개선	2025년 1월 21일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크 및 SHA256
4.1.0	사소한 버그 수정 및 개선	2024년 11월 12일	더 이상 지원되지 않습니다.
4.0.0	사소한 개선 사항.	2024년 9월 25일	다운로드 버전 4.0.0 sha256: 6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc
3.14.2	`mssfix` OpenVPN 플래그에 대한 지원이 추가되었습니다.	2024년 9월 4일	다운로드 버전 3.14.2 sha256: c171639d7e07e5fd48998cf76f74e6e49e5cbe3356c6264a67b4a9bf473b5f5d

버전	변경	날짜	다운로드 링크 및 SHA256
3.14.1	사소한 버그 수정 및 개선	2024년 8월 22일	다운로드 버전 3.14.1 sha256: f743a7b4bc82daa4b803c2994390529997bb57a4bb54d1f5195ab28827283335
3.14.0	• `tap-sleep` OpenVPN 플래그에 대한 지원이 추가되었습니다. • OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	다운로드 버전 3.14.0 sha256: 812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516
3.13.0	OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 7월 29일	다운로드 버전 3.13.0 sha256: c9cc896e81a74411840951e349eed9384507c53337fb703c5ec64d522c29388b

버전	변경	날짜	다운로드 링크 및 SHA256
3.12.1	Windows 클라이언트 버전 3.12.0이 일부 사용자에 대해 VPN 연결을 설정하지 못하도록 하는 문제를 수정했습니다.	2024년 7월 18일	다운로드 버전 3.12.1 sha256: 5ed34aee6c03aa281e625acdbed272896c67046364a9e5846ca697e05dbfec08
3.12.0	• 로컬 영역 네트워크 범위가 변경될 때 자동으로 다시 연결합니다. • SAML 엔드포인트와 연결 시 자동 애플리케이션 포커스를 제거했습니다.	2024년 5월 21일	더 이상 지원되지 않음
3.11.2	버전 123 이후 Chromium 기반 브라우저의 SAML 인증 문제를 해결했습니다.	2024년 4월 11일	다운로드 버전 3.11.2 sha256: 8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc

버전	변경	날짜	다운로드 링크 및 SHA256
3.11.1	• 로컬 액터가 권한이 높은 임의 명령을 실행하도록 허용할 수 있는 버퍼 오버플로 작업을 수정했습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	다운로드 버전 3.11.1 sha256: fb67b60aa837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Windows VM으로 인한 연결 문제를 해결했습니다. • 일부 LAN 구성의 연결 문제를 해결했습니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9
3.10.0	• 클라이언트 네트워크에서 NAT64 활성화 시 발생하는 연결 문제를 해결했습니다. • Hyper-V 네트워크 어댑터가 클라이언트 머신에 설치될 때 발생하는 연결 문제를 해결했습니다. • 사소한 버그 수정 및 개선	2023년 8월 24일	다운로드 버전 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f

버전	변경	날짜	다운로드 링크 및 SHA256
3.9.0	보안 태세가 개선되었습니다.	2023년 8월 3일	다운로드 버전 3.9.0 sha256: de9a3800ea23491555 40bd32bbae472404c6 36d8d8267a0e1fb217 3a8aae21ed
3.8.0	보안 태세가 개선되었습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.7.0	버전 3.6.0에서 변경 사항을 롤백했습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.6.0	보안 태세가 개선되었습니다.	2023년 7월 14일	더 이상 지원되지 않음
3.5.0	사소한 버그 수정 및 개선	2023년 4월 3일	더 이상 지원되지 않음
3.4.0	버전 3.3.0에서 변경 사항을 롤백했습니다.	2023년 3월 28일	더 이상 지원되지 않음
3.3.0	사소한 버그 수정 및 개선	2023년 3월 17일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크 및 SHA256
3.2.0	• 'verify-x509-name' OpenVPN 플래그에 대한 지원이 추가되었습니다. • 클라이언트의 업데이트된 버전을 사용할 수 있을 때 자동으로 감지합니다. • 사용 가능한 경우 새 클라이언트 버전을 자동으로 설치하는 기능이 추가되었습니다.	2023년 1월 23일	더 이상 지원되지 않음
3.1.0	보안 태세가 개선되었습니다.	2022년 5월 23일	더 이상 지원되지 않음
3.0.0	• Windows 11 지원이 추가되었습니다. • TAP Windows 드라이버 이름 지정으로 인해 다른 드라이버 이름이 영향을 받는 문제를 수정했습니다. • 페더레이션 인증을 사용할 때 배너 메시지가 표시되지 않는 문제를 수정했습니다. • 더 긴 텍스트에 대한 배너 텍스트 표시를 수정했습니다. • 보안 태세를 강화했습니다.	2022년 3월 3일	더 이상 지원되지 않음
2.0.0	• 새로운 연결이 설정된 후의 배너 텍스트에 대한 지원이 추가되었습니다. • 에코와 관련하여 풀 필터를 사용하는 기능(즉, pull-filter * echo)이 제거되었습니다. • 사소한 버그 수정 및 개선	2022년 1월 20일	더 이상 지원되지 않음
1.3.7	• 일부 경우에 페더레이션 인증 연결 시도가 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 11월 8일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크 및 SHA256
1.3.6	• OpenVPN 플래그에 대한 지원이 추가되었습니다. 추가: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • 사소한 버그 수정 및 개선	2021년 9월 20일	더 이상 지원되지 않음
1.3.5	대량 Windows 로그 파일을 삭제하는 패치입니다.	2021년 8월 16일	더 이상 지원되지 않음
1.3.4	• OpenVPN 플래그: dhcp-option에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않음
1.3.3	• OpenVPN 플래그에 대한 다음 지원이 추가되었습니다. 비활성, 풀 필터, 경로. • 연결 해제 또는 종료시 앱 충돌이 발생하는 문제가 수정되었습니다. • 백슬래시가 있는 Active Directory 사용자 이름 문제가 수정되었습니다. • 앱 외부에서 프로파일 목록을 조작할 때 앱 충돌이 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 7월 1일	더 이상 지원되지 않음
1.3.2	• IPv6 누출 방지를 구성할 때 추가합니다. • [연결(Connection)] 아래의 [세부 정보 표시(Show Details)] 옵션을 사용할 때 발생할 수 있는 충돌 문제를 수정했습니다.	2021년 5월 12일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크 및 SHA256
1.3.1	• 동일한 제목의 여러 클라이언트 인증서에 대한 지원이 추가되었습니다. 만료된 인증서는 무시됩니다. • 디스크 사용량을 줄이기 위한 로컬 로그 보존이 수정되었습니다. • 'route-ipv6' OpenVPN 지시문에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 4월 5일	더 이상 지원되지 않음
1.3.0	오류 보고, 진단 로그 전송 및 분석 등의 지원 기능이 추가되었습니다.	2021년 3월 8일	더 이상 지원되지 않음
1.2.7	• 암호화 인증서 OpenVPN 지시문에 대한 지원이 추가되었습니다. • 연결 간에 오래된 경로가 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 2월 25일	더 이상 지원되지 않음
1.2.6	사소한 버그 수정 및 개선	2020년 10월 26일	더 이상 지원되지 않음
1.2.5	• OpenVPN 구성의 댓글에 대한 지원이 추가되었습니다. • TLS 핸드셰이크 오류에 대한 오류 메시지가 추가되었습니다.	2020년 10월 8일	더 이상 지원되지 않음
1.2.4	사소한 버그 수정 및 개선	2020년 9월 1일	더 이상 지원되지 않음
1.2.3	버전 1.2.2의 변경 사항을 롤백합니다.	2020년 8월 20일	더 이상 지원되지 않음
1.2.1	사소한 버그 수정 및 개선	2020년 7월 1일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크 및 SHA256
1.2.0	• SAML 2.0 기반 페더레이션 인증에 대한 지원이 추가되었습니다. • Windows 7 플랫폼에 대한 지원이 중단되었습니다.	2020년 5월 19일	더 이상 지원되지 않음
1.1.1	사소한 버그 수정 및 개선	2020년 4월 21일	더 이상 지원되지 않음
1.1.0	• 사용자 인터페이스에 표시된 텍스트를 숨기거나 표시하는 OpenVPN 정적 질문 에코 기능에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2020년 3월 9일	더 이상 지원되지 않음
1.0.0	최초 릴리스입니다.	2020년 2월 4일	더 이상 지원되지 않음

AWS Client VPN macOS용

이 섹션에서는 macOS용 AWS 제공 클라이언트를 사용하여 VPN 연결을 설정하는 방법을 설명합니다. AWS Client VPN 다운로드에서 클라이언트를 다운로드하여 설치할 수 있습니다. AWS 제공된 클라이언트는 자동 업데이트를 지원하지 않습니다.

요구 사항

macOS에 AWS 제공된 클라이언트를 사용하려면 다음이 필요합니다.

- macOS Ventura(13.0), Sonoma(14.0) 또는 Sequoia(15.0).
- x86_64 프로세서 호환.
- SAML 기반 페더레이션 인증(Single Sign-On)을 사용하는 Client VPN 엔드포인트의 경우 클라이언트는 컴퓨터에 TCP 포트 8096-8115을 예약합니다.

> **Note**
>
> Mac을 Apple 실리콘 프로세서와 함께 사용하는 경우 클라이언트 소프트웨어를 실행하려면 Rosetta 2를 설치해야 합니다. 자세한 내용은 Apple 웹 사이트의 Rosetta 변환 환경 정보를 참조하세요.

주제

- macOS용 제공 클라이언트를 AWS Client VPNAWS 사용하여에 연결
- AWS Client VPN macOS용 릴리스 정보

macOS용 제공 클라이언트를 AWS Client VPNAWS 사용하여에 연결

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

또한 요구 사항을 읽어야 합니다. 다음 단계에서는 AWS 제공된 클라이언트를 AWS VPN 클라이언트라고도 합니다.

macOS용 AWS 제공 클라이언트를 사용하여 연결하려면

1. [AWS VPN Client] 앱을 엽니다.
2. 파일, 프로파일 관리를 선택합니다.
3. 프로파일 추가를 선택합니다.
4. 표시 이름에 프로파일의 이름을 입력합니다.
5. VPN 구성 파일(VPN Configuration File)의 경우 Client VPN 관리자로부터 받은 구성 파일을 찾아 선택한 다음 프로파일 추가(Add Profile)를 선택합니다.
6. 여러 연결을 생성하려면 추가하려는 각 구성 파일에 대해 프로필 추가 단계를 반복합니다. 원하는 만큼 프로필을 추가할 수 있지만 최대 5개의 열린 연결만 가질 수 있습니다.
7. AWS VPN 클라이언트 창에서 연결할 프로필을 선택한 다음 연결을 선택합니다. Client VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 시작하려는 각 프로필 연결에 대해이 단계를 반복하여 최대 5개의 동시 엔드포인트를 연결합니다.

> **Note**
>
> 에 연결하는 프로필이 현재 열려 있는 세션과 충돌하는 경우 연결할 수 없습니다. 새 연결을 선택하거나 세션 연결을 끊어 충돌을 일으킵니다.

8. 연결에 대한 통계를 보려면 AWS VPN 클라이언트 창에서 연결을 선택하고 세부 정보 표시를 선택한 다음 세부 정보를 보려는 연결을 선택합니다.
9. 연결을 해제하려면 AWS VPN 클라이언트 창에서 연결을 선택한 다음 연결 해제를 선택합니다. 열린 연결이 여러 개 있는 경우 각 연결을 개별적으로 닫아야 합니다.

AWS Client VPN macOS용 릴리스 정보

다음 표에는 macOS용의 현재 및 이전 버전에 대한 릴리스 정보와 다운로드 링크가 나와 AWS Client VPN 있습니다.

> **Note**
>
> 모든 릴리스에서 사용성 및 보안 수정 사항을 지속적으로 제공합니다. 항상 모든 플랫폼의 최신 버전을 사용하는 것이 좋습니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크
5.2.1	• ping-exit OpenVPN 플래그에 대한 지원이 추가되었습니다. • OpenSSL 라이브러리를 업데이트했습니다. • 보안 태세가 개선되었습니다. • 사소한 버그 수정 및 개선	2025년 6월 18일	버전 5.2.1 다운로드 sha256: 906f77fbca3334fbdcd1145dd6f2725beab82a30b9b51eafd1a25c3fe7d669eb

버전	변경	날짜	다운로드 링크
5.2.0	• 사소한 개선 사항. • 클라이언트 라우팅 적용에 대한 지원이 추가되었습니다.	2025년 4월 8일	버전 5.2.0 다운로드 sha256: f062e971a84e98d8a61caced3d7f6be322c28dab02ec81194c0f9a3e62bd8249
5.1.0	• 비활성 제한 시간 연결 해제 후 AWS Client VPN 버전 5.0.x가 VPN에 자동으로 다시 연결하는 문제를 수정했습니다. • 가 Windows 스타일 줄 끝이 있는 구성 파일에 대한 VPN 연결을 AWS Client VPN 설정하지 못하는 문제를 수정했습니다. • 사소한 버그 수정 및 개선	2025년 3월 17일	버전 5.1.0 다운로드 sha256: ef7ff34ae85a29f90212514568c93849ef6e67f30b2c83ae1494d307f7650e10
5.0.3	사소한 버그 수정 및 개선	2025년 3월 6일	버전 5.0.3 다운로드 sha256: 8ce0f91ce81c322cead3ed27948ddeda4d5a61f5ed5a6115ab8e18f5d8963f6b

버전	변경	날짜	다운로드 링크
5.0.2	연결을 선택할 때 산발적인 오류가 발생하는 문제를 수정했습니다.	2025년 2월 17일	버전 5.0.2 다운로드 sha256: e81287746 08147e65b 14f992a4b 5a6d75364 6424fe3b6 8fab23181 0addac1f7c
5.0.1	클라이언트 버전 5.0.0에서 공백이 포함된 프로필 이름에 대한 VPN 연결을 설정하지 못하는 문제를 수정했습니다.	2025년 1월 22일	버전 5.0.1 다운로드 sha256: 7d9de8c89 154c9a99b fd56b1966 00a9a09eb 6a952cb10 a7b16d01b dbadb0e57a
5.0.0	• 동시 연결에 대한 지원이 추가되었습니다. • 그래픽 사용자 인터페이스를 업데이트했습니다. • 사소한 버그 수정 및 개선	2025년 1월 21일	버전 5.0.0 다운로드 sha256:e9 c95ecdd6d 582e72e1a f0b05d03f e678f96b8 b1028b5f5 69f962902 943ecf02

버전	변경	날짜	다운로드 링크
4.1.0	사소한 버그 수정 및 개선	2024년 11월 12일	버전 4.1.0 다운로드 sha256:afe1ec8a6d7e2e1d618a6507f44a8c41db744fb55f94573e318d75bc5e96cd269
4.0.0	사소한 개선 사항.	2024년 9월 25일	다운로드 버전 4.0.0 sha256:ad574475a80b614499c97ae75612ef1ff905bb4aa1b5f7109420e80bf95aefcbd
3.12.1	`mssfix` OpenVPN 플래그에 대한 지원이 추가되었습니다.	2024년 9월 4일	다운로드 버전 3.12.1 sha256:a5c31d3e0e8bf8937682805c9ff f76ca9205875e009e949ad1b0532f449cee47

버전	변경	날짜	다운로드 링크
3.12.0	• `tap-sleep` OpenVPN 플래그에 대한 지원이 추가되었습니다. • OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	다운로드 버전 3.12.0 sha256: 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 7월 29일	다운로드 버전 3.11.0 sha256: 44b5e6f84 788bf45dd b77871d74 3e09007e1 597555850 6221b8cae a81732848f
3.10.0	• 로컬 영역 네트워크 범위가 변경될 때 자동으로 다시 연결합니다. • 네트워크 전환 중 DNS 복원 문제를 해결했습니다. • SAML 엔드포인트와 연결 시 자동 애플리케이션 포커스를 제거했습니다.	2024년 5월 21일	다운로드 버전 3.10.0 sha256: 28bf26fa1 34b01ff12703cf59ff fa4adba7c 44ceb793d ce4addd44 04e84287dd

버전	변경	날짜	다운로드 링크
3.9.2	• 버전 123 이후 Chromium 기반 브라우저의 SAML 인증 문제를 해결했습니다. • macOS Sonoma에 대한 지원이 추가되었습니다. macOS Big Sur에 대한 지원을 중단합니다. • 보안 태세가 개선되었습니다.	2024년 4월 11일	다운로드 버전 3.9.2 sha256: 374467d991e8953b5032e5b985cda80a0ea27fb5d5f23cf16c556a1568b0d480
3.9.1	• 로컬 액터가 권한이 높은 임의 명령을 실행하도록 허용할 수 있는 버퍼 오버플로 작업을 수정했습니다. • 애플리케이션 업데이트 다운로드 진행률 표시줄이 수정되었습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	다운로드 버전 3.9.1 sha256: 9bba4b27a635e75038703e2cf4cd814aa75306179fac8e500e2c7af4e899e971
3.9.0	• 일부 LAN 구성의 연결 문제를 해결했습니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8

버전	변경	날짜	다운로드 링크
3.8.0	• 클라이언트 네트워크에서 NAT64 활성화 시 발생하는 연결 문제를 해결했습니다. • 사소한 버그 수정 및 개선	2023년 8월 24일	다운로드 버전 3.8.0 sha256: d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• 보안 태세가 개선되었습니다.	2023년 8월 3일	다운로드 버전 3.7.0 sha256: 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a
3.6.0	• 보안 태세가 개선되었습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.5.0	• 버전 3.4.0에서 변경 사항을 롤백했습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.4.0	• 보안 태세가 개선되었습니다.	2023년 7월 14일	더 이상 지원되지 않음
3.3.0	• macOS Ventura(13.0)에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2023년 4월 27일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크
3.2.0	• 'verify-x509-name' OpenVPN 플래그에 대한 지원이 추가되었습니다. • 클라이언트의 업데이트된 버전을 사용할 수 있을 때 자동으로 감지합니다. • 사용 가능한 경우 새 클라이언트 버전을 자동으로 설치하는 기능이 추가되었습니다.	2023년 1월 23일	더 이상 지원되지 않음
3.1.0	• macOS Monterey에 대한 지원이 추가되었습니다. • 드라이브 유형 감지 문제가 해결되었습니다. • 보안 태세가 개선되었습니다.	2022년 5월 23일	더 이상 지원되지 않음
3.0.0	• 페더레이션 인증을 사용할 때 배너 메시지가 표시되지 않는 문제를 수정했습니다. • 더 긴 텍스트에 대한 배너 텍스트 표시를 수정했습니다. • 보안 태세를 강화했습니다.	2022년 3월 3일	더 이상 지원되지 않습니다.
2.0.0	• 새로운 연결이 설정된 후의 배너 텍스트에 대한 지원이 추가되었습니다. • 에코와 관련하여 풀 필터를 사용하는 기능(즉, pull-filter * echo)이 제거되었습니다. • 사소한 버그 수정 및 개선	2022년 1월 20일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.4.0	• 연결 중 DNS 서버 모니터링 기능을 추가했습니다. 설정은 VPN 설정과 일치하지 않을 경우 다시 구성됩니다. • 일부 경우에 페더레이션 인증 연결 시도가 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 11월 9일	더 이상 지원되지 않습니다.
1.3.5	• OpenVPN 플래그에 대한 지원이 추가되었습니다. 추가: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • 사소한 버그 수정 및 개선	2021년 9월 20일	더 이상 지원되지 않습니다.
1.3.4	• OpenVPN 플래그: dhcp-option에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않습니다.
1.3.3	• OpenVPN 플래그에 대한 다음 지원이 추가되었습니다. 비활성, 풀 필터, 경로. • 구성 파일 이름에 공백 또는 유니코드 문제가 수정되었습니다. • 연결 해제 또는 종료시 앱 충돌이 발생하는 문제가 수정되었습니다. • 백슬래시가 있는 Active Directory 사용자 이름 문제가 수정되었습니다. • 앱 외부에서 프로파일 목록을 조작할 때 앱 충돌이 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 7월 1일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.3.2	• IPv6 누출 방지를 구성할 때 추가합니다. • [연결(Connection)] 아래의 [세부 정보 표시(Show Details)] 옵션을 사용할 때 발생할 수 있는 충돌 문제를 수정했습니다. • 데몬 로그 교체를 추가합니다.	2021년 5월 12일	더 이상 지원되지 않습니다.
1.3.1	• macOS Big Sur(10.16)에 대한 지원이 추가되었습니다. • 다른 애플리케이션에서 구성한 DNS 설정이 제거되는 문제가 해결되었습니다. • 상호 인증에 유효하지 않은 인증서를 사용할 때 연결 문제가 야기되는 문제가 수정되었습니다. • 'route-ipv6' OpenVPN 지시문에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 4월 5일	더 이상 지원되지 않습니다.
1.3.0	오류 보고, 진단 로그 전송 및 분석 등의 지원 기능이 추가되었습니다.	2021년 3월 8일	더 이상 지원되지 않습니다.
1.2.5	사소한 버그 수정 및 개선	2021년 2월 25일	더 이상 지원되지 않습니다.
1.2.4	사소한 버그 수정 및 개선	2020년 10월 26일	더 이상 지원되지 않습니다.
1.2.3	• OpenVPN 구성의 댓글에 대한 지원이 추가되었습니다. • TLS 핸드셰이크 오류에 대한 오류 메시지가 추가되었습니다. • 일부 사용자에게 영향을 미치는 제거 버그가 수정되었습니다.	2020년 10월 8일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.2.2	사소한 버그 수정 및 개선	2020년 8월 12일	더 이상 지원되지 않습니다.
1.2.1	• 애플리케이션 제거에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2020년 7월 1일	더 이상 지원되지 않습니다.
1.2.0	• SAML 2.0 기반 페더레이션 인증에 대한 지원이 추가되었습니다. • macOS Catalina(10.15)에 대한 지원이 추가되었습니다.	2020년 5월 19일	더 이상 지원되지 않습니다.
1.1.2	사소한 버그 수정 및 개선	2020년 4월 21일	더 이상 지원되지 않습니다.
1.1.1	• DNS가 확인되지 않는 문제가 수정되었습니다. • 더 긴 연결로 인한 앱 충돌 문제를 수정되었습니다. • MFA 문제가 수정되었습니다.	2020년 4월 2일	더 이상 지원되지 않습니다.
1.1.0	• macOS DNS 구성에 대한 지원이 추가되었습니다. • 사용자 인터페이스에 표시된 텍스트를 숨기거나 표시하는 OpenVPN 정적 질문 에코 기능에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2020년 3월 9일	더 이상 지원되지 않습니다.
1.0.0	최초 릴리스입니다.	2020년 2월 4일	더 이상 지원되지 않습니다.

AWS Client VPN Linux용

이 섹션에서는 Linux용 AWS 제공 클라이언트를 설치한 다음 AWS 제공된 클라이언트를 사용하여 VPN 연결 설정을 설정하는 방법을 설명합니다. Linux용 AWS 제공 클라이언트는 자동 업데이트를 지원하지 않습니다. 최신 업데이트 및 다운로드는 the section called “릴리스 정보” 섹션을 참조하세요.

Linux용 AWS 제공 클라이언트를 사용하여 Client VPN에 연결하기 위한 요구 사항

Linux용 AWS 제공 클라이언트를 사용하려면 다음이 필요합니다.

- Ubuntu 22.04 LTS(AMD64) 또는 Ubuntu 24.04 LTS(AMD64만 해당)

SAML 기반 페더레이션 인증(Single Sign-On)을 사용하는 Client VPN 엔드포인트의 경우 클라이언트는 컴퓨터에 TCP 포트 8096-8115을 예약합니다.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

주제

- Linux AWS Client VPN 용으로 제공된 설치
- Linux AWS Client VPN 용에 연결
- AWS Client VPN Linux용 릴리스 정보

Linux AWS Client VPN 용으로 제공된 설치

Linux용 AWS 제공 클라이언트를 설치하는 데 사용할 수 있는 방법은 여러 가지가 있습니다. 다음 옵션에서 제공하는 방법 중 하나를 사용합니다. 시작하기 전에 먼저 요구 사항을 읽으십시오.

옵션 1: 패키지 리포지토리를 통해 설치

1. Ubuntu OS에 AWS VPN 클라이언트 퍼블릭 키를 추가합니다.

```
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. 다음 명령을 사용하여 Ubuntu OS(버전 22.04 이상)에 리포지토리를 추가합니다.

```
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. 다음 명령을 사용하여 시스템의 리포지토리를 업데이트합니다.

```
sudo apt-get update
```

4. 다음 명령을 사용하여 Linux용 AWS 제공 클라이언트를 설치합니다.

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

옵션 2: .deb 패키지 파일을 사용하여 설치

1. AWS Client VPN 다운로드에서 또는 다음 명령을 사용하여 .deb 파일을 다운로드합니다.

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

2. dpkg 유틸리티를 사용하여 Linux용 AWS 제공 클라이언트를 설치합니다.

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

옵션 3 - Ubuntu 소프트웨어 센터를 사용하여 .deb 패키지를 설치합니다.

1. AWS Client VPN 다운로드에서 .deb 패키지를 다운로드합니다.
2. .deb 패키지 파일을 다운로드한 후 Ubuntu 소프트웨어 센터를 사용하여 패키지를 설치합니다. Ubuntu Wiki에서 설명한 대로 Ubuntu 소프트웨어 센터를 사용하여 독립 실행형 .deb 패키지에서 설치하는 단계를 따르세요.

Linux AWS Client VPN 용에 연결

AWS 제공된 클라이언트는 다음 단계에서 AWS VPN 클라이언트라고도 합니다.

Linux용 AWS 제공된 클라이언트를 사용하여 연결하려면

1. [AWS VPN Client] 앱을 엽니다.

2. 파일, 프로파일 관리를 선택합니다.
3. 프로파일 추가를 선택합니다.
4. 표시 이름에 프로파일의 이름을 입력합니다.
5. VPN 구성 파일(VPN Configuration File)에서 Client VPN 관리자로부터 받은 구성 파일을 찾습니다. [Open]을 선택합니다.
6. 프로파일 추가를 선택합니다.
7. 여러 연결을 생성하려면 추가하려는 각 구성 파일에 대해 프로필 추가 단계를 반복합니다. 원하는 만큼 프로필을 추가할 수 있지만 최대 5개의 열린 연결만 가질 수 있습니다.
8. AWS VPN 클라이언트 창에서 연결할 프로필을 선택한 다음 연결을 선택합니다. Client VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 시작하려는 각 프로필 연결에 대해이 단계를 반복하여 최대 5개의 동시 엔드포인트를 연결합니다.

   > **Note**
   >
   > 에 연결하는 프로필이 현재 열려 있는 세션과 충돌하는 경우 연결할 수 없습니다. 새 연결을 선택하거나 충돌을 일으키는 세션과의 연결을 해제합니다.

9. 연결에 대한 통계를 보려면 AWS VPN 클라이언트 창에서 연결을 선택하고 세부 정보 표시를 선택한 다음 세부 정보를 보려는 연결을 선택합니다.
10. 연결을 해제하려면 AWS VPN 클라이언트 창에서 연결을 선택한 다음 연결 해제를 선택합니다. 열린 연결이 여러 개 있는 경우 각 연결을 개별적으로 닫아야 합니다.

AWS Client VPN Linux용 릴리스 정보

다음 표에는 Linux용의 현재 및 이전 버전에 대한 릴리스 정보와 다운로드 링크가 나와 AWS Client VPN 있습니다.

> **Note**
>
> 모든 릴리스에서 사용성 및 보안 수정 사항을 지속적으로 제공합니다. 항상 모든 플랫폼의 최신 버전을 사용하는 것이 좋습니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크
5.2.0	• 사소한 개선 사항. • 클라이언트 라우팅 적용에 대한 지원이 추가되었습니다.	2025년 4월 8일	버전 5.2.0 다운로드 sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• 비활성 제한 시간 연결 해제 후 AWS Client VPN 버전 5.0.x가 VPN에 자동으로 다시 연결하는 문제를 수정했습니다. • 사소한 버그 수정 및 개선	2025년 3월 17일	버전 5.1.0 다운로드 sha256: 14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba
5.0.0	• 여러 동시 연결에 대한 지원이 추가되었습니다. • 그래픽 사용자 인터페이스를 업데이트했습니다. • 사소한 버그 수정 및 개선	2025년 1월 21일	버전 5.0.0 다운로드 sha256: 645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c
4.1.0	• Ubuntu 22.04 및 24.04에 대한 지원이 추가되었습니다.	2024년 11월 12일	버전 4.1.0 다운로드

버전	변경	날짜	다운로드 링크
	• 버그 수정		sha256: 334d00222 458fbfe9d ade16c99f e97e9ebcb d51fff017 d0d6b1d1b 764e7af472
4.0.0	사소한 개선 사항.	2024년 9월 25일	다운로드 버전 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	`mssfix` OpenVPN 플래그에 대한 지원이 추가되었습니다.	2024년 9월 4일	다운로드 버전 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2

버전	변경	날짜	다운로드 링크
3.15.0	• `tap-sleep` OpenVPN 플래그에 대한 지원이 추가되었습니다. • OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	다운로드 버전 3.15.0 sha256: 5cf3eb08de96821b0ad3d0c93174b2e308041d5490a3edb772dfd89a6d89d012
3.14.0	• OpenVPN 및 OpenSSL 라이브러리를 업데이트했습니다.	2024년 7월 29일	다운로드 버전 3.14.0 sha256: bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60
3.13.0	• 로컬 영역 네트워크 범위가 변경될 때 자동으로 다시 연결합니다.	2024년 5월 21일	다운로드 버전 3.13.0 sha256: e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1

버전	변경	날짜	다운로드 링크
3.12.2	• 버전 123 이후 Chromium 기반 브라우저의 SAML 인증 문제를 해결했습니다.	2024년 4월 11일	다운로드 버전 3.12.2 sha256: f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
3.12.1	• 로컬 액터가 권한이 높은 임의 명령을 실행하도록 허용할 수 있는 버퍼 오버플로 작업을 수정했습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	다운로드 버전 3.12.1 sha256: 547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• 일부 LAN 구성의 연결 문제를 해결했습니다.	2023년 12월 19일	다운로드 버전 3.12.0 sha256: 9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1

버전	변경	날짜	다운로드 링크
3.11.0	• “일부 LAN 구성의 연결 문제 해결”에 대한 롤백입니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.11.0 sha256: 86c0fa1bf1c9719408 2835a739ec7f1c87e5 40194955f414a35c67 9b94538970
3.10.0	• 일부 LAN 구성의 연결 문제를 해결했습니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	• 클라이언트 네트워크에서 NAT64 활성화 시 발생하는 연결 문제를 해결했습니다. • 사소한 버그 수정 및 개선	2023년 8월 24일	다운로드 버전 3.9.0 sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454

버전	변경	날짜	다운로드 링크
3.8.0	• 보안 태세가 개선되었습니다.	2023년 8월 3일	다운로드 버전 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• 보안 태세가 개선되었습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.6.0	• 버전 3.5.0에서 변경 사항을 롤백했습니다.	2023년 7월 15일	더 이상 지원되지 않음
3.5.0	• 보안 태세가 개선되었습니다.	2023년 7월 14일	더 이상 지원되지 않음
3.4.0	• 'verify-x509-name' OpenVPN 플래그에 대한 지원이 추가되었습니다.	2023년 2월 14일	더 이상 지원되지 않음
3.1.0	• 드라이브 유형 감지 문제가 해결되었습니다. • 보안 태세가 개선되었습니다.	2022년 5월 23일	더 이상 지원되지 않음
3.0.0	• 페더레이션 인증을 사용할 때 배너 메시지가 표시되지 않는 문제를 수정했습니다. • 더 긴 텍스트와 특정 문자 시퀀스에 대한 배너 텍스트 표시를 수정했습니다. • 보안 태세를 강화했습니다.	2022년 3월 3일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
2.0.0	• 새로운 연결이 설정된 후의 배너 텍스트에 대한 지원이 추가되었습니다. • 에코와 관련하여 풀 필터를 사용하는 기능(즉, pull-filter * echo)이 제거되었습니다. • 사소한 버그 수정 및 개선	2022년 1월 20일	더 이상 지원되지 않습니다.
1.0.3	• 일부 경우에 페더레이션 인증 연결 시도가 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 11월 8일	더 이상 지원되지 않습니다.
1.0.2	• OpenVPN 플래그에 대한 지원이 추가되었습니다. 추가: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • 사소한 버그 수정 및 개선	2021년 9월 28일	더 이상 지원되지 않습니다.
1.0.1	• Ubuntu 애플리케이션 바에서 종료하는 옵션이 활성화되었습니다. • OpenVPN 플래그에 대한 다음 지원이 추가되었습니다. 비활성, 풀 필터, 경로. • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않습니다.
1.0.0	최초 릴리스입니다.	2021년 6월 11일	더 이상 지원되지 않습니다.

OpenVPN 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결

일반적인 Open VPN 클라이언트 애플리케이션을 사용하여 Client VPN 엔드포인트에 연결을 설정할 수 있습니다. Client VPN은 다음 운영 체제에서 지원됩니다.

- Windows

  Windows Certificate Store에서 인증서와 프라이빗 키를 사용합니다. 인증서와 키를 생성한 후에는 OpenVPN GUI AWS 클라이언트 애플리케이션 또는 OpenVPN GUI Connect 클라이언트를 사용하여 클라이언트 연결을 설정할 수 있습니다. 인증서 및 키를 생성하는 단계는 Windows에서 인증서를 사용하여 VPN 연결 설정 섹션을 참조하세요.

- Android 및 iOS

  Android 또는 iOS 디바이스에서 OpenVPN 클라이언트 애플리케이션을 사용하여 VPN 연결을 설정합니다. 자세한 내용은 Android 및 iOS의 Client VPN 연결을 참조하세요.

- macOS

  macOS 기반 Tunnelblick 또는 AWS Client VPN에 대한 구성 파일을 사용하여 VPN 연결을 설정합니다. 자세한 내용은 macOS에서 VPN 연결 설정 단원을 참조하십시오.

- Linux

  OpenVPN - Network Manager 인터페이스 또는 OpenVPN 애플리케이션을 사용하여 Linux에서 VPN 연결을 설정합니다. OpenVPN - Network Manager 인터페이스를 사용하려면 네트워크 관리자 모듈이 아직 설치되지 않은 경우 먼저 설치해야 합니다. 자세한 내용은 Linux에서 VPN 연결 설정 단원을 참조하십시오.

> **Important**
>
> Client VPN 엔드포인트가 SAML 기반 페더레이션 인증을 사용하도록 구성된 경우 OpenVPN 기반 VPN 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다. 여기에는 모든 ARM 기반 아키텍처가 포함됩니다. ARM 프로세서가 있는 디바이스(예: Apple Silicon Macs 또는 ARM 기반 Windows 디바이스)를 사용하는 경우 OpenVPN 클라이언트 대신 AWS 제공된 클라이언트와 함께 SAML 기반 VPN 엔드포인트를 사용해야 합니다.

클라이언트 애플리케이션

- Windows 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결
- AWS Client VPN Android 및 iOS 애플리케이션의 연결
- macOS 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결
- OpenVPN 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결

Windows 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결

이 섹션에서는 Windows 기반 VPN 클라이언트를 사용하여 VPN 연결을 설정하는 방법을 설명합니다.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

문제 해결 정보는 Windows 기반 클라이언트와의 AWS Client VPN 연결 문제 해결를 참조하십시오.

> **Important**
>
> Client VPN 엔드포인트가 SAML 기반 페더레이션 인증을 사용하도록 구성된 경우 OpenVPN 기반 VPN 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다. 여기에는 모든 ARM 기반 아키텍처가 포함됩니다. ARM 프로세서가 있는 디바이스(예: Apple Silicon Macs 또는 ARM 기반 Windows 디바이스)를 사용하는 경우 OpenVPN 클라이언트 대신 AWS 제공된 클라이언트와 함께 SAML 기반 VPN 엔드포인트를 사용해야 합니다.

업무

- Windows에서 인증서 사용 및 AWS Client VPN 연결 설정

Windows에서 인증서 사용 및 AWS Client VPN 연결 설정

Windows 인증서 시스템 스토어의 인증서 및 개인 키를 사용하도록 OpenVPN 클라이언트를 구성할 수 있습니다. 이 옵션은 Client VPN 연결의 일부로 스마트 카드를 사용할 때 유용합니다. OpenVPN 클라이언트 암호화 인증서 옵션에 대한 자세한 내용은 OpenVPN 웹 사이트에서 OpenVPN에 대한 참조 설명서를 참조하세요.

> **Note**
> 인증서는 로컬 컴퓨터에 저장되어야 합니다.

인증서를 사용하고 연결을 설정하려면

1. 클라이언트 인증서 및 개인 키가 포함된 .pfx 파일을 생성합니다.
2. .pfx 파일을 로컬 컴퓨터의 개인 인증서 저장소로 가져옵니다. 자세한 내용은 Microsoft 웹 사이트에서 방법: MMC 스냅인을 사용하여 인증서 보기를 참조하세요.
3. 계정에 로컬 컴퓨터 인증서를 읽을 수 있는 권한이 있는지 확인합니다. Microsoft Management Console을 사용하여 권한을 수정할 수 있습니다. 자세한 내용은 Microsoft 웹 사이트에서 로컬 컴퓨터 인증서 스토어를 볼 수 있는 권한을 참조하세요.
4. OpenVPN 구성 파일을 업데이트하고 인증서 주체 또는 인증서 지문을 사용하여 인증서를 지정합니다.

   다음은 주체를 사용하여 인증서를 지정하는 예제입니다.

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

   다음은 지문을 사용하여 인증서를 지정하는 예제입니다. Microsoft Management Console을 사용하여 지문을 찾을 수 있습니다. 자세한 내용은 Microsoft 웹 사이트에서 How to: Retrieve the Thumbprint of a Certificate를 참조하세요.

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

5. 구성을 완료한 후 OpenVPN을 사용하여 다음 중 하나를 수행하여 VPN 연결을 설정합니다.

   - OpenVPN GUI 클라이언트 애플리케이션 사용
     1. OpenVPN 클라이언트 애플리케이션을 시작합니다.
     2. Windows 작업 표시줄에서 아이콘 표시/숨기기를 선택합니다. OpenVPN GUI 를 마우스 오른쪽 버튼으로 클릭한 다음 파일 가져오기 를 선택합니다.
     3. 열기 대화 상자에서 Client VPN 관리자에게서 받은 구성 파일을 선택하고 열기(Open)를 선택합니다.
     4. Windows 작업 표시줄에서 아이콘 표시/숨기기를 선택합니다. OpenVPN GUI를 마우스 오른쪽 버튼으로 클릭한 다음 연결을 선택합니다.

- OpenVPN GUI Connect 클라이언트 사용
  1. OpenVPN 애플리케이션을 시작하고 가져오기, 로컬 파일에서...를 선택합니다.
  2. VPN 관리자로부터 받은 구성 파일로 이동하여 [열기(Open)]를 선택합니다.

AWS Client VPN Android 및 iOS 애플리케이션의 연결

> **Important**
>
> Client VPN 엔드포인트가 SAML 기반 페더레이션 인증을 사용하도록 구성된 경우 OpenVPN 기반 VPN 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다. 여기에는 모든 ARM 기반 아키텍처가 포함됩니다. ARM 프로세서가 있는 디바이스(예: Apple Silicon Macs 또는 ARM 기반 Windows 디바이스)를 사용하는 경우 OpenVPN 클라이언트 대신 AWS 제공된 클라이언트와 함께 SAML 기반 VPN 엔드포인트를 사용해야 합니다.

다음 정보는 Android 또는 iOS 모바일 디바이스에서 OpenVPN 클라이언트 애플리케이션을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다. Android와 iOS는 단계가 동일합니다.

> **Note**
>
> iOS 또는 Android용 OpenVPN 클라이언트 애플리케이션 다운로드 및 사용에 대한 자세한 내용은 OpenVPN 웹 사이트에서 OpenVPN Connect 사용 설명서를 참조하세요.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

연결을 시작하려면 OpenVPN 클라이언트 애플리케이션을 시작한 후 Client VPN 관리자로부터 받은 파일을 가져옵니다.

macOS 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결

이 섹션에서는 macOS 기반 VPN 클라이언트, Tunnelblick 또는 AWS Client VPN을 사용하여 VPN 연결을 설정하는 방법을 설명합니다.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

문제 해결 정보는 macOS 클라이언트와의 AWS Client VPN 연결 문제 해결를 참조하십시오.

> **Important**
>
> Client VPN 엔드포인트가 SAML 기반 페더레이션 인증을 사용하도록 구성된 경우 OpenVPN 기반 VPN 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다. 여기에는 모든 ARM 기반 아키텍처가 포함됩니다. ARM 프로세서가 있는 디바이스(예: Apple Silicon Macs 또는 ARM 기반 Windows 디바이스)를 사용하는 경우 OpenVPN 클라이언트 대신 AWS 제공된 클라이언트와 함께 SAML 기반 VPN 엔드포인트를 사용해야 합니다.

주제

- macOS에서 AWS Client VPN 연결 설정

macOS에서 AWS Client VPN 연결 설정

macOS 컴퓨터에서 Tunnelblick 클라이언트 애플리케이션을 사용하여 VPN 연결을 설정할 수 있습니다.

> **Note**
>
> macOS용 Tunnelblick 클라이언트 애플리케이션에 대한 자세한 내용은 Tunnelblick 웹 사이트에서 Tunnelblick 설명서를 참조하십시오.

Tunnelblick을 사용하여 VPN 연결을 설정하려면

1. Tunnelblick 클라이언트 애플리케이션을 시작하고 I have configuration files(구성 파일이 있음)를 선택합니다.
2. VPN 관리자에게서 받은 구성 파일을 구성 패널로 드래그 앤 드롭합니다.
3. Configurations(구성) 패널에서 구성 파일을 선택하고 Connect(연결)를 선택합니다.

AWS Client VPN을 사용하여 VPN 연결을 설정합니다.

1. OpenVPN 애플리케이션을 시작하고 [가져오기(Import)], [로컬 파일에서...(From local file...)]를 선택합니다.
2. VPN 관리자로부터 받은 구성 파일로 이동하여 [열기(Open)]를 선택합니다.

OpenVPN 클라이언트 애플리케이션을 사용하여 AWS Client VPN 엔드포인트에 연결

이 섹션에서는 OpenVPN - Network Manager 또는 OpenVPN을 사용하여 VPN 연결을 설정하는 방법을 설명합니다.

시작하기 전에 Client VPN 관리자가 Client VPN 엔드포인트를 생성했으며 Client VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. 여러 프로필에 동시에 연결하려면 각 프로필에 대한 구성 파일이 필요합니다.

문제 해결 정보는 Linux 기반 클라이언트와의 AWS Client VPN 연결 문제 해결를 참조하십시오.

> **Important**
>
> Client VPN 엔드포인트가 SAML 기반 페더레이션 인증을 사용하도록 구성된 경우 OpenVPN 기반 VPN 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 없습니다. 여기에는 모든 ARM 기반 아키텍처가 포함됩니다. ARM 프로세서가 있는 디바이스(예: Apple Silicon Macs 또는 ARM 기반 Windows 디바이스)를 사용하는 경우 OpenVPN 클라이언트 대신 AWS 제공된 클라이언트와 함께 SAML 기반 VPN 엔드포인트를 사용해야 합니다.

주제

- Linux에서 AWS Client VPN 연결 설정

Linux에서 AWS Client VPN 연결 설정

Ubuntu 컴퓨터에서 Network Manager GUI를 사용하거나 OpenVPN 애플리케이션을 사용하여 VPN 연결을 설정합니다.

OpenVPN - Network Manager를 사용하여 VPN 연결을 설정하려면

1. 다음 명령을 사용하여 네트워크 관리자 모듈을 설치합니다.

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

2. 설정, 네트워크로 이동합니다.
3. VPN 옆에 있는 더하기 기호(+)를 선택한 다음 파일에서 가져오기...를 선택합니다.
4. VPN 관리자로부터 받은 구성 파일로 이동하여 열기를 선택합니다.
5. VPN 추가 창에서 추가를 선택합니다.
6. 추가한 VPN 프로필 옆에 있는 토글을 활성화하여 연결을 시작합니다.

OpenVPN을 사용하여 VPN 연결을 설정하려면

1. 다음 명령을 사용하여 OpenVPN을 설치합니다.

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

2. VPN 관리자로부터 받은 구성 파일을 로드하여 연결을 시작합니다.

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

AWS Client VPN 연결 문제 해결

다음 주제를 사용하여 클라이언트 애플리케이션을 통해 Client VPN 엔드포인트에 연결할 때 발생할 수 있는 문제를 해결하십시오.

주제

- 관리자를 위한 Client VPN 엔드포인트 문제 해결
- AWS 제공된 클라이언트 AWS Support 의에 진단 로그 전송
- Windows 기반 클라이언트와의 AWS Client VPN 연결 문제 해결
- macOS 클라이언트와의 AWS Client VPN 연결 문제 해결
- Linux 기반 클라이언트와의 AWS Client VPN 연결 문제 해결
- 일반적인 AWS Client VPN 문제 해결

관리자를 위한 Client VPN 엔드포인트 문제 해결

이 안내서의 일부 단계는 사용자가 수행할 수 있습니다. 다른 단계는 Client VPN 관리자가 Client VPN 엔드포인트 자체에서 수행해야 합니다. 다음 섹션에서는 관리자에게 문의해야 하는 경우를 알려줍니다.

Client VPN 엔드포인트 문제 해결에 대한 자세한 내용은 AWS Client VPN 관리자 안내서의 Client VPN 문제 해결을 참조하세요.

AWS 제공된 클라이언트 AWS Support 의에 진단 로그 전송

AWS 제공된 클라이언트에 문제가 있고 문제 해결을 AWS Support 위해에 문의해야 하는 경우 AWS 제공된 클라이언트는 진단 로그를 로 전송할 수 있습니다 AWS Support. 이 옵션은 Windows, macOS 및 Linux 클라이언트 애플리케이션 모두에서 사용할 수 있습니다.

파일을 보내기 전에가 진단 로그에 액세스하도록 허용하는 AWS Support 데 동의해야 합니다. 사용자가 동의하면 사용자가 파일에 즉시 액세스할 수 AWS Support 있도록에 제공할 수 있는 참조 번호가 제공됩니다.

진단 로그 보내기

다음 단계에서는 AWS 제공된 클라이언트를 AWS VPN 클라이언트라고도 합니다.

Windows용 AWS 제공 클라이언트를 사용하여 진단 로그를 보내려면

1. AWS VPN Client 앱을 엽니다.
2. 도움말(Help),진단 로그 보내기(Send Diagnostic Logs)를 선택합니다.
3. 진단 로그 보내기(Send Diagnostic Logs) 창에서 예(Yes)를 선택합니다.
4. 진단 로그 보내기(Send Diagnostic Logs) 창에서 다음 작업 중 하나를 수행합니다.
   - 참조 번호를 클립보드에 복사하려면 [예(Yes)]를 선택한 다음 [확인(OK)]을 선택합니다.
   - 참조 번호를 수동으로 추적하려면 아니요(No)를 선택합니다.

   에 문의 AWS Support할 때 참조 번호를 제공해야 합니다.

macOS용 AWS 제공 클라이언트를 사용하여 진단 로그를 보내려면

1. AWS VPN Client 앱을 엽니다.
2. 도움말(Help),진단 로그 보내기(Send Diagnostic Logs)를 선택합니다.
3. 진단 로그 보내기(Send Diagnostic Logs) 창에서 예(Yes)를 선택합니다.
4. 확인 창의 참조 번호를 적어 둔 다음 확인(OK)을 선택합니다.

   에 문의 AWS Support할 때 참조 번호를 제공해야 합니다.

Ubuntu용 AWS 제공 클라이언트를 사용하여 진단 로그를 보내려면

1. AWS VPN Client 앱을 엽니다.
2. 도움말(Help),진단 로그 보내기(Send Diagnostic Logs)를 선택합니다.
3. [진단 로그 보내기(Send Diagnostic Logs)] 창에서 [전송(Send)]을 선택합니다.
4. 확인 창의 참조 번호를 기록합니다. 정보를 클립보드로 복사할 수도 있습니다.

   에 문의 AWS Support할 때 참조 번호를 제공해야 합니다.

Windows 기반 클라이언트와의 AWS Client VPN 연결 문제 해결

다음 섹션은 Windows 기반 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 때 발생할 수 있는 문제에 대한 정보를 포함합니다.

AWS 제공된 클라이언트 이벤트 로그

AWS 제공된 클라이언트는 이벤트 로그를 생성하여 컴퓨터의 다음 위치에 저장합니다.

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

다음과 같은 유형의 로그를 사용할 수 있습니다.

- 애플리케이션 로그: 애플리케이션에 대한 정보를 포함합니다. 이러한 로그 앞에 'aws_vpn_client_'가 붙습니다.
- OpenVPN 로그: OpenVPN 프로세스에 대한 정보를 포함합니다. 이러한 로그 앞에 'ovpn_aws_vpn_client_'가 붙습니다.

AWS 제공된 클라이언트는 Windows 서비스를 사용하여 루트 작업을 수행합니다. Windows 서비스 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

주제 문제 해결

- 클라이언트가 연결할 수 없습니다.
- 클라이언트가 연결할 수 없고 "no TAP-Windows adapters" 로그 메시지가 표시됨
- 클라이언트가 다시 연결 중 상태로 멈췄습니다.
- VPN 연결 프로세스가 예기치 않게 종료됩니다.
- 애플리케이션을 시작하지 못했습니다.
- 클라이언트가 프로필을 만들 수 없습니다.
- 팝업 메시지와 함께 VPN 연결 해제
- Windows 10 또는 11을 사용하는 Dell PC에서 클라이언트 충돌 발생
- OpenVPN GUI
- OpenVPN 연결 클라이언트
- DNS를 확인할 수 없습니다.
- PKI 별칭 누락

클라이언트가 연결할 수 없습니다.

문제

AWS 제공된 클라이언트는 Client VPN 엔드포인트에 연결할 수 없습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 다른 OpenVPN 프로세스가 컴퓨터에서 이미 실행 중이므로 클라이언트가 연결되지 않습니다.
- 구성 파일(.ovpn)이 잘못되었습니다.

Solution

컴퓨터에서 실행 중인 다른 OpenVPN 애플리케이션이 있는지 확인합니다. 있는 경우 이러한 프로세스를 중지하거나 종료하고 Client VPN 엔드포인트에 연결을 다시 시도합니다. OpenVPN 로그에서 오류를 확인하고 Client VPN 관리자에게 다음 정보를 확인하도록 요청합니다.

- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.
- CRL은 여전히 유효합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하세요.

클라이언트가 연결할 수 없고 "no TAP-Windows adapters" 로그 메시지가 표시됨

문제

AWS 제공된 클라이언트는 Client VPN 엔드포인트에 연결할 수 없으며 애플리케이션 로그에 “이 시스템에는 TAP-Windows 어댑터가 없습니다. You should be able to create a TAP-Windows adapter by going to Start -> All Programs -> TAP-Windows -> Utilities -> Add a new TAP-Windows virtual ethernet adapter".

Solution

다음 조치 중 하나 이상을 수행하여 이 문제를 해결할 수 있습니다.

- TAP-Windows 어댑터를 다시 시작합니다.

- TAP-Windows 드라이버를 다시 설치합니다.
- 새 TAP-Windows 어댑터를 생성합니다.

클라이언트가 다시 연결 중 상태로 멈췄습니다.

문제

AWS 제공된 클라이언트가 Client VPN 엔드포인트에 연결하려고 하지만 재연결 상태에 멈췄습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터가 인터넷에 연결되어 있지 않습니다.
- DNS 호스트 이름이 IP 주소로 확인되지 않습니다.
- OpenVPN 프로세스가 엔드포인트에 연결을 무기한으로 시도하고 있습니다.

Solution

컴퓨터가 인터넷에 연결되어 있는지 확인합니다. Client VPN 관리자에게 구성 파일의 `remote` 지시문이 유효한 IP 주소로 확인되는지 문의합니다. VPN 클라이언트 창에서 연결 해제를 선택하여 AWS VPN 세션의 연결을 해제하고 다시 연결을 시도할 수도 있습니다.

VPN 연결 프로세스가 예기치 않게 종료됩니다.

문제

Client VPN 엔드포인트에 연결하는 동안 클라이언트가 예기치 않게 종료됩니다.

원인

TAP-Windows가 컴퓨터에 설치되어 있지 않습니다. 이 소프트웨어는 클라이언트를 실행하는 데 필요합니다.

Solution

AWS 제공된 클라이언트 설치 관리자를 다시 실행하여 필요한 모든 종속성을 설치합니다.

애플리케이션을 시작하지 못했습니다.

문제

Windows 7에서는 AWS 제공된 클라이언트가 열려고 할 때 시작되지 않습니다.

원인

.NET Framework 4.7.2 이상이 컴퓨터에 설치되어 있지 않습니다. 클라이언트를 실행하는 데 필요합니다.

Solution

AWS 제공된 클라이언트 설치 관리자를 다시 실행하여 필요한 모든 종속성을 설치합니다.

클라이언트가 프로필을 만들 수 없습니다.

문제

AWS 제공 클라이언트를 사용하여 프로파일을 생성할 때 다음 오류가 발생합니다.

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

원인

Client VPN 엔드포인트가 상호 인증을 사용하는 경우 구성(.ovpn) 파일에 클라이언트 인증서와 키가 포함되지 않습니다.

Solution

Client VPN 관리자가 클라이언트 인증서와 키를 구성 파일에 추가하는지 확인합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.

팝업 메시지와 함께 VPN 연결 해제

문제

VPN 연결이 끊어지고 다음과 같은 팝업 메시지가 표시됩니다. "디바이스가 연결된 로컬 네트워크의 주소 스페이스가 변경되어 VPN 연결이 종료됩니다. 새 VPN 연결을 설정하세요.”

원인

TAP-Windows 어댑터에는 필요한 설명이 포함되어 있지 않습니다.

Solution

아래 `Description` 필드가 일치하지 않는 경우 먼저 TAP-Windows 어댑터를 제거한 다음 AWS 제공된 클라이언트 설치 관리자를 다시 실행하여 필요한 모든 종속성을 설치합니다.

```
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
```

Windows 10 또는 11을 사용하는 Dell PC에서 클라이언트 충돌 발생

문제

Windows 10 또는 11을 실행하는 특정 Dell PC(데스크탑 및 랩톱)에서 파일 시스템을 탐색하여 VPN 구성 파일을 가져올 때 충돌이 발생할 수 있습니다. 이 문제가 발생하면 AWS 제공된 클라이언트의 로그에 다음과 같은 메시지가 표시됩니다.

```
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()
```

원인

Windows 10 및 11의 Dell 백업 및 복구 시스템은 AWS 제공된 클라이언트, 특히 다음 세 DLLs.

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll

- DBROverlayIconNotBackuped.dll

Solution

이 문제를 방지하려면 먼저 클라이언트가 AWS 제공된 클라이언트의 최신 버전으로 최신 상태인지 확인합니다. AWS Client VPN 다운로드로 이동하여 더 최신 버전이 있다면 최신 버전으로 업그레이드합니다.

또한 다음 작업을 수행해야 합니다.

- Dell 백업 및 복구 애플리케이션을 사용하는 경우 최신 버전인지 확인합니다. Dell 포럼 게시물에서는 이 문제가 애플리케이션 최신 버전에서 해결되었다고 설명합니다.
- Dell 백업 및 복구 애플리케이션을 사용하지 않는데 이 문제가 발생할 경우 일부 조치를 취해야 합니다. 애플리케이션 업그레이드를 원하지 않는 경우, 대신 DLL 파일을 삭제하거나 이름을 바꿀 수 있습니다. 그러나 이렇게 하면 Dell 백업 및 복구 애플리케이션이 제대로 작동하지 않습니다.

DLL 파일 삭제 또는 이름 바꾸기

1. Windows 탐색기로 이동하여 Dell 백업 및 복구가 설치된 위치를 찾습니다. 일반적으로 다음 위치에 설치되지만, 검색을 해야 할 수 있습니다.

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

2. 설치 디렉터리에서 다음 DLL 파일을 수동으로 삭제하거나 이름을 바꿉니다. 두 작업 중 하나만 해도 로드되는 것을 방지할 수 있습니다.

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

   파일 이름 끝에 '.bak'를 추가하여 파일 이름을 바꿀 수 있습니다 (예:DBROverlayIconBackuped.dll.bak).

OpenVPN GUI

다음 문제 해결 정보는 Windows 10 Home(64비트) 및 Windows Server 2016(64비트) 기반의 OpenVPN GUI 소프트웨어의 버전 11.10.0.0 및 11.11.0.0에서 테스트되었습니다.

구성 파일은 컴퓨터의 다음 위치에 저장됩니다.

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

연결 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

OpenVPN 연결 클라이언트

다음 문제 해결 정보는 Windows 10 Home(64비트) 및 Windows Server 2016(64비트) 기반의 OpenVPN Connect Client 소프트웨어의 버전 2.6.0.100 및 2.7.1.101에서 테스트되었습니다.

구성 파일은 컴퓨터의 다음 위치에 저장됩니다.

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

연결 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

DNS를 확인할 수 없습니다.

문제

다음 오류로 인해 연결이 실패합니다.

```
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.
```

원인

DNS 이름을 확인할 수 없습니다. DNS 캐싱을 방지하기 위해 클라이언트는 DNS 이름 앞에 임의의 문자열을 붙여야 하지만 일부 클라이언트는 이 작업을 수행하지 않습니다.

Solution

AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트 DNS 이름을 확인할 수 없음에 대한 해결 방법을 참조하세요.

PKI 별칭 누락

문제

상호 인증을 사용하지 않는 Client VPN 엔드포인트에 대한 연결이 실패하고 다음 오류가 발생합니다.

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

원인

OpenVPN Connect Client 소프트웨어에는 상호 인증을 사용하여 인증을 시도하는 알려진 문제가 있습니다. 구성 파일에 클라이언트 키와 인증서가 없으면 인증이 실패합니다.

Solution

Client VPN 구성 파일에 임의의 클라이언트 키와 인증서를 지정하고 새 구성을 OpenVPN Connect Client 소프트웨어로 가져옵니다. 또는 OpenVPN GUI 클라이언트(v11.12.0.0)나 Viscosity 클라이언트(v.1.7.14) 등, 다른 클라이언트를 사용합니다.

macOS 클라이언트와의 AWS Client VPN 연결 문제 해결

다음 섹션에는 macOS 클라이언트를 사용할 때 발생할 수 있는 로깅 및 문제에 대한 정보가 포함되어 있습니다. 최신 버전의 클라이언트를 실행하고 있는지 확인합니다.

AWS 제공된 클라이언트 이벤트 로그

AWS 제공된 클라이언트는 이벤트 로그를 생성하여 컴퓨터의 다음 위치에 저장합니다.

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

다음과 같은 유형의 로그를 사용할 수 있습니다.

- 애플리케이션 로그: 애플리케이션에 대한 정보를 포함합니다. 이러한 로그 앞에 'aws_vpn_client_'가 붙습니다.
- OpenVPN 로그: OpenVPN 프로세스에 대한 정보를 포함합니다. 이러한 로그 앞에 'ovpn_aws_vpn_client_'가 붙습니다.

AWS 제공된 클라이언트는 클라이언트 데몬을 사용하여 루트 작업을 수행합니다. 데몬 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

AWS 제공된 클라이언트는 구성 파일을 컴퓨터의 다음 위치에 저장합니다.

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

주제 문제 해결

- 클라이언트가 연결할 수 없습니다.
- 클라이언트가 다시 연결 중 상태로 멈췄습니다.
- 클라이언트가 프로필을 만들 수 없습니다.
- Helper 도구 필요함 오류
- Tunnelblick
- 암호 알고리즘 'AES-256-GCM'을 찾을 수 없습니다.
- 연결 응답이 중지되고 재설정됨
- 확장 키 사용(EKU)
- 만료된 인증서
- OpenVPN
- DNS를 확인할 수 없습니다.

클라이언트가 연결할 수 없습니다.

문제

AWS 제공된 클라이언트는 Client VPN 엔드포인트에 연결할 수 없습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 다른 OpenVPN 프로세스가 컴퓨터에서 이미 실행 중이므로 클라이언트가 연결되지 않습니다.
- 구성 파일(.ovpn)이 잘못되었습니다.

Solution

컴퓨터에서 실행 중인 다른 OpenVPN 애플리케이션이 있는지 확인합니다. 있는 경우 이러한 프로세스를 중지하거나 종료하고 Client VPN 엔드포인트에 연결을 다시 시도합니다. OpenVPN 로그에서 오류를 확인하고 Client VPN 관리자에게 다음 정보를 확인하도록 요청합니다.

- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.
- CRL은 여전히 유효합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하세요.

클라이언트가 다시 연결 중 상태로 멈췄습니다.

문제

AWS 제공된 클라이언트가 Client VPN 엔드포인트에 연결하려고 하지만 재연결 상태에 멈췄습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터가 인터넷에 연결되어 있지 않습니다.
- DNS 호스트 이름이 IP 주소로 확인되지 않습니다.
- OpenVPN 프로세스가 엔드포인트에 연결을 무기한으로 시도하고 있습니다.

Solution

컴퓨터가 인터넷에 연결되어 있는지 확인합니다. Client VPN 관리자에게 구성 파일의 `remote` 지시문이 유효한 IP 주소로 확인되는지 문의합니다. VPN 클라이언트 창에서 연결 해제를 선택하여 AWS VPN 세션의 연결을 끊고 다시 연결을 시도할 수도 있습니다.

클라이언트가 프로필을 만들 수 없습니다.

문제

AWS 제공 클라이언트를 사용하여 프로파일을 생성할 때 다음 오류가 발생합니다.

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

원인

Client VPN 엔드포인트가 상호 인증을 사용하는 경우 구성(.ovpn) 파일에 클라이언트 인증서와 키가 포함되지 않습니다.

Solution

Client VPN 관리자가 클라이언트 인증서와 키를 구성 파일에 추가하는지 확인합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.

Helper 도구 필요함 오류

문제

VPN 연결을 시도할 때 다음 오류가 발생합니다.

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

Solution

AWS re:Post에서 다음 문서를 참조하세요. AWS VPN Client - Helper 도구 필요함 오류

Tunnelblick

다음 문제 해결 정보는 macOS High Sierra 10.13.6 기반 Tunnelblick 소프트웨어의 버전 3.7.8(빌드 5180)에서 테스트되었습니다.

프라이빗 구성의 구성 파일은 컴퓨터의 다음 위치에 저장됩니다.

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

공유 구성에 대한 구성 파일은 컴퓨터의 다음 위치에 저장됩니다.

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

연결 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

로그 세부 수준을 높이려면 Tunnelblick 애플리케이션을 열고 설정을 선택한 다음 VPN 로그 수준 값을 조정합니다.

암호 알고리즘 'AES-256-GCM'을 찾을 수 없습니다.

문제

연결이 실패하고 로그에 다음 오류가 반환됩니다.

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

원인

애플리케이션은 암호 알고리즘 AES-256-GCM을 지원하지 않는 OpenVPN 버전을 사용하고 있습니다.

Solution

다음을 수행하여 호환되는 OpenVPN 버전을 선택합니다.

1. Tunnelblick 애플리케이션을 엽니다.
2. 설정을 선택합니다.
3. OpenVPN 버전의 경우 2.4.6 - OpenSSL version is v1.0.2q를 선택합니다.

연결 응답이 중지되고 재설정됨

문제

연결이 실패하고 로그에 다음 오류가 반환됩니다.

```
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
```

원인

클라이언트 인증서가 취소되었습니다. 인증을 시도한 후 연결 응답이 중지되고 결국 서버 측에서 재설정됩니다.

Solution

Client VPN 관리자에게 새 구성 파일을 요청합니다.

확장 키 사용(EKU)

문제

연결이 실패하고 로그에 다음 오류가 반환됩니다.

```
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,,,,,
```

원인

서버 인증에 성공했습니다. 그러나 클라이언트 인증서에 서버 인증에 사용할 수 있는 확장 키 사용(EKU) 필드가 있기 때문에 클라이언트 인증이 실패합니다.

Solution

올바른 클라이언트 인증서와 키를 사용하고 있는지 확인합니다. 필요한 경우 Client VPN 관리자에게 확인합니다. 이 오류는 클라이언트 인증서가 아닌 서버 인증서를 사용하여 Client VPN 엔드포인트에 연결하는 경우에 발생할 수 있습니다.

만료된 인증서

문제

서버 인증은 성공하지만 다음 오류와 함께 클라이언트 인증이 실패합니다.

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

원인

클라이언트 인증서 유효성이 만료되었습니다.

Solution

Client VPN 관리자에게 새 클라이언트 인증서를 요청합니다.

OpenVPN

다음 문제 해결 정보는 macOS High Sierra 10.13.6 기반 OpenVPN Connect Client 소프트웨어의 버전 2.7.1.100에서 테스트되었습니다.

구성 파일은 컴퓨터의 다음 위치에 저장됩니다.

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

연결 로그는 컴퓨터의 다음 위치에 저장됩니다.

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

DNS를 확인할 수 없습니다.

문제

다음 오류로 인해 연결이 실패합니다.

```
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
```

원인

OpenVPN 연결이 Client VPN DNS 이름을 확인할 수 없습니다.

Solution

AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트 DNS 이름을 확인할 수 없음에 대한 해결 방법을 참조하세요.

Linux 기반 클라이언트와의 AWS Client VPN 연결 문제 해결

다음 섹션에서는 로깅 및 Linux 기반 클라이언트를 사용할 때 발생할 수 있는 문제에 대해 설명합니다. 최신 버전의 클라이언트를 실행하고 있는지 확인합니다.

주제

- AWS 제공된 클라이언트 이벤트 로그
- DNS 쿼리는 기본 네임서버로 이동합니다.
- OpenVPN(명령줄)
- 네트워크 관리자를 통한 OpenVPN(GUI)

AWS 제공된 클라이언트 이벤트 로그

AWS 제공된 클라이언트는 로그 파일과 구성 파일을 시스템의 다음 위치에 저장합니다.

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

AWS 제공된 클라이언트 데몬 프로세스는 시스템의 다음 위치에 로그 파일을 저장합니다.

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

예를 들어 다음 로그 파일을 확인하여 연결 실패를 유발하는 DNS 업/다운 스크립트의 오류를 찾을 수 있습니다.

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

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

DNS 쿼리는 기본 네임서버로 이동합니다.

문제

경우에 따라 VPN 연결이 설정된 후에도 ClientVPN VPN 엔드포인트에 대해 구성된 이름 서버가 아닌 기본 시스템 이름 서버로 DNS 쿼리가 계속 이동합니다.

원인

클라이언트는 Linux 시스템에서 사용할 수 있는 서비스인 systemd-resolved와 상호 작용하며 DNS 관리의 중앙 부분으로 사용됩니다. ClientVPN 엔드포인트에서 푸시되는 DNS 서버를 구성하는 데 사용됩니다. 이 문제는 systemd-resolved가 ClientVPN 엔드포인트에서 제공하는 DNS 서버에 가장 높은 우선 순위를 설정하지 않기 때문에 발생합니다. 대신 로컬 시스템에 구성된 기존 DNS 서버 목록에 서버를 추가합니다. 따라서 원래 DNS 서버의 우선 순위가 가장 높을 수 있으므로 DNS 쿼리를 확인하는 데 사용할 수 있습니다.

Solution

1. OpenVPN 구성 파일의 첫 번째 줄에 다음 지시문을 추가하여 모든 DNS 쿼리가 VPN 터널로 전송되도록 합니다.

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

2. systemd-resolved에서 제공하는 스터브 리졸버를 사용합니다. 이렇게 하려면 시스템에서 다음 명령을 실행하여 `/etc/resolv.conf`을 `/run/systemd/resolve/stub-resolv.conf`에 symlink로 연결합니다.

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

3. (선택 사항) systemd-resolved가 DNS 쿼리를 프록시하지 않도록 하고 대신 실제 DNS 이름 서버로 쿼리를 직접 전송하려면 `/run/systemd/resolve/resolv.conf`대신 `/etc/resolv.conf`에 symlink를 연결합니다.

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

   DNS 응답 캐싱, 인터페이스별 DNS 구성, DNSec 적용 등과 같이 systemd-resolved 구성을 건너뛰기 위해 이 절차를 수행할 수 있습니다. 이 옵션은 VPN에 연결된 경우 퍼블릭 DNS 레코드

를 프라이빗 레코드로 재정의해야 하는 경우에 특히 유용합니다. 예를 들어 프라이빗 VPC에 www.example.com에 대한 레코드가 있는 프라이빗 DNS 리졸버가 있을 수 있으며 이 레코드는 프라이빗 IP로 확인됩니다. 이 옵션을 사용하여 퍼블릭 IP로 확인되는 www.example.com의 퍼블릭 레코드를 재정의할 수 있습니다.

OpenVPN(명령줄)

문제

DNS 확인이 작동하지 않기 때문에 연결이 제대로 작동하지 않습니다.

원인

DNS 서버가 Client VPN 엔드포인트에서 구성되지 않았거나 클라이언트 소프트웨어에서 준수되지 않습니다.

Solution

DNS 서버가 올바르게 구성되고 작동하는지 확인하려면 다음 단계를 수행하십시오.

1. DNS 서버 항목이 로그에 있는지 확인합니다. 다음 예에서는 Client VPN 엔드포인트에 구성된 DNS 서버 `192.168.0.2`가 마지막 줄에 반환됩니다.

   ```
   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
   ```

   지정된 DNS 서버가 없는 경우 Client VPN 관리자에게 Client VPN 엔드포인트를 수정하도록 요청하고 Client VPN 엔드포인트에 대해 DNS 서버(예: VPC DNS 서버)가 지정되었는지 확인합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트를 참조하세요.
2. 다음 명령을 실행하여 `resolvconf` 패키지가 설치되어 있는지 확인합니다.

   ```
   sudo apt list resolvconf
   ```

   출력은 다음을 반환해야합니다.

   ```
   Listing... Done
   ```

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

설치되어 있지 않은 경우 다음 명령을 사용하여 설치합니다.

```
sudo apt install resolvconf
```

3. 텍스트 편집기에서 Client VPN 구성 파일(.ovpn 파일)을 열고 다음 줄을 추가합니다.

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

로그를 확인하여 `resolvconf` 스크립트가 호출되었는지 확인합니다. 로그에는 다음과 유사한 행이 포함되어야 합니다.

```
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
```

네트워크 관리자를 통한 OpenVPN(GUI)

문제

네트워크 관리자 OpenVPN 클라이언트를 사용할 때 다음 오류와 함께 연결이 실패합니다.

```
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
```

원인

`remote-random-hostname` 플래그가 적용되지 않으며 클라이언트는 `network-manager-gnome` 패키지를 사용하여 연결할 수 없습니다.

Solution

AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트 DNS 이름을 확인할 수 없음에 대한 해결 방법을 참조하세요.

일반적인 AWS Client VPN 문제 해결

클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 때 발생할 수 있는 일반적인 문제는 다음과 같습니다.

TLS 키 협상 실패

문제

TLS 협상이 실패하고 다음 오류가 발생합니다.

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

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 방화벽 규칙이 UDP 또는 TCP 트래픽을 차단하고 있습니다.
- 구성 파일(.ovpn)에서 잘못된 클라이언트 키와 인증서를 사용하고 있습니다.
- CRL(클라이언트 인증서 취소 목록)이 만료되었습니다.

Solution

컴퓨터의 방화벽 규칙이 포트 443 또는 1194의 인바운드 또는 아웃바운드 TCP 또는 UDP 트래픽을 차단하는지 확인합니다. Client VPN 관리자에게 다음 정보를 확인하도록 요청합니다.

- Client VPN 엔드포인트에 대한 방화벽 규칙은 포트 443 또는 1194의 TCP 또는 UDP 트래픽을 차단하지 않습니다.
- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.
- CRL은 여전히 유효합니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 Client VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하세요.

문서 기록

다음 표에서는 AWS Client VPN 사용 설명서 업데이트를 설명합니다.

변경 사항	설명	날짜
AWS macOS용 제공 클라이언트(5.2.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 6월 18일
AWS Windows용 제공 클라이언트(5.2.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 6월 2일
AWS Windows용 제공 클라이언트(5.2.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 4월 21일
AWS macOS용 제공 클라이언트(5.2.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 4월 8일
AWS Windows용 제공 클라이언트(5.2.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 4월 8일
AWS Ubuntu용 제공 클라이언트(5.2.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 4월 8일
AWS macOS용 제공 클라이언트(5.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 3월 17일
AWS Windows용 제공 클라이언트(5.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 3월 17일
AWS Ubuntu용 제공 클라이언트(5.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 3월 17일
macOS Monterey에 대한 지원 제거 및 macOS Sonoma(14.0)에 대한 지원 추가	자세한 내용은 Client VPN for macOS 요구 사항을 참조하세요.	2025년 3월 12일

Ubuntu 18.0.4(LTS) 및 Ubuntu 20.04 LTS(AMD64만 해당) 모두에 대한 지원 제거	자세한 내용은 Linux용 Client VPN 요구 사항을 참조하세요.	2025년 3월 12일
AWS macOS용 제공 클라이언트(5.0.3) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 3월 6일
AWS Windows용 제공 클라이언트(5.0.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 2월 24일
AWS macOS용 제공 클라이언트(5.0.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 2월 17일
AWS Windows용 제공 클라이언트(5.0.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 1월 30일
AWS macOS용 제공 클라이언트(5.0.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 1월 22일
이제 AWS 제공된 클라이언트가 최대 5개의 동시 연결을 지원합니다.	자세한 내용은 AWS 제공된 클라이언트를 사용한 동시 연결 지원을 참조하세요.	2025년 1월 21일
AWS macOS용 제공 클라이언트(5.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 1월 21일
AWS Windows용 제공 클라이언트(5.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2025년 1월 21일
AWS Ubuntu용 제공 클라이언트(5.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 11월 12일
AWS macOS용 제공 클라이언트(4.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 11월 12일
AWS Windows용 제공 클라이언트(4.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 11월 12일
AWS Ubuntu용 제공 클라이언트(4.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 11월 12일

AWS macOS용 제공 클라이언트(4.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 25일
AWS Windows용 제공 클라이언트(4.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 25일
AWS Ubuntu용 제공 클라이언트(4.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 25일
AWS Ubuntu용 제공 클라이언트(3.15.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 4일
AWS Windows용 제공 클라이언트(3.14.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 4일
AWS macOS용 제공 클라이언트(3.12.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 9월 4일
AWS Windows용 제공 클라이언트(3.14.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 22일
AWS Ubuntu용 제공 클라이언트(3.15.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS Windows용 제공 클라이언트(3.14.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS macOS용 제공 클라이언트(3.12.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS Ubuntu용 제공 클라이언트(3.14.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일
AWS Windows용 제공 클라이언트(3.13.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일
AWS macOS용 제공 클라이언트(3.11.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일

AWS Windows용 제공 클라이언트(3.12.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 18일
AWS Ubuntu용 제공 클라이언트(3.13.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS Windows용 제공 클라이언트(3.12.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS macOS용 제공 클라이언트(3.10.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS macOS용 제공 클라이언트(3.9.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일
AWS Ubuntu용 제공 클라이언트(3.12.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일
AWS Windows용 제공 클라이언트(3.11.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일
AWS macOS용 제공 클라이언트(3.9.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS Ubuntu용 제공 클라이언트(3.12.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS Windows용 제공 클라이언트(3.11.1) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS Ubuntu용 제공 클라이언트(3.12.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 19일
AWS macOS용 제공 클라이언트(3.9.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS Windows용 제공 클라이언트(3.11.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일

AWS Ubuntu용 제공 클라이언트(3.11.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS Ubuntu용 제공 클라이언트(3.10.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS Ubuntu용 제공 클라이언트(3.9.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일
AWS macOS용 제공 클라이언트(3.8.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일
AWS Windows용 제공 클라이언트(3.10.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일
AWS Windows용 제공 클라이언트(3.9.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS Ubuntu용 제공 클라이언트(3.8.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS macOS용 제공 클라이언트(3.7.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS Windows용 제공 클라이언트(3.8.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS Windows용 제공 클라이언트(3.7.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS Ubuntu용 제공 클라이언트(3.7.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS macOS용 제공 클라이언트(3.6.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS Ubuntu용 제공 클라이언트(3.6.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일

AWS macOS용 제공 클라이언트(3.5.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS Windows용 제공 클라이언트(3.6.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS Ubuntu용 제공 클라이언트(3.5.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS macOS용 제공 클라이언트(3.4.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS macOS용 제공 클라이언트(3.3.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 4월 27일
AWS Windows용 제공 클라이언트(3.5.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 4월 3일
AWS Windows용 제공 클라이언트(3.4.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 3월 28일
AWS Windows용 제공 클라이언트(3.3.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 3월 17일
AWS Ubuntu용 제공 클라이언트(3.4.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 2월 14일
AWS macOS용 제공 클라이언트(3.2.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 1월 23일
AWS Windows용 제공 클라이언트(3.2.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2023년 1월 23일
AWS macOS용 제공 클라이언트(3.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일
AWS Windows용 제공 클라이언트(3.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일

AWS Ubuntu용 제공 클라이언트(3.1.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일
AWS macOS용 제공 클라이언트(3.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS Windows용 제공 클라이언트(3.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS Ubuntu용 제공 클라이언트(3.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS macOS용 제공 클라이언트(2.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일
AWS Windows용 제공 클라이언트(2.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일
AWS Ubuntu용 제공 클라이언트(2.0.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일
AWS macOS용 제공 클라이언트(1.4.0) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 9일
AWS Windows용 제공 클라이언트(1.3.7) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 8일
AWS Ubuntu용 제공 클라이언트(1.0.3) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 8일
AWS Ubuntu용 제공 클라이언트(1.0.2) 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2021년 9월 28일
AWS Windows(1.3.6) 및 macOS(1.3.5)용 제공 클라이언트 릴리스	세부 정보는 릴리스 정보를 참조하세요.	2021년 9월 20일
AWS Ubuntu 18.04 LTS 및 Ubuntu 20.04 LTS용 제공 클라이언트 릴리스	Ubuntu 18.04 LTS 및 Ubuntu 20.04 LTS에서 AWS제공 클라이언트를 사용할 수 있습니다.	2021년 6월 11일

Windows 인증서 시스템 스토어의 인증서를 사용하여 OpenVPN 지원	Windows 인증서 시스템 스토어의 인증서로 OpenVPN을 사용할 수 있습니다.	2021년 2월 25일
셀프 서비스 포털	셀프 서비스 포털에 액세스하여 AWS 제공된 최신 클라이언트 및 구성 파일을 가져올 수 있습니다.	2020년 10월 29일
AWS 제공된 클라이언트	AWS 제공된 클라이언트를 사용하여 Client VPN 엔드포인트에 연결할 수 있습니다.	2020년 2월 4일
최초 릴리스	이 릴리스에서는 AWS Client VPN을 소개합니다.	2018년 12월 18일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.