사용자 가이드

AWS 고객사 VPN

AWS 고객사 VPN: 사용자 가이드

Table of Contents

AWS 클라이언트란 VPN 무엇입니까?

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

이 가이드에서는 디바이스의 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 VPN 연결하는 단계를 제공합니다.

클라이언트 VPN 구성 요소

다음은 AWS Client를 사용하기 위한 주요 구성 요소입니다VPN.

- 클라이언트 VPN 엔드포인트 - 클라이언트 VPN 관리자가 에서 클라이언트 VPN 엔드포인트를 생성하고 구성합니다. AWS관리자는 연결을 설정할 때 액세스할 수 있는 네트워크와 리소스를 제어합니다. VPN
- VPN클라이언트 애플리케이션 - 클라이언트 VPN 엔드포인트에 연결하고 보안 VPN 연결을 설정하는 데 사용하는 소프트웨어 애플리케이션입니다.
- 클라이언트 VPN 엔드포인트 구성 파일 - 클라이언트 VPN 관리자가 제공하는 구성 파일입니다. 이 파일에는 클라이언트 VPN 엔드포인트에 대한 정보와 VPN 연결을 설정하는 데 필요한 인증서가 들어 있습니다. 이 파일을 선택한 VPN 클라이언트 애플리케이션에 로드합니다.

클라이언트 구성을 위한 추가 리소스 VPN

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

다음으로 시작하세요 AWS Client VPN

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

클라이언트 VPN 엔드포인트를 만들어야 하는 관리자인 경우 AWS Client VPN 관리자 안내서를 참조하십시오.

주제

클라이언트 사용을 위한 사전 요구 사항 VPN

VPN연결을 설정하려면 다음이 있어야 합니다.

- 인터넷 액세스
- 지원되는 디바이스
- SAML기반 페더레이션 인증 (Single Sign-On) 을 사용하는 클라이언트 VPN 엔드포인트의 경우 다음 브라우저 중 하나를 사용하십시오.
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

1단계: 클라이언트 애플리케이션 가져오기 VPN

AWS 제공된 클라이언트 또는 다른 오픈 VPN 기반 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 연결하고 VPN 연결을 설정할 수 있습니다.

AWS 제공된 클라이언트는 윈도우, macOS, 우분투 18.04LTS, 우분투 20.04에서 지원됩니다. LTS

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

- 관리자가 엔드포인트 구성 파일을 설정하지 않은 경우 클라이언트 다운로드에서AWS 클라이언트를 다운로드하여 설치하십시오. VPN 애플리케이션을 다운로드하고 설치한 후 관리자로부터 엔드포인트 구성 파일을 받으십시오. the section called “2단계: 클라이언트 VPN 엔드포인트 구성 파일 가져오기”
- 관리자가 이미 엔드포인트 구성 파일을 사전 구성한 경우 셀프 서비스 포털에서 구성 파일과 함께 클라이언트 VPN 애플리케이션을 다운로드할 수 있습니다. 셀프 서비스 포털에서 클라이언트 및 구성 파일을 다운로드하는 단계는 을 참조하십시오. the section called “클라이언트 다운로드 VPN” 응용 프로그램 및 파일을 다운로드하고 설치한 후 로 이동하십시오the section called “3단계: 연결 VPN”.

또는 VPN 연결을 설정하려는 장치에 Open VPN Client 애플리케이션을 다운로드하여 설치하십시오.

2단계: 클라이언트 VPN 엔드포인트 구성 파일 가져오기

관리자로부터 클라이언트 VPN 엔드포인트 구성 파일을 받습니다. 구성 파일에는 클라이언트 VPN 엔드포인트에 대한 정보와 VPN 연결을 설정하는 데 필요한 인증서가 들어 있습니다.

또는 클라이언트 VPN 관리자가 클라이언트 VPN 엔드포인트에 대한 셀프 서비스 포털을 구성한 경우 AWS 제공된 클라이언트의 최신 버전과 최신 버전의 클라이언트 VPN 엔드포인트 구성 파일을 직접 다운로드할 수 있습니다. 자세한 내용은 셀프 서비스 AWS Client VPN 포털에서 다운로드 단원을 참조하십시오.

3단계: 연결 VPN

클라이언트 VPN 엔드포인트 구성 파일을 AWS 제공된 클라이언트 또는 Open VPN Client 애플리케이션으로 가져와서 에 연결합니다VPN. 엔드포인트 구성 파일 가져오기를 VPN 포함하여 a에 연결하는 단계는 다음 항목을 참조하십시오.

- AWS 제공된 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결
- 오픈 클라이언트를 사용하여 클라이언트 VPN VPN 엔드포인트에 연결

Active Directory 인증을 사용하는 클라이언트 VPN 엔드포인트의 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 디렉터리에 대해 다단계 인증 (MFA) 이 활성화된 경우 코드를 MFA 입력하라는 메시지도 표시됩니다.

SAML기반 페더레이션 인증 (Single Sign-On) 을 사용하는 클라이언트 VPN 엔드포인트의 경우 AWS 제공된 클라이언트가 사용자 컴퓨터에서 브라우저 창을 엽니다. 클라이언트 엔드포인트에 연결하려면 먼저 회사 자격 증명을 입력하라는 메시지가 표시됩니다. VPN

셀프 서비스 AWS Client VPN 포털에서 다운로드

셀프 서비스 포털은 AWS 제공된 클라이언트의 최신 버전과 최신 버전의 클라이언트 VPN 엔드포인트 구성 파일을 다운로드할 수 있는 웹 페이지입니다. 클라이언트 VPN 엔드포인트 관리자가 클라이언트 VPN 클라이언트의 구성 파일을 사전 구성한 경우 이 포털에서 구성 파일과 함께 해당 클라이언트 VPN 애플리케이션을 다운로드하여 설치할 수 있습니다.

> **Note**
>
> 관리자로서 셀프 서비스 포털을 구성하려는 경우 관리자 안내서의 클라이언트 VPN 엔드포인트를 참조하십시오.AWS Client VPN

시작하기 전에 클라이언트 VPN 엔드포인트의 ID가 있어야 합니다. 클라이언트 VPN 엔드포인트 관리자가 ID를 제공하거나 ID가 URL 포함된 셀프 서비스 포털을 제공할 수 있습니다.

셀프 서비스 포털에 액세스하려면

1. https://self-service.clientvpn.amazonaws.com/ 셀프 서비스 포털로 이동하거나 관리자가 URL 제공한 포털을 사용하십시오.
2. 필요한 경우 클라이언트 VPN 엔드포인트의 ID를 입력합니다 (예:). `cvpn-endpoint-0123456abcd123456` Next(다음)를 선택합니다.
3. 사용자 이름과 암호를 입력하고 로그인(Sign In)을 선택합니다. 이는 클라이언트 VPN 엔드포인트에 연결할 때 사용하는 것과 동일한 사용자 이름 및 암호입니다.
4. 셀프 서비스 포털에서 다음을 수행할 수 있습니다.
   - 클라이언트 VPN 엔드포인트에 대한 최신 버전의 클라이언트 구성 파일을 다운로드하십시오.
   - 플랫폼에 AWS 제공된 클라이언트의 최신 버전을 다운로드하십시오.

AWS 제공된 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결

AWS 제공된 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 있습니다. AWS 제공된 클라이언트는 윈도우, macOS, 우분투 18.04LTS, 우분투 20.04에서 지원됩니다. LTS

클라이언트

- AWS Client VPN 윈도우용
- AWS Client VPN macOS용
- AWS Client VPN 리눅스용

오픈 디렉티브 VPN

AWS 제공된 클라이언트는 다음과 같은 Open VPN 디렉티브를 지원합니다.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- 암호
- 클라이언트
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- 비활성

- keepalive
- 키
- nobind
- persist-key
- persist-tun
- ping
- 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
- tun-mtu
- tun-mtu-extra
- 동사
- verify-x509-name

AWS Client VPN 윈도우용

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

요구 사항

AWS 제공된 Windows용 클라이언트를 사용하려면 다음이 필요합니다.

- 윈도우 10 또는 윈도우 11 (64비트 운영 체제, x64 프로세서)
- . NET프레임워크 4.7.2 이상

클라이언트는 컴퓨터에 TCP 포트 8096을 예약합니다. SAML기반 페더레이션 인증 (Single Sign-On)을 사용하는 클라이언트 VPN 엔드포인트의 경우 클라이언트는 포트 35001을 예약합니다. TCP

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

주제

- AWS 제공된 Windows용 클라이언트를 VPN 사용하여 클라이언트에 연결
- AWS Client VPN 윈도우용 릴리스 노트

AWS 제공된 Windows용 클라이언트를 VPN 사용하여 클라이언트에 연결

시작하기 전에 먼저 요구 사항을 읽으십시오. 다음 단계에서는 AWS 제공된 AWS VPN 클라이언트를 클라이언트라고도 합니다.

AWS 제공된 Windows용 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. VPN구성 파일의 경우 클라이언트 VPN 관리자로부터 받은 구성 파일을 찾아 선택하고 프로필 추가를 선택합니다.
6. [AWS VPN Client] 창에서 프로파일이 선택되어 있는지 확인한 다음 [연결(Connect)]을 선택합니다. 클라이언트 VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
7. 연결에 대한 통계를 보려면 연결, 세부 정보 표시를 선택합니다.
8. 연결을 해제하려면 [AWS VPN Client] 창에서 [연결 해제(Disconnect)]를 선택합니다. 또는 Windows 작업 표시줄에서 클라이언트 아이콘을 선택한 다음 연결 해제를 선택합니다.

AWS Client VPN 윈도우용 릴리스 노트

다음 표에는 AWS Client VPN Windows용 현재 및 이전 버전의 릴리스 노트와 다운로드 링크가 나와 있습니다.

> **Note**
>
> 우리는 매 릴리스마다 사용성 및 보안 수정 사항을 계속 제공합니다. 모든 플랫폼에 최신 버전을 사용할 것을 강력히 권장합니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크 및 SHA256
3.14.0	• `tap-sleep` 오픈 VPN 플래그에 대한 지원이 추가되었습니다. • 오픈 VPN 및 오픈 SSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	버전 3.14.0 다운로드 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516
3.13.0	오픈 VPN 라이브러리와 오픈 SSL 라이브러리를 업데이트했습니다.	2024년 7월 29일	버전 3.13.0 다운로드 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b

버전	변경	날짜	다운로드 링크 및 SHA256
3.12.1	Windows 클라이언트 버전 3.12.0에서 일부 사용자의 VPN 연결을 설정하지 못하는 문제가 해결되었습니다.	2024년 7월 18일	버전 3.12.1 다운로드 sha256:5ed34aee6c03aa281e625acdbed272896c67046364a9e5846ca697e05dbfec08
3.12.0	• 근거리 통신망 범위가 변경되면 자동으로 다시 연결합니다. • SAML엔드포인트와 연결했을 때 자동 애플리케이션 포커스가 제거되었습니다.	2024년 5월 21일	더 이상 지원되지 않음
3.11.2	버전 123 이후 Chromium 기반 브라우저의 SAML 인증 문제가 해결되었습니다.	2024년 4월 11일	버전 3.11.2 다운로드 sha256:8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc

버전	변경	날짜	다운로드 링크 및 SHA256
3.11.1	• 로컬 액터가 상승된 권한으로 임의의 명령을 실행할 수 있도록 허용할 수 있는 버퍼 오버플로 액션을 수정했습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	버전 3.11.1 다운로드 sha256: fb67b60aa837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• 윈도우로 인한 연결 문제를 수정했습니다. VMs • 일부 LAN 구성의 연결 문제를 수정했습니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9
3.10.0	• NAT64이 (가) 클라이언트 네트워크에서 활성화되었을 때 발생하는 연결 문제를 수정했습니다. • 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: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 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” 오픈 플래그에 대한 지원이 추가되었습니다. VPN • 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. • TAPWindows 드라이버 이름 지정으로 인해 다른 드라이버 이름이 영향을 받던 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	• 오픈 VPN 플래그 connect-retry-max, 개발자 유형, 킵얼라이브, 핑, 핑-리스타트, 풀, rcvbuf 등에 대한 지원이 추가되었습니다. 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	• 오픈 VPN 플래그: dhcp-option에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않음
1.3.3	• 오픈 VPN 플래그 (비활성, 풀 필터, 경로) 에 대한 지원이 추가되었습니다. • 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	• 구성되면 IPv6 누수 방지 기능을 추가하세요. • [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' 오픈 디렉티브에 대한 지원이 추가되었습니다. VPN • 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	• cryptoapicert 오픈 디렉티브에 대한 지원이 추가되었습니다. VPN • 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	• Open 구성에서 코멘트에 대한 지원이 추가되었습니다. VPN • TLS핸드셰이크 오류에 대한 오류 메시지를 추가했습니다.	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	• SAML2.0 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 개방형 VPN 정적 챌린지 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 AWS 제공된 macOS용 클라이언트를 사용하여 VPN 연결을 설정하는 방법을 설명합니다. 클라이언트 다운로드에서 AWS VPN클라이언트를 다운로드하고 설치할 수 있습니다. AWS 제공된 클라이언트는 자동 업데이트를 지원하지 않습니다.

요구 사항

AWS 제공된 macOS용 클라이언트를 사용하려면 다음이 필요합니다.

- macOS 몬터레이 (12.0), 벤츄라 (13.0) 또는 소노마 (14.0).
- x86_64 프로세서 호환.
- 클라이언트는 컴퓨터에 포트 8096을 예약합니다. TCP
- SAML기반 페더레이션 인증 (Single Sign-On) 을 사용하는 클라이언트 VPN 엔드포인트의 경우 클라이언트는 포트 35001을 예약합니다. TCP

> **Note**
>
> Apple 실리콘 프로세서가 장착된 Mac을 사용하는 경우 Rosetta 2를 설치하여 클라이언트 소프트웨어를 실행해야 합니다. 자세한 내용은 Apple 웹 사이트의 Rosetta 번역 환경에 대한 정보를 참조하십시오.

주제

- AWS 제공된 macOS용 클라이언트를 VPN 사용하여 클라이언트에 연결
- AWS Client VPN macOS용 릴리스 노트

AWS 제공된 macOS용 클라이언트를 VPN 사용하여 클라이언트에 연결

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

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

AWS 제공된 macOS용 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. VPN구성 파일의 경우 클라이언트 VPN 관리자로부터 받은 구성 파일을 찾아보십시오. [Open]을 선택합니다.
6. 프로파일 추가를 선택합니다.
7. [AWS VPN Client] 창에서 프로파일이 선택되어 있는지 확인한 다음 [연결(Connect)]을 선택합니다. 클라이언트 VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
8. 연결에 대한 통계를 보려면 연결, 세부 정보 표시를 선택합니다.
9. 연결을 해제하려면 [AWS VPN Client] 창에서 [연결 해제(Disconnect)]를 선택합니다. 또는 메뉴 표시줄에서 클라이언트 아이콘을 선택한 다음 Disconnect < >를 선택합니다. your-profile-name

AWS Client VPN macOS용 릴리스 노트

다음 표에는 AWS Client VPN macOS용 최신 및 이전 버전의 릴리스 노트와 다운로드 링크가 나와 있습니다.

> **Note**
>
> 우리는 매 릴리스마다 사용성 및 보안 수정 사항을 계속 제공합니다. 모든 플랫폼에 최신 버전을 사용할 것을 강력히 권장합니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크
3.12.0	• `tap-sleep` Open VPN 플래그에 대한 지원이 추가되었습니다. • 오픈 VPN 및 오픈 SSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	다운로드 버전 3.12.0 sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa e33ac18ec edafd366d9e4b13
3.11.0	• 오픈 라이브러리 및 오픈 라이브러리를 업데이트했습니다VPN. SSL	2024년 7월 29일	다운로드 버전 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f

버전	변경	날짜	다운로드 링크
3.10.0	• 근거리 통신망 범위가 변경되면 자동으로 다시 연결합니다. • 네트워크 전환 중 DNS 복원 문제가 해결되었습니다. • SAML엔드포인트와 연결된 경우 자동 애플리케이션 포커스가 제거되었습니다.	2024년 5월 21일	다운로드 버전 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4add d4404e84287dd
3.9.2	• 버전 12.3 이후 Chromium 기반 브라우저의 SAML 인증 문제가 해결되었습니다. • macOS 소노마에 대한 지원이 추가되었습니다. macOS Big Sur에 대한 지원을 중단하십시오. • 보안 태세가 개선되었습니다.	2024년 4월 11일	버전 3.9.2 다운로드 sha256:37 4467d991e 8953b5032 e5b985cda 80a0a0ea2 7f5d5f23c f16c556a1 568b0d480
3.9.1	• 로컬 액터가 상승된 권한으로 임의의 명령을 실행할 수 있도록 허용할 수 있는 버퍼 오버플로 액션을 수정했습니다. • 애플리케이션 업데이트 다운로드 진행률 표시줄을 수정했습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	버전 3.9.1 다운로드 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e8e899e971

버전	변경	날짜	다운로드 링크
3.9.0	• 일부 구성의 연결 문제가 수정되었습니다. LAN • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• NAT64이 (가) 클라이언트 네트워크에서 활성화되었을 때 발생하는 연결 문제를 수정했습니다. • 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

버전	변경	날짜	다운로드 링크
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
3.2.0	• “verify-x509-name” 오픈 플래그에 대한 지원이 추가되었습니다. VPN • 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.

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.
1.4.0	• 연결 중 서버 모니터링이 추가되었습니다. DNS 설정과 일치하지 않는 경우 VPN 설정이 다시 구성됩니다. • 일부 경우에 페더레이션 인증 연결 시도가 수정되었습니다. • 사소한 버그 수정 및 개선	2021년 11월 9일	더 이상 지원되지 않습니다.
1.3.5	• 오픈 VPN 플래그에 대한 지원이 추가되었습니다: connect-retry-max, 개발자 유형, 킵얼라이브, 핑, 핑-리스타트, 풀, rcvbuf,. server-poll-timeout • 사소한 버그 수정 및 개선	2021년 9월 20일	더 이상 지원되지 않습니다.
1.3.4	• 오픈 VPN 플래그: dhcp-option에 대한 지원이 추가되었습니다. • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.3.3	• 오픈 VPN 플래그 (비활성, 풀 필터, 경로) 에 대한 지원이 추가되었습니다. • 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.
1.3.2	• 구성되면 IPv6 누수 방지 기능을 추가하세요. • [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 설정을 제거하던 문제가 해결되었습니다. • 상호 인증에 유효하지 않은 인증서를 사용할 때 연결 문제가 야기되는 문제가 수정되었습니다. • 'route-ipv6' 오픈 디렉티브에 대한 지원이 추가되었습니다. VPN • 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.

버전	변경	날짜	다운로드 링크
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	• Open 구성에 주석에 대한 지원이 추가되었습니다. VPN • TLS핸드셰이크 오류에 대한 오류 메시지를 추가했습니다. • 일부 사용자에게 영향을 미치는 제거 버그가 수정되었습니다.	2020년 10월 8일	더 이상 지원되지 않습니다.
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	• SAML2.0 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	• 해결되지 않던 문제가 DNS 해결되었습니다. • 더 긴 연결로 인한 앱 충돌 문제를 수정되었습니다. • MFA문제가 해결되었습니다.	2020년 4월 2일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.1.0	• macOS DNS 구성에 대한 지원이 추가되었습니다. • 사용자 인터페이스에 표시된 텍스트를 숨기거나 표시하는 개방형 VPN 정적 챌린지 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 리눅스용

이 섹션에서는 AWS 제공된 Linux용 클라이언트를 설치한 다음 AWS 제공된 클라이언트를 사용하여 VPN 연결을 설정하는 방법을 설명합니다. AWS 제공된 Linux용 클라이언트는 자동 업데이트를 지원하지 않습니다. 최신 업데이트 및 다운로드에 대해서는 를 참조하십시오the section called “릴리스 정보”.

AWS 제공된 Linux용 클라이언트를 VPN 사용하여 클라이언트에 연결하기 위한 요구 사항

AWS 제공된 Linux용 클라이언트를 사용하려면 다음이 필요합니다.

- 우분투 18.04 LTS 또는 우분투 20.04 (전용) LTS AMD64

클라이언트는 컴퓨터에 포트 8096을 TCP 예약합니다. SAML기반 페더레이션 인증 (Single Sign-On)을 사용하는 클라이언트 VPN 엔드포인트의 경우 클라이언트는 포트 35001을 예약합니다. TCP

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

주제

- AWS 제공된 Linux용 클라이언트 설치
- AWS 제공된 Linux용 클라이언트에 연결

- AWS Client VPN 리눅스용 릴리스 노트

AWS 제공된 Linux용 클라이언트 설치

AWS 제공된 Linux용 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 공개 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. Ubuntu 버전에 따라 해당 명령을 사용하여 Ubuntu OS에 리포지토리를 추가합니다.

   Ubuntu 18.04

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

   Ubuntu 20.04

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

3. 다음 명령을 사용하여 시스템의 리포지토리를 업데이트합니다.

```
sudo apt-get update
```

4. 다음 명령을 사용하여 AWS 제공된 Linux용 클라이언트를 설치합니다.

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

옵션 2: .deb 패키지 파일을 사용하여 설치

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

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

2. 유틸리티를 사용하여 AWS 제공된 Linux용 클라이언트를 설치합니다. dpkg

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

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

1. AWS 클라이언트 VPN 다운로드에서.deb 패키지 파일을 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.

AWS 제공된 Linux용 클라이언트에 연결

다음 단계에서는 AWS 제공된 클라이언트를 AWS VPN 클라이언트라고도 합니다.

AWS 제공된 Linux용 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. VPN구성 파일의 경우 클라이언트 VPN 관리자로부터 받은 구성 파일을 찾아보십시오. [Open]을 선택합니다.
6. 프로파일 추가를 선택합니다.
7. [AWS VPN Client] 창에서 프로파일이 선택되어 있는지 확인한 다음 [연결(Connect)]을 선택합니다. 클라이언트 VPN 엔드포인트가 자격 증명 기반 인증을 사용하도록 구성된 경우 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
8. 연결에 대한 통계를 보려면 연결, 세부 정보 표시를 선택합니다.
9. 연결을 해제하려면 [AWS VPN Client] 창에서 [연결 해제(Disconnect)]를 선택합니다.

AWS Client VPN 리눅스용 릴리스 노트

다음 표에는 AWS Client VPN Linux용 최신 및 이전 버전에 대한 릴리스 노트와 다운로드 링크가 나와 있습니다.

> **Note**
>
> 우리는 매 릴리스마다 사용성 및 보안 수정 사항을 계속 제공합니다. 모든 플랫폼에 최신 버전을 사용할 것을 강력히 권장합니다. 이전 버전은 사용성 및/또는 보안 문제의 영향을 받을 수 있습니다. 세부 정보는 릴리스 정보를 참조하세요.

버전	변경	날짜	다운로드 링크
3.15.0	• `tap-sleep` 오픈 VPN 플래그에 대한 지원이 추가되었습니다. • 오픈 VPN 및 오픈 SSL 라이브러리를 업데이트했습니다.	2024년 8월 12일	버전 3.15.0 다운로드 sha256:5cf3eb08de96821b0ad3d3d3d3174b2e308041d5490a3edb772dfd89a6d89d012
3.14.0	• 오픈 VPN 라이브러리와 오픈 SSL 라이브러리를 업데이트했습니다.	2024년 7월 29일	버전 3.14.0 다운로드 sha256:bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60

버전	변경	날짜	다운로드 링크
3.13.0	• 근거리 통신망 범위가 변경되면 자동으로 다시 연결합니다.	2024년 5월 21일	버전 3.13.0 다운로드 sha256: e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1
3.12.2	• 버전 12.3 이후 Chromium 기반 브라우저의 SAML 인증 문제가 해결되었습니다.	2024년 4월 11일	버전 3.12.2 다운로드 sha256: f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
3.12.1	• 로컬 액터가 상승된 권한으로 임의의 명령을 실행할 수 있도록 허용할 수 있는 버퍼 오버플로 액션을 수정했습니다. • 보안 태세가 개선되었습니다.	2024년 2월 16일	버전 3.12.1 다운로드 sha256:547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0

버전	변경	날짜	다운로드 링크
3.12.0	• 일부 구성의 연결 문제가 수정되었습니다. LAN	2023년 12월 19일	다운로드 버전 3.12.0 sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1
3.11.0	• “일부 LAN 구성의 연결 문제 해결됨”에 대한 롤백 • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• 일부 LAN 구성의 연결 문제를 수정했습니다. • 접근성을 개선했습니다.	2023년 12월 6일	다운로드 버전 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51

버전	변경	날짜	다운로드 링크
3.9.0	• NAT64이 (가) 클라이언트 네트워크에서 활성화되었을 때 발생하는 연결 문제를 수정했습니다. • 사소한 버그 수정 및 개선	2023년 8월 24일	다운로드 버전 3.9.0 sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454
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” 오픈 플래그에 대한 지원이 추가되었습니다. VPN	2023년 2월 14일	더 이상 지원되지 않음

버전	변경	날짜	다운로드 링크
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.
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	• 오픈 VPN 플래그에 대한 지원이 추가되었습니다: 개발 유형, 킵얼라이브 connect-retry-max, 핑, 핑-리스타트, 풀, rcvbuf 등. server-poll-timeout • 사소한 버그 수정 및 개선	2021년 9월 28일	더 이상 지원되지 않습니다.
1.0.1	• Ubuntu 애플리케이션 바에서 종료하는 옵션이 활성화되었습니다. • 비활성, 풀 필터, 라우트와 같은 오픈 플래그에 대한 지원이 추가되었습니다. VPN • 사소한 버그 수정 및 개선	2021년 8월 4일	더 이상 지원되지 않습니다.

버전	변경	날짜	다운로드 링크
1.0.0	최초 릴리스입니다.	2021년 6월 11일	더 이상 지원되지 않습니다.

오픈 클라이언트를 사용하여 클라이언트 VPN VPN 엔드포인트에 연결

일반 Open Client 애플리케이션을 사용하여 클라이언트 VPN VPN 엔드포인트에 연결할 수 있습니다.

> **Important**
>
> 클라이언트 VPN 엔드포인트가 SAML기반 페더레이션 인증을 사용하도록 구성된 경우 개방형 VPN 기반 VPN 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

클라이언트 애플리케이션

- Windows 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 연결
- Android 또는 iOS 클라이언트 애플리케이션을 사용하여 VPN 클라이언트 VPN 엔드포인트에 연결
- macOS 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 연결
- Open Client 애플리케이션을 사용하여 VPN 클라이언트 VPN 엔드포인트에 연결

Windows 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 연결

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

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

문제 해결 정보는 Windows 기반 클라이언트와의 클라이언트 VPN 연결 문제 해결를 참조하세요.

> **Important**
>
> 클라이언트 VPN 엔드포인트가 SAML기반 페더레이션 인증을 사용하도록 구성된 경우 개방형 VPN 기반 VPN 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

Tasks

- Open이 설치된 Windows 인증서 시스템 저장소의 인증서를 사용하십시오. VPN

- Open을 사용하세요. VPN GUI
- 오픈 VPN 커넥트 클라이언트 사용

Open이 설치된 Windows 인증서 시스템 저장소의 인증서를 사용하십시오. VPN

Windows 인증서 시스템 저장소의 인증서와 개인 키를 사용하도록 Open VPN 클라이언트를 구성할 수 있습니다. 이 옵션은 스마트 카드를 클라이언트 VPN 연결의 일부로 사용할 때 유용합니다. VPN클라이언트 cryptoapicert 열기 옵션에 대한 자세한 내용은 Open 웹 사이트의 VPNOpen용 참조 설명서를 참조하십시오. VPN

> **Note**
>
> 인증서는 로컬 컴퓨터에 저장되어야 합니다.

크립토APICert 옵션을 Open과 함께 사용하려면 VPN

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 참조하십시오.
3. 계정에 로컬 컴퓨터 인증서를 읽을 수 있는 권한이 있는지 확인합니다. Microsoft Management Console을 사용하여 권한을 수정할 수 있습니다. 자세한 내용은Microsoft Technet 웹 사이트에서 로컬 컴퓨터 인증서 저장소를 볼 수 있는 권한을 참조하세요.
4. Open VPN 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 Technet 웹 사이트에서 방법: 인증서의 지문 검색을 참조하세요.

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

구성을 완료한 후 VPN Open을 사용하여 연결을 설정합니다.

Open을 사용하세요. VPN GUI

다음 절차는 Windows 컴퓨터에서 Open VPN GUI Client 응용 프로그램을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다.

> **Note**
>
> Open VPN Client 애플리케이션에 대한 자세한 내용은 Open VPN 웹 사이트의 커뮤니티 다운로드를 참조하십시오.

VPN연결을 설정하려면

1. Open VPN 클라이언트 애플리케이션을 시작합니다.
2. Windows 작업 표시줄에서 아이콘 표시/숨기기를 선택합니다. [열기 VPN GUI] 를 마우스 오른쪽 단추로 클릭한 다음 [파일 가져오기] 를 선택합니다.
3. [열기] 대화 상자에서 클라이언트 VPN 관리자로부터 받은 구성 파일을 선택하고 [열기] 를 선택합니다.
4. Windows 작업 표시줄에서 아이콘 표시/숨기기를 선택합니다. 열기를 VPN GUI 마우스 오른쪽 단추로 클릭한 다음 Connect를 선택합니다.

오픈 VPN 커넥트 클라이언트 사용

다음 절차는 Windows 컴퓨터에서 Open VPN Connect Client 응용 프로그램을 사용하여 VPN 연결을 설정하는 방법을 보여 줍니다.

> **Note**
>
> 자세한 내용은 Open VPN 웹 사이트의 Windows를 사용하여 액세스 서버에 연결을 참조하십시오.

VPN연결을 설정하려면

1. Open VPN Connect 클라이언트 애플리케이션을 시작합니다.

2. Windows 작업 표시줄에서 아이콘 표시/숨기기를 선택합니다. 열기를 마우스 오른쪽 단추로 클릭한 다음 VPN 프로필 가져오기를 선택합니다.
3. 파일에서 가져오기를 선택하고 클라이언트 VPN 관리자로부터 받은 구성 파일을 선택합니다.
4. 연결을 시작하려면 연결 프로파일을 선택합니다.

Android 또는 iOS 클라이언트 애플리케이션을 사용하여 VPN 클라이언트 VPN 엔드포인트에 연결

> **Important**
>
> 클라이언트 VPN 엔드포인트가 SAML기반 페더레이션 인증을 사용하도록 구성된 경우 개방형 VPN 기반 VPN 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

다음 정보는 Android 또는 iOS 모바일 장치에서 Open VPN Client 애플리케이션을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다. Android와 iOS는 단계가 동일합니다.

> **Note**
>
> iOS 또는 Android용 Open VPN Client 애플리케이션을 다운로드하고 사용하는 방법에 대한 자세한 내용은 Open VPN 웹 사이트의 Open VPN Connect 사용 설명서를 참조하십시오.

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

연결을 설정하려면 Open VPN client 애플리케이션을 시작한 다음 클라이언트 VPN 관리자로부터 받은 파일을 가져오십시오.

macOS 클라이언트 애플리케이션을 사용하여 클라이언트 VPN 엔드포인트에 연결

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

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

문제 해결 정보는 macOS 클라이언트와의 클라이언트 VPN 연결 문제 해결를 참조하세요.

> **Important**
>
> 클라이언트 VPN 엔드포인트가 SAML기반 페더레이션 인증을 사용하도록 구성된 경우 개방형 VPN 기반 VPN 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

주제

- Tunnelblick을 시작하여 연결을 설정합니다. AWS Client VPN
- Open VPN Connect 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결

Tunnelblick을 시작하여 연결을 설정합니다. AWS Client VPN

다음 절차는 macOS 컴퓨터에서 Tunnelblick 클라이언트 애플리케이션을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다.

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

연결을 설정하려면 VPN

1. Tunnelblick 클라이언트 애플리케이션을 시작하고 I have configuration files(구성 파일이 있음)를 선택합니다.
2. VPN관리자로부터 받은 구성 파일을 구성 패널에 끌어다 놓습니다.
3. Configurations(구성) 패널에서 구성 파일을 선택하고 Connect(연결)를 선택합니다.

Open VPN Connect 클라이언트를 사용하여 AWS Client VPN 엔드포인트에 연결

다음 절차는 macOS 컴퓨터에서 Open VPN Connect Client 응용 프로그램을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다.

> **Note**
>
> 자세한 내용은 Open VPN 웹 사이트에서 macOS를 사용하여 액세스 서버에 연결을 참조하십시오.

연결을 설정하려면 VPN

1. Open VPN 애플리케이션을 시작하고 가져오기, 로컬 파일에서... 를 선택합니다. .
2. VPN관리자로부터 받은 구성 파일을 찾아 [Open] 을 선택합니다.

Open Client 애플리케이션을 사용하여 VPN 클라이언트 VPN 엔드포인트에 연결

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

시작하기 전에 클라이언트 VPN 관리자가 클라이언트 엔드포인트를 생성하고 클라이언트 VPN 엔드포인트 구성 파일을 제공했는지 확인하십시오. VPN

문제 해결 정보는 Linux 기반 클라이언트와의 클라이언트 VPN 연결 문제 해결를 참조하세요.

> **Important**
>
> 클라이언트 VPN 엔드포인트가 SAML기반 페더레이션 인증을 사용하도록 구성된 경우 개방형 VPN 기반 VPN 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

주제

- Open VPN - 네트워크 AWS Client VPN 관리자를 사용하여 연결 생성
- Open을 AWS Client VPN 사용하여 연결을 생성합니다. VPN

Open VPN - 네트워크 AWS Client VPN 관리자를 사용하여 연결 생성

다음 절차는 Ubuntu GUI 컴퓨터에서 네트워크 관리자를 통해 Open VPN 애플리케이션을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다.

연결을 설정하려면 VPN

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. 옆에 있는 더하기 VPN기호 (+) 를 선택한 다음 파일에서 가져오기... 를 선택합니다. .
4. VPN관리자로부터 받은 구성 파일을 찾아 [Open] 을 선택합니다.
5. 추가 VPN 창에서 추가를 선택합니다.
6. 추가한 VPN 프로필 옆의 토글을 활성화하여 연결을 시작합니다.

Open을 AWS Client VPN 사용하여 연결을 생성합니다. VPN

다음 절차는 Ubuntu 컴퓨터에서 Open VPN 애플리케이션을 사용하여 VPN 연결을 설정하는 방법을 보여줍니다.

연결을 설정하려면 VPN

1. 다음 명령을 VPN 사용하여 Open을 설치합니다.

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

2. VPN관리자로부터 받은 구성 파일을 로드하여 연결을 시작합니다.

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

클라이언트 VPN 연결 문제 해결

다음 항목을 사용하여 클라이언트 애플리케이션을 사용하여 클라이언트 엔드포인트에 연결할 때 발생할 수 있는 문제를 해결하십시오. VPN

주제

관리자를 위한 클라이언트 VPN 엔드포인트 문제 해결

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

클라이언트 VPN 엔드포인트 문제 해결에 대한 추가 정보는 AWS Client VPN 관리자 안내서의 클라이언트 VPN 문제 해결을 참조하십시오.

AWS 제공된 클라이언트에 진단 로그를 전송하십시오. AWS Support

AWS 제공된 클라이언트에 문제가 있어 문제 해결을 AWS Support 위해 문의해야 하는 경우 AWS 제공된 클라이언트에 진단 로그를 보낼 수 있는 옵션이 있습니다. AWS Support이 옵션은 Windows, macOS 및 Linux 클라이언트 애플리케이션 모두에서 사용할 수 있습니다.

파일을 전송하기 전에 진단 로그 액세스 AWS Support 허용에 동의해야 합니다. 동의하면 참조 번호가 제공되어 해당 사용자가 파일에 즉시 액세스할 수 AWS Support 있도록 제공할 수 있습니다.

진단 로그 보내기

다음 단계에서는 AWS 제공된 클라이언트를 AWS VPN 클라이언트라고도 합니다.

AWS 제공된 Windows용 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.

   AWS Support연락할 때 참조 번호를 제공해야 합니다.

AWS 제공된 macOS용 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.

   AWS Support연락할 때 참조 번호를 제공해야 합니다.

AWS 제공된 Ubuntu용 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 클립보드에 복사할 수 있습니다.

   AWS Support연락할 때 참조 번호를 제공해야 합니다.

Windows 기반 클라이언트와의 클라이언트 VPN 연결 문제 해결

다음 섹션에는 Windows 기반 클라이언트를 사용하여 클라이언트 엔드포인트에 연결할 때 발생할 수 있는 문제에 대한 정보가 포함되어 있습니다. VPN

주제

- AWS 제공된 클라이언트
- 열기 VPN GUI
- VPN연결 클라이언트를 엽니다.

AWS 제공된 클라이언트

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.
- 오픈 VPN 로그: 오픈 VPN 프로세스에 대한 정보가 들어 있습니다. 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

- 클라이언트가 연결할 수 없습니다.
- “TAP-Windows 어댑터 없음” 로그 메시지와 함께 클라이언트에 연결할 수 없습니다.
- 클라이언트가 다시 연결 중 상태로 멈췄습니다.
- VPN연결 프로세스가 예기치 않게 종료됩니다.
- 애플리케이션을 시작하지 못했습니다.
- 클라이언트가 프로필을 만들 수 없습니다.
- Windows 10 또는 11을 PCs 사용하는 Dell에서 클라이언트 충돌이 발생합니다.
- VPN팝업 메시지와 함께 연결이 끊깁니다.

클라이언트가 연결할 수 없습니다.

문제

AWS 제공된 클라이언트는 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터에서 다른 Open VPN 프로세스가 이미 실행 중이므로 클라이언트가 연결할 수 없습니다.
- 구성 파일(.ovpn)이 잘못되었습니다.

Solution

컴퓨터에 실행 중인 다른 Open VPN 애플리케이션이 있는지 확인하세요. 문제가 있는 경우 이러한 프로세스를 중지하거나 종료한 다음 클라이언트 VPN 엔드포인트에 다시 연결해 보십시오. 열린 VPN 로그에 오류가 있는지 확인하고 클라이언트 VPN 관리자에게 다음 정보를 확인하도록 요청하십시오.

- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.
- 아직 유효한지 확인하세요. CRL 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하십시오.

“TAP-Windows 어댑터 없음” 로그 메시지와 함께 클라이언트에 연결할 수 없습니다.

문제

AWS 제공된 클라이언트가 클라이언트 VPN 엔드포인트에 연결할 수 없으며 애플리케이션 로그에 다음과 같은 오류 메시지가 나타납니다. “이 시스템에는 TAP -Windows 어댑터가 없습니다. 시작 -> 모든 프로그램 -> TAP Windows -> 유틸리티 -> 새 TAP -Windows 가상 이더넷 어댑터 추가”로 이동하여 TAP -Windows 어댑터를 생성할 수 있어야 합니다.

Solution

다음 조치 중 하나 이상을 수행하여 이 문제를 해결할 수 있습니다.

- -Windows 어댑터를 다시 시작합니다. TAP
- TAP-Windows 드라이버를 다시 설치합니다.
- 새 TAP -Windows 어댑터를 생성하십시오.

클라이언트가 다시 연결 중 상태로 멈췄습니다.

문제

AWS 제공된 클라이언트가 클라이언트 VPN 엔드포인트에 연결을 시도하지만 재연결 상태에서 멈췄습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터가 인터넷에 연결되어 있지 않습니다.
- DNS호스트 이름이 IP 주소로 확인되지 않습니다.
- Open VPN 프로세스는 끝점에 무한정 연결을 시도합니다.

Solution

컴퓨터가 인터넷에 연결되어 있는지 확인합니다. 클라이언트 VPN 관리자에게 문의하여 구성 파일의 `remote` 지시문이 유효한 IP 주소로 확인되는지 확인하십시오. AWS VPN클라이언트 창에서 연결 끊기를 선택하여 VPN 세션 연결을 끊고 다시 연결해 볼 수도 있습니다.

VPN연결 프로세스가 예기치 않게 종료됩니다.

문제

클라이언트 VPN 엔드포인트에 연결하는 동안 클라이언트가 예기치 않게 종료됩니다.

원인

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

Solution

AWS 제공된 클라이언트 설치 프로그램을 다시 실행하여 필요한 종속 항목을 모두 설치합니다.

애플리케이션을 시작하지 못했습니다.

문제

Windows 7에서는 AWS 제공된 클라이언트를 열려고 해도 해당 클라이언트가 시작되지 않습니다.

원인

. NET프레임워크 4.7.2 이상이 컴퓨터에 설치되어 있지 않습니다. 클라이언트를 실행하는 데 필요합니다.

Solution

AWS 제공된 클라이언트 설치 프로그램을 다시 실행하여 필요한 종속 항목을 모두 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

클라이언트 VPN 엔드포인트가 상호 인증을 사용하는 경우 구성 (.ovpn) 파일에는 클라이언트 인증서 및 키가 포함되지 않습니다.

Solution

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

Windows 10 또는 11을 PCs 사용하는 Dell에서 클라이언트 충돌이 발생합니다.

문제

Windows 10 또는 11을 실행하는 특정 Dell PCs (데스크탑 및 랩톱) 에서 VPN 구성 파일을 가져오기 위해 파일 시스템을 탐색할 때 충돌이 발생할 수 있습니다. 이 문제가 발생하는 경우 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 특히 다음 세 DLLs 가지 경우 AWS 제공된 클라이언트와 충돌을 일으킬 수 있습니다.

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

Solution

이 문제를 방지하려면 먼저 클라이언트가 AWS 제공된 클라이언트의 최신 버전을 사용하고 있는지 확인하십시오. AWS 클라이언트 VPN 다운로드로 이동하여 새 버전을 사용할 수 있는 경우 최신 버전으로 업그레이드하십시오.

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. 애플리케이션을 업그레이드하지 않으려면 파일을 삭제하거나 이름을 바꿀 수도 있습니다. DLL 그러나 이렇게 하면 Dell 백업 및 복구 애플리케이션이 제대로 작동하지 않습니다.

파일 삭제 또는 이름 변경 DLL

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 디렉토리에서 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: .dll.bak). DBROverlayIconBackuped

VPN팝업 메시지와 함께 연결이 끊깁니다.

문제

다음과 같은 팝업 메시지와 함께 VPN 연결이 VPN 끊깁니다. “기기가 연결된 로컬 네트워크의 주소 공간이 변경되어 연결이 종료됩니다. 새 VPN 연결을 설정하세요.”

원인

TAP-Windows 어댑터에 필요한 설명이 포함되어 있지 않습니다.

Solution

아래 `Description` 필드가 일치하지 않는 경우 먼저 TAP -Windows 어댑터를 제거한 다음 AWS 제공된 클라이언트 설치 프로그램을 다시 실행하여 필요한 종속성을 모두 설치하십시오.

```
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
```

열기 VPN GUI

다음 문제 해결 정보는 윈도우 10 홈 (64비트) 및 윈도우 서버 2016 (64비트) 의 오픈 VPN GUI 소프트웨어 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
```

VPN연결 클라이언트를 엽니다.

다음 문제 해결 정보는 윈도우 10 홈 (64비트) 및 윈도우 서버 2016 (64비트) 의 Open VPN Connect Client 소프트웨어 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
```

해결할 수 없습니다. DNS

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

DNS이름을 확인할 수 없습니다. DNS캐싱을 방지하려면 클라이언트가 DNS 이름 앞에 임의의 문자열을 추가해야 하지만 일부 클라이언트는 이렇게 하지 않습니다.

Solution

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

PKI별칭이 없습니다.

문제

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

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

원인

Open VPN Connect Client 소프트웨어에서 상호 인증을 사용하여 인증을 시도하는 알려진 문제가 있습니다. 구성 파일에 클라이언트 키와 인증서가 없으면 인증이 실패합니다.

Solution

클라이언트 VPN 구성 파일에 임의의 클라이언트 키와 인증서를 지정하고 새 구성을 Open VPN Connect Client 소프트웨어로 가져옵니다. 또는 오픈 클라이언트 (v11.12.0.0) 또는 Viscosity VPN GUI 클라이언트 (v.1.7.14) 와 같은 다른 클라이언트를 사용할 수도 있습니다.

macOS 클라이언트와의 클라이언트 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.

주제

- AWS 제공된 클라이언트
- Tunnelblick
- 열기 VPN

AWS 제공된 클라이언트

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.
- 오픈 VPN 로그: 오픈 VPN 프로세스에 대한 정보가 들어 있습니다. 이러한 로그 앞에 'ovpn_aws_vpn_client_'가 붙습니다.

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

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

AWS 제공된 클라이언트는 컴퓨터의 다음 위치에 구성 파일을 저장합니다.

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

주제

클라이언트가 연결할 수 없습니다.

문제

AWS 제공된 클라이언트는 클라이언트 VPN 엔드포인트에 연결할 수 없습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터에서 다른 Open VPN 프로세스가 이미 실행 중이므로 클라이언트가 연결할 수 없습니다.
- 구성 파일(.ovpn)이 잘못되었습니다.

Solution

컴퓨터에 실행 중인 다른 Open VPN 애플리케이션이 있는지 확인하세요. 문제가 있는 경우 이러한 프로세스를 중지하거나 종료한 다음 클라이언트 VPN 엔드포인트에 다시 연결해 보십시오. 열린 VPN 로그에 오류가 있는지 확인하고 클라이언트 VPN 관리자에게 다음 정보를 확인하도록 요청하십시오.

- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.

- 아직 유효한지 확인하세요. CRL 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하십시오.

클라이언트가 다시 연결 중 상태로 멈췄습니다.

문제

AWS 제공된 클라이언트가 클라이언트 VPN 엔드포인트에 연결을 시도하지만 재연결 상태에서 멈췄습니다.

원인

이 문제의 원인은 다음 중 하나일 수 있습니다.

- 컴퓨터가 인터넷에 연결되어 있지 않습니다.
- DNS호스트 이름이 IP 주소로 확인되지 않습니다.
- Open VPN 프로세스는 끝점에 무한정 연결을 시도합니다.

Solution

컴퓨터가 인터넷에 연결되어 있는지 확인합니다. 클라이언트 VPN 관리자에게 문의하여 구성 파일의 `remote` 지시문이 유효한 IP 주소로 확인되는지 확인하십시오. AWS VPN클라이언트 창에서 연결 끊기를 선택하여 VPN 세션 연결을 끊고 다시 연결해 볼 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

클라이언트 VPN 엔드포인트가 상호 인증을 사용하는 경우 구성 (.ovpn) 파일에는 클라이언트 인증서 및 키가 포함되지 않습니다.

Solution

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

도우미 도구가 필요합니다. 오류

문제

연결을 시도할 때 다음 오류가 발생합니다. VPN

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

Solution

AWS re:Post에 대한 다음 문서를 참조하십시오. AWSVPN클라이언트 - 헬퍼 도구가 필요합니다. 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 상세 정보를 높이려면 Tunnelblick 애플리케이션을 열고 설정을 선택한 다음 로그 수준 값을 조정합니다. VPN

암호 알고리즘 '-256-'를 찾을 수 없습니다. AES GCM

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

응용 프로그램이 암호 알고리즘 -256-를 지원하지 않는 Open VPN 버전을 사용하고 있습니다. AES GCM

Solution

다음과 같이 호환되는 Open VPN 버전을 선택하십시오.

1. Tunnelblick 애플리케이션을 엽니다.
2. 설정을 선택합니다.
3. 오픈 VPN 버전의 경우 2.4.6을 선택합니다. 오픈 SSL 버전은 v1.0.2q입니다.

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

클라이언트 관리자에게 새 구성 파일을 요청하십시오. VPN

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. 하지만 클라이언트 인증서에 확장 키 사용 (EKU) 필드가 서버 인증을 위해 활성화되어 있기 때문에 클라이언트 인증이 실패합니다.

Solution

올바른 클라이언트 인증서와 키를 사용하고 있는지 확인합니다. 필요한 경우 클라이언트 VPN 관리자에게 확인하십시오. 클라이언트 VPN 엔드포인트에 연결하는 데 클라이언트 인증서가 아닌 서버 인증서를 사용하는 경우 이 오류가 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

클라이언트 VPN 관리자에게 새 클라이언트 인증서를 요청하세요.

열기 VPN

다음 문제 해결 정보는 macOS High Sierra 10.13.6의 Open VPN Connect Client 소프트웨어 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
```

해결할 수 없습니다. DNS

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

Open VPN Connect에서는 클라이언트 VPN DNS 이름을 확인할 수 없습니다.

Solution

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

Linux 기반 클라이언트와의 클라이언트 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

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

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

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

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

문제

VPN연결이 설정된 후에도 클라이언트 엔드포인트에 구성된 네임서버 대신 기본 시스템 네임서버로 DNS 쿼리가 이동하는 경우도 있습니다. VPN

원인

클라이언트는 Linux 시스템에서 사용할 수 있는 서비스인 systemd-resolve 서비스와 상호 작용하며, 이 서비스는 중앙 관리 역할을 합니다. DNS 클라이언트 엔드포인트에서 푸시되는 DNS 서버를 구성하는 데 사용됩니다. VPN Systemd-Resolved는 클라이언트 VPN 엔드포인트에서 제공하는 DNS 서버에 가장 높은 우선 순위를 설정하지 않기 때문에 문제가 발생합니다. 대신 로컬 시스템에 구성된 기존 서버 목록에 DNS 서버를 추가합니다. 따라서 원본 DNS 서버가 여전히 우선 순위가 가장 높아 DNS 쿼리를 해결하는 데 사용될 수 있습니다.

Solution

1. Open VPN config 파일의 첫 줄에 다음 지시문을 추가하여 모든 DNS 쿼리가 터널로 전송되도록 하십시오VPN.

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

2. systemd-resolved에서 제공하는 스터브 리졸버를 사용합니다. 이렇게 하려면 시스템에서 다음 명령을 실행하여 /etc/resolv.conf을 /run/systemd/resolve/stub-resolv.conf에 symlink로 연결합니다.

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

3. (선택 사항) 시스템 해결 방식의 프록시 DNS 쿼리를 원하지 않고 쿼리를 실제 DNS 네임서버로 직접 보내려면 대신 로 심볼릭 링크를 연결하세요. /etc/resolv.conf /run/systemd/resolve/resolv.conf

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

DNS응답 캐싱, 인터페이스별 구성, 적용 등과 같이 시스템에서 확인된 구성을 우회하려면 이 절차를 수행하는 것이 좋습니다. DNS DNSSec 이 옵션은 연결 시 공개 DNS 레코드를 개인 레코드로 재정의해야 하는 경우에 특히 유용합니다. VPN 예를 들어, DNS 사설 VPC IP로 확인되는 www.example.com용 레코드가 있는 사설 확인자가 비공개에 있을 수 있습니다. 이 옵션을 사용하여 퍼블릭 IP로 확인되는 www.example.com의 퍼블릭 레코드를 재정의할 수 있습니다.

VPN열기 (명령줄)

문제

DNS해상도가 작동하지 않아 연결이 제대로 작동하지 않습니다.

원인

DNS서버가 클라이언트 VPN 엔드포인트에 구성되어 있지 않거나 클라이언트 소프트웨어에서 서버를 준수하지 않습니다.

Solution

다음 단계를 사용하여 DNS 서버가 구성되어 있고 제대로 작동하는지 확인하십시오.

1. 로그에 DNS 서버 항목이 있는지 확인하십시오. 다음 예제에서는 클라이언트 VPN 엔드포인트에 구성된 DNS 서버가 192.168.0.2 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 클라이언트 VPN 관리자에게 클라이언트 엔드포인트를 수정하고 클라이언트 VPN 엔드포인트에 DNS 서버 (예: VPC DNS 서버) 가 지정되었는지 확인하도록 요청하십시오. VPN 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 VPN 엔드포인트를 참조하십시오.

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 클라이언트 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 VPN 통해 열기 () GUI

문제

네트워크 관리자 열기 VPN 클라이언트를 사용할 때 연결이 실패하고 다음 오류가 발생합니다.

```
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 클라이언트 VPN 엔드포인트 DNS 이름을 확인할 수 없음에 대한 해결 방법을 참조하십시오.

일반적인 클라이언트 VPN 문제 해결

다음은 클라이언트를 사용하여 클라이언트 VPN 엔드포인트에 연결할 때 발생할 수 있는 일반적인 문제입니다.

TLS키 협상에 실패했습니다.

문제

TLS협상이 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 규칙으로 인해 TCP 트래픽이 UDP 차단되고 있습니다.
- 구성 파일(.ovpn)에서 잘못된 클라이언트 키와 인증서를 사용하고 있습니다.

- 클라이언트 인증서 취소 목록 (CRL) 이 만료되었습니다.

Solution

컴퓨터의 방화벽 규칙이 인바운드 또는 아웃바운드 TCP 또는 포트 443 또는 1194의 UDP 트래픽을 차단하는지 확인하십시오. 클라이언트 VPN 관리자에게 문의하여 다음 정보를 확인하십시오.

- 클라이언트 VPN 엔드포인트의 방화벽 규칙이 포트 443 TCP 또는 1194를 UDP 통한 트래픽을 차단하지 않는지 확인하십시오.
- 구성 파일에는 올바른 클라이언트 키와 인증서가 들어 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 구성 내보내기를 참조하세요.
- 여전히 CRL 유효하다는 것. 자세한 내용은 AWS Client VPN 관리자 안내서의 클라이언트 VPN 엔드포인트에 연결할 수 없는 클라이언트를 참조하십시오.

문서 기록

다음 표에서는 AWS 클라이언트 VPN 사용 설명서 업데이트에 대해 설명합니다.

변경 사항	설명	날짜
AWS 우분투용 제공 클라이언트 (3.15.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS 윈도우용 제공 클라이언트 (3.14.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS macOS용 제공 클라이언트 (3.12.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 8월 12일
AWS 우분투용 제공 클라이언트 (3.14.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일
AWS 윈도우용 제공 클라이언트 (3.13.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일
AWS macOS용 제공 클라이언트 (3.11.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 29일
AWS 윈도우용 제공 클라이언트 (3.12.1) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 7월 18일
AWS 우분투용 제공 클라이언트 (3.13.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS 윈도우용 제공 클라이언트 (3.12.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS macOS용 제공 클라이언트 (3.10.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 5월 21일
AWS macOS용 제공 클라이언트 (3.9.2) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일

AWS 우분투용 제공 클라이언트 (3.12.2) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일
AWS 윈도우용 제공 클라이언트 (3.11.2) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 4월 11일
AWS macOS용 제공 클라이언트 (3.9.1) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS 우분투용 제공 클라이언트 (3.12.1) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS 윈도우용 제공 클라이언트 (3.11.1) 출시	세부 정보는 릴리스 정보를 참조하세요.	2024년 2월 16일
AWS 우분투용 제공 클라이언트 (3.12.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 19일
AWS macOS용 제공 클라이언트 (3.9.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS 윈도우용 제공 클라이언트 (3.11.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS 우분투용 제공 클라이언트 (3.11.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS 우분투용 제공 클라이언트 (3.10.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 12월 6일
AWS 우분투용 제공 클라이언트 (3.9.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일
AWS macOS용 제공 클라이언트 (3.8.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일
AWS 윈도우용 제공 클라이언트 (3.10.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 24일

AWS 윈도우용 클라이언트 제공 (3.9.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS 우분투용 제공 클라이언트 (3.8.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS macOS용 제공 클라이언트 (3.7.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 8월 3일
AWS 윈도우용 제공 클라이언트 (3.8.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS 윈도우용 제공 클라이언트 (3.7.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS 우분투용 제공 클라이언트 (3.7.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS macOS용 제공 클라이언트 (3.6.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS 우분투용 제공 클라이언트 (3.6.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS macOS용 제공 클라이언트 (3.5.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 15일
AWS 윈도우용 제공 클라이언트 (3.6.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS 우분투용 제공 클라이언트 (3.5.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS macOS용 제공 클라이언트 (3.4.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 7월 14일
AWS macOS용 제공 클라이언트 (3.3.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 4월 27일

AWS 윈도우용 제공 클라이언트 (3.5.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 4월 3일
AWS 윈도우용 제공 클라이언트 (3.4.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 3월 28일
AWS 윈도우용 클라이언트 제공 (3.3.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 3월 17일
AWS 우분투용 클라이언트 제공 (3.4.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 2월 14일
AWS macOS용 제공 클라이언트 (3.2.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 1월 23일
AWS 윈도우용 제공 클라이언트 (3.2.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2023년 1월 23일
AWS macOS용 제공 클라이언트 (3.1.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일
AWS 윈도우용 제공 클라이언트 (3.1.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일
AWS 우분투용 제공 클라이언트 (3.1.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 5월 23일
AWS macOS용 제공 클라이언트 (3.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS 윈도우용 제공 클라이언트 (3.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS 우분투용 제공 클라이언트 (3.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 3월 3일
AWS macOS용 제공 클라이언트 (2.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일

AWS 윈도우용 클라이언트 제공 (2.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일
AWS 우분투용 클라이언트 제공 (2.0.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2022년 1월 20일
AWS macOS용 제공 클라이언트 (1.4.0) 출시	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 9일
AWS 윈도우용 제공 클라이언트 (1.3.7) 출시	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 8일
AWS 우분투용 제공 클라이언트 (1.0.3) 출시	세부 정보는 릴리스 정보를 참조하세요.	2021년 11월 8일
AWS 우분투용 제공 클라이언트 (1.0.2) 출시	세부 정보는 릴리스 정보를 참조하세요.	2021년 9월 28일
AWS 윈도우 (1.3.6) 및 macOS (1.3.5) 용 클라이언트 제공	세부 정보는 릴리스 정보를 참조하세요.	2021년 9월 20일
AWS 우분투 18.04 및 우분투 20.04용 클라이언트 제공 LTS LTS	AWS-제공 클라이언트는 우분투 18.04와 우분투 20.04에서 사용할 수 있습니다. LTS LTS	2021년 6월 11일
Windows 인증서 시스템 저장소의 인증서를 VPN 사용한 Open 지원	Windows 인증서 시스템 저장소의 인증서와 VPN 함께 Open을 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 클라이언트 VPN 엔드포인트에 연결할 수 있습니다.	2020년 2월 4일

최초 릴리스	이번 릴리스에는 AWS 클라이언트가 VPN 도입되었습니다.	2018년 12월 18일

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