Secure Access Support Team의 문제 해결 및 기본 정보 수집

목차

소개

이 문서에서는 Cisco Secure Access Support Team과 작업하는 동안 수집해야 하는 기본 정보에 대해 설명합니다

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- Cisco 보안 클라이언트
- Wireshark 및 tcpdump를 통한 패킷 캡처

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Secure Access를 작업하는 동안 Cisco 지원 팀에 문의해야 하거나 문제에 대한 기본 조사를

수행하고 로그를 검토하여 문제를 삭제하려는 문제가 발생할 수 있습니다. 이 문서에서는 보안 액세스와 관련된 기본 문제 해결 로그를 수집하는 방법에 대해 설명합니다. 모든 단계가 모든 시나리오에 적용되는 것은 아닙니다.

Secure Access 조직 ID 찾기

Cisco 엔지니어가 계정을 찾으려면 Secure Access Dashboard(보안 액세스 대시보드)에 로그인한 후 URL에서 찾을 수 있는 조직 ID를 제공합니다.

조직 ID를 찾는 단계:

1. sse.cisco.com에 로그인합니다
2. 여러 조직이 있는 경우 오른쪽 조직으로 전환합니다.
3. 조직 ID는 https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview의 URL에서 찾을 수 있습니다.

Cisco Secure Client Diagnostic and Reporting Tool(DART)

Cisco Secure Client Diagnostic and Reporting Tool(DART)은 Secure Client 패키지와 함께 설치되는 툴로서 사용자 엔드포인트에 대한 중요한 정보를 수집하는 데 도움이 됩니다.

DART 번들에 의해 수집된 정보의 예:

- ZTNA 로그
- 보안 클라이언트 로그 및 프로필 정보
- 시스템 정보
- 다른 Secure Client 추가 기능 또는 플러그인 로그에 설치

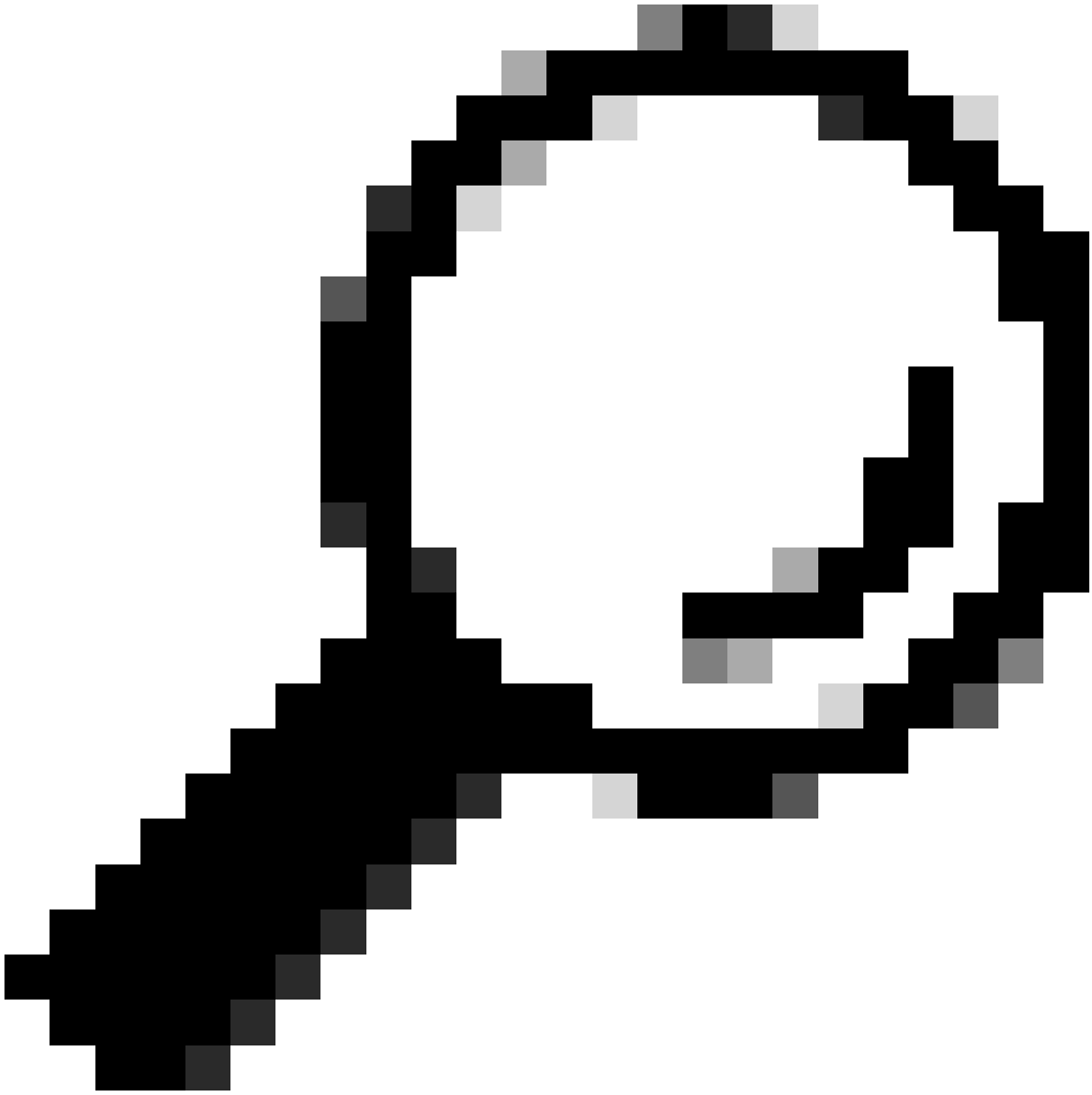
DART 수집 지침:

1단계. DART를 시작합니다.

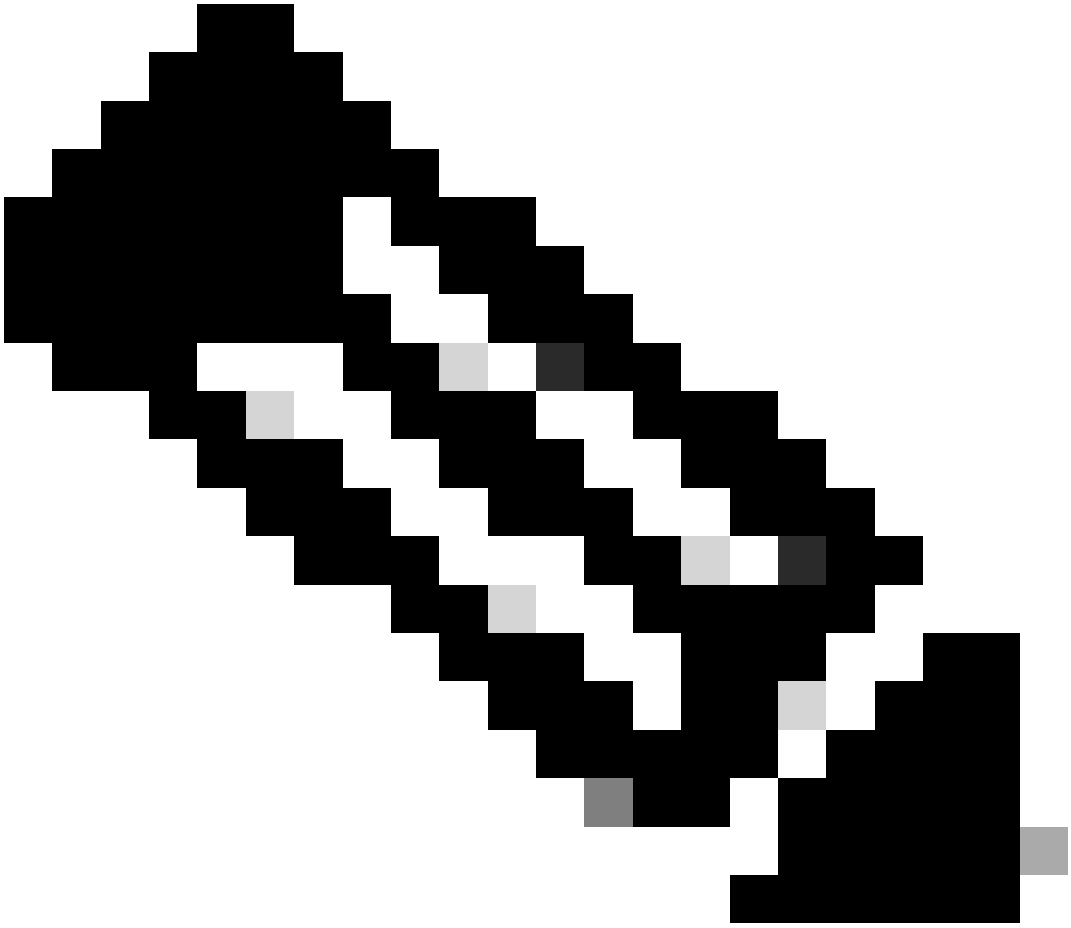
1. Windows 컴퓨터의 경우 Cisco Secure Client를 실행합니다.
2. Linux 컴퓨터의 경우 /opt/cisco/ **Applications** > **Internet** > **Cisco DART**anyconnect/dart/dartui를 선택합니다.
3. Mac 컴퓨터의 경우 를 선택합니다Applications > Cisco > Cisco DART.

2단계. Statistics(통계) 탭을 클릭한 다음 Details(세부사항)를 클릭합니다.

3단계. Default(기본값) 또는 Custom bundle creation(사용자 지정 번들 생성)을 선택합니다.



팁: 번들의 기본 이름은 DARTBundle.zip이며 로컬 데스크톱에 저장됩니다.



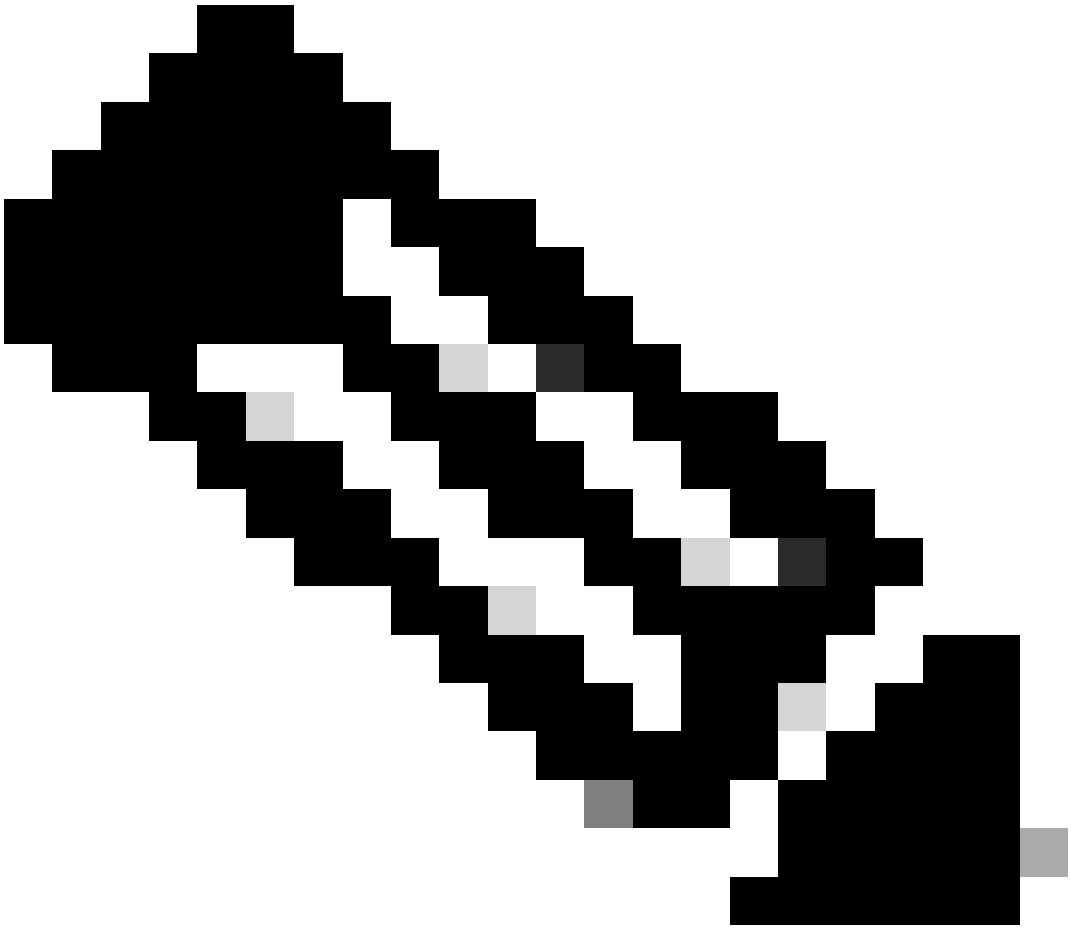
참고: Default(기본값)를 선택하면 DART가 번들 생성을 시작합니다. Custom(사용자 지정)을 선택한 경우 마법사 프롬프트를 계속 진행하여 로그, 환경 설정 파일, 진단 정보 및 기타 사용자 지정을 지정합니다

HTTP 아카이브(HAR) 캡처

HAR은 서로 다른 브라우저에서 수집할 수 있으며 다음과 같은 여러 정보를 제공합니다.

1. HTTPS 요청의 암호 해독된 버전
2. 오류 메시지, 요청 내용 및 헤더에 대한 내부 정보
3. 시기와 지연에 관한 정보
4. 그 밖에 브라우저 기반 요청에 관한 기타 정보

HAR 캡처를 수집하려면 이 소스에서 설명한 단계를 사용하십시오. https://toolbox.googleapps.com/apps/har_analyzer/



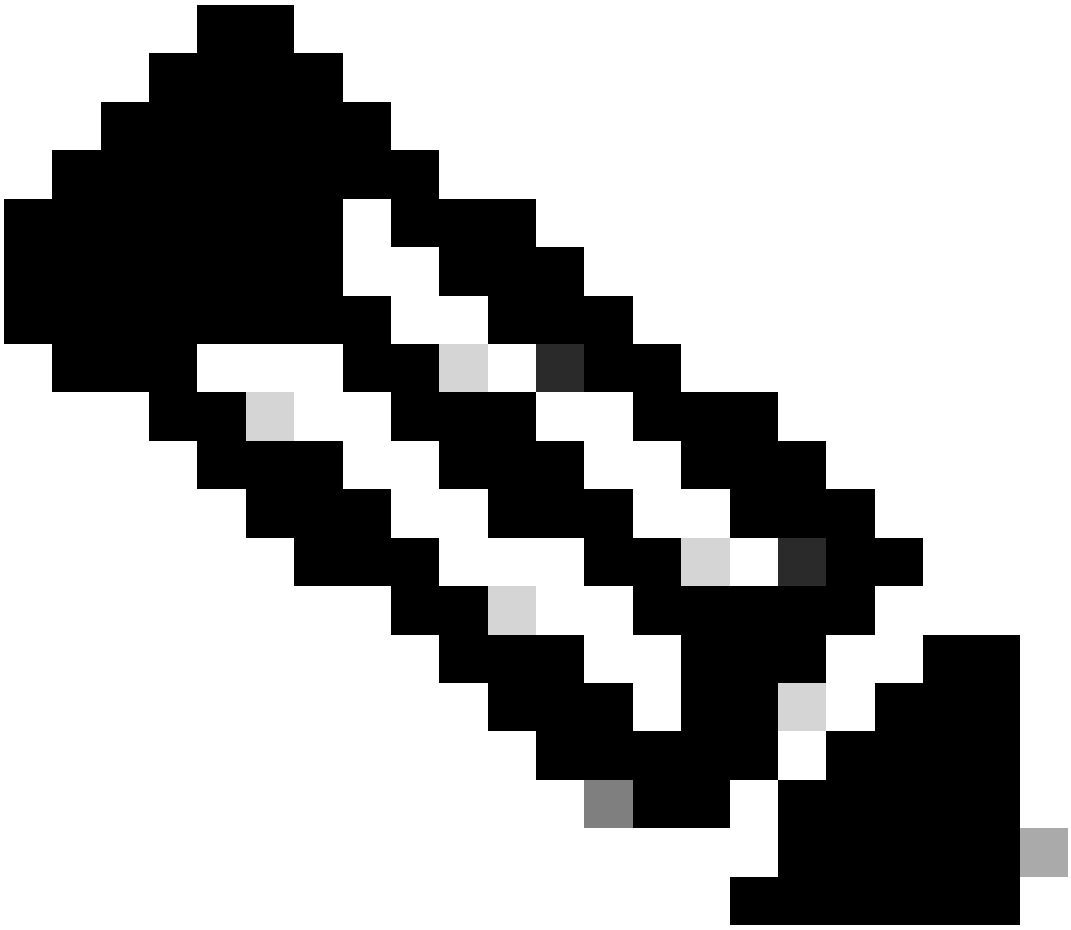
참고: 올바른 데이터를 수집하려면 브라우저 세션을 새로 고쳐야 합니다

패킷 캡처

패킷 캡처는 성능 문제 또는 패킷 손실이 감지되거나 네트워크에 대한 총 가동 중단이 발생한 시나리오에서 유용합니다. 캡처를 수집하는 가장 일반적인 툴은 wireshark 및 **tcpdump**입니다. 또는 Cisco 방화벽 또는 라우터와 같이 디바이스 자체 내에서 pcap 파일 형식을 수집하는 내장형 기능입니다.

엔드포인트에서 유용한 패킷 캡처를 수집하려면 다음을 포함해야 합니다.

1. Secure Client 애드온을 통해 전송된 트래픽을 캡처하기 위한 루프백 인터페이스.
2. 패킷 경로와 관련된 다른 모든 인터페이스.
3. 최소 필터를 적용하거나, 모든 데이터가 수집되었는지 확인하기 위해 필터를 전혀 적용하지 않습니다.



참고: 네트워크 디바이스에서 캡처가 수집될 때 트래픽의 소스와 대상을 필터링하고 캡처를 관련 포트 및 서비스로만 제한하여 이 활동으로 인한 성능을 방지해야 합니다.

정책 디버그 출력

정책 디버그 출력은 Secure Access에 의해 보호될 때 사용자 브라우저를 통해 전송되는 진단 출력입니다. 여기에는 배포에 대한 중요 정보가 포함됩니다.

1. 조직 ID
2. 구축 유형
3. 연결된 프록시
4. 공용 및 사설 IP 주소
5. 그 밖에 교통의 발생원과 관련된 정보

정책 테스트 결과를 실행하려면 보호된 엔드포인트에서 이 링크에 로그인하십시오. https://policy.test.sse.cisco.com/

브라우저에 인증서 오류 메시지가 표시되면 보안 액세스 루트 인증서를 신뢰해야 합니다.

보안 액세스 루트 인증서를 다운로드하려면

Secure Access(보안 액세스)로 이동 Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Cisco 지원 서비스 요청에 결과 업로드

다음 단계를 통해 지원 케이스에 파일을 업로드할 수 있습니다.

1단계. SCM에 로그인합니다.

2단계. 케이스를 보고 편집하려면 목록에서 케이스 번호 또는 케이스 제목을 클릭합니다. Case Summary(케이스 요약) 페이지가 열립니다.

3단계. 파일을 선택하고 케이스에 첨부 파일로 업로드하려면 Add Files(파일 추가)를 클릭합니다. 시스템에 SCM 파일 업로더 도구가 표시됩니다.

4단계. 업로드할 파일 선택 대화 상자에서 업로드할 파일을 끌거나 내부를 클릭하여 업로드할 파일을 로컬 시스템에서 찾습니다.

5단계. 설명을 추가하고 모든 파일 또는 개별적으로 범주를 지정합니다.

관련 정보

- **Cisco 기술 지원 및 다운로드**
- **Secure Access 설명서 및 사용 설명서**
- **Cisco Secure Client Software 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.