상태 확인 실패 또는 상태가 너무 오래됨(&Quot;) ZTNA 플로우에 대한 활동 검색 오류

목차

문제

제로 트러스트 네트워크 액세스 포스처 검사를 시행하면 정책 컨피그레이션에 따라 두 가지 방법으로 문제가 발생합니다.

- fail-open 규칙이 있는 경우: 트래픽은 포스처 시행을 건너뛰고 "No Posture Checks(포스처 확인 없음)" 규칙을 확인합니다.
- 엄격한 적용이 활성화된 경우: 사용자는 프라이빗 애플리케이션에 대한 액세스가 거부됩니다.

환경

- Cisco Secure Access — 제로 트러스트 네트워크 액세스 플로우
- 듀오 데스크톱

해결

Duo Desktop 진단 수집: 디버그 로깅 활성화 및 지원 도구 실행

1단계 - 디버그 로깅 사용(macOS 및 Windows)

1. Duo Desktop 앱을 엽니다.

2. 환경설정으로 이동합니다.

3. 상세 진단 보고서 사용을 선택합니다.

2단계 - 문제 재현

—

3단계 — Dart 번들 수집 - Secure Client용 DART 번들 수집

4단계 — 지원 툴 실행

지원 툴 스크립트는 macOS 및 Windows용 Duo Desktop 6.0.0 이상 및 Duo Device Health 2.26.1 이상과 함께 제공됩니다.

필요한 파일을 수집하고 중요한 정보를 검사하며 즉시 전송할 수 있는 ZIP을 생성합니다.

스크립트 위치

창

- Duo 데스크탑: `C:\Program 파일(x86)\Duo Desktop\DuoDesktop-Support.ps1`

- 듀오 디바이스 상태: `C:\Program 파일(x86)\Duo 장치 상태\DeviceHealth-Support.ps1`

맥OS

- Duo 데스크탑: `/Applications/Duo Desktop.app/Contents/Resources/duo_desktop_support.sh`

- 듀오 디바이스 상태: `/Applications/Duo 디바이스 상태 .app/Contents/Resources/device_health_support.sh`

참고: 이전 Duo Device Health 릴리스와 최신 Duo Desktop 릴리스 간 경로는 다릅니다.

Support Tool에서 수집하는 정보

창

1. 수집된 정보를 저장할 ZIP을 생성합니다.

2. Invoke-WebRequest를 실행하여 듀오에 대한 연결을 테스트합니다.

3. 포획 시스템 프록시 설정; OS 버전, 빌드 및 비트; BitLocker 상태; 표준 시간대; 듀오 관련 애플리케이션 이벤트 로그

4. 사본...(또는...\DuoDeviceHealth\Logs)를 ZIP에 저장합니다.

5. Duo 레지스트리 키를 HKLM:\SOFTWARE\Duo 및 HKCU\SOFTWARE\Duo Device Health에서 system_info.txt로 내보냅니다.

6. 루프백 어댑터 127.0.0.1)와 관련된 인증서를 복사합니다.

7 . (선택 사항) 시스템 이벤트 로그를 내보냅니다.

8. 로그인된 사용자의 바탕 화면에 ZIP을 저장합니다(예: C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip(또는 DHA_Support_...).zip).

MacOS

1. 수집된 정보를 저장할 ZIP을 생성합니다.

2. curl을 실행하여 듀오와의 연결을 테스트합니다.

3. 포획 시스템 프록시 설정; install.log; system.log; Duo 관련 충돌 로그 OS 및 커널 버전.

4. /Users/user_name/Library/Logs/Duo Desktop/*.log(또는 Duo Device Health)를 ZIP으로 복사합니다.

5. 루프백 어댑터 127.0.0.1)와 관련된 인증서를 복사합니다.

6. (선택 사항) 모든 사용자 및 커널 로그를 내보냅니다.

7. 로그인된 사용자의 바탕 화면에 ZIP을 저장합니다(예: /Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip(또는 DHA_Support_...).zip).

명령줄 옵션

Windows(PowerShell)

옵션 | 설명

| `-이벤트 로그` | 시스템 로그를 내보냅니다. 옵션: `시스템` |

| `일` | 내보낼 보안 이벤트 로그 기간(일) |

| `사용자` | 어떤 사용자가 로그를 수집할지 지정합니다(다른 사용자 이름으로 admin으로 실행할 때 필요함) |

| `도움말 보기` | 기본 제공 cmdlet; 스크립트 앞에 호출합니다(예: `Get-Help .\DuoDesktop-Support.ps1)`. |

macOS(터미널)

`-a` | 모든 사용자 및 커널 패닉 로그를 내보냅니다.

`-h` | 도움말 메시지를 표시합니다.

—

엔드 투 엔드 절차

Windows(예: 지난 2일간의 시스템 이벤트 로그 내보내기)

1. Duo Desktop이 설치된 엔드포인트에서 관리 PowerShell 세션을 엽니다.

2. 디버그 로깅을 활성화합니다(1부).

3. 듀오 문제를 재현합니다.

4. 스크립트를 실행합니다.

- Duo 데스크탑:

"PowerShell

& 'C:\Program 파일(x86)\Duo Desktop\DuoDesktop-Support.ps1' -eventlogs system -days 2

"

- 듀오 디바이스 상태:

"PowerShell

& 'C:\Program Files (x86)\Duo Device Health\DeviceHealth-Support.ps1' -eventlogs system -days 2

"

> "이 시스템에서 스크립트 실행이 비활성화되어 있습니다."가 표시되면 스크립트를 실행할 수 있도록 PowerShell 실행 정책을 조정한 다음 명령을 다시 실행합니다.

MacOS(예: 모든 사용자 및 커널 패닉 로그 내보내기)

1. Duo Desktop이 설치된 엔드포인트에서 터미널 세션을 엽니다.

2. 디버그 로깅을 활성화합니다(1부).

3. 듀오 문제를 재현합니다.

4. 스크립트를 실행합니다.

- Duo 데스크탑:

"배쉬"

/Applications/Duo\ Desktop.app/Contents/Resources/duo_desktop_support.sh -a

"

- 듀오 디바이스 상태:

"배쉬"

/Applications/Duo\ Device\ Health.app/Contents/Resources/device_health_support.sh -a

"

—

Cisco TAC에 전송 -

데스크톱의 Dart 및 Duo_Desktop_Support 폴더 1개를 Cisco TAC로 보냅니다.

실패한 시도의 2개 기간

3 Posture Checks는 Posture Profile에서 시행됩니다.

원인

하나 이상의 상태 검사(OS 버전, AV 상태, 디스크 암호화, 도메인 가입, 방화벽 상태)가 제로 트러스트 네트워크 액세스 정책에 정의된 임계값을 충족하지 않았습니다.

관련 콘텐츠

- Duo Desktop 디버그 로깅 구성
- Duo 데스크탑 지원 도구
- Cisco 기술 지원 및 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.