문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.

Secure Firewall ASA 디바이스 문제 해결

재부팅 후 ASA가 CDO에 다시 연결하지 못함

ASA를 재부팅한 후 CDO와 ASA가 연결되지 않으면 ASA가 CDO의 SDC(보안 디바이스 커넥터)에서 지원하지 않는 OpenSSL 암호 그룹을 사용하도록 대체되었기 때문일 수 있습니다. 이 문제 해결 항목은 해당 사례를 테스트하고 문제 해결 단계를 제공합니다.

증상

- ASA가 재부팅되고 CDO와 ASA가 다시 연결되지 않습니다. CDO는 "다시 연결하지 못했습니다."라는 메시지를 표시합니다.
- ASA 온보딩을 시도할 때 CDO는 다음 메시지를 표시합니다. <*ASA_IP_Address*>에 대한 인증서를 검색할 수 없습니다.

인증서 오류로 인해 ASA를 온보딩할 수 없음

환경: ASA가 클라이언트 측 인증서 인증으로 구성되었습니다.

해결책 : 클라이언트 측 인증서 인증을 비활성화합니다.

세부 정보: ASA는 자격 증명 기반 인증 및 클라이언트 측 인증서 인증을 지원합니다. CDO는 클라이언트 측 인증서 인증을 사용하는 ASA에 연결할 수 없습니다. ASA를 CDO에 온보딩하기 전에 다음 절차를 사용하여 클라이언트 인증서 인증이 활성화되어 있지 않은지 확인합니다.

단계 **1** 터미널 창을 열고 SSH를 사용하여 ASA에 연결합니다.

단계 **2** 전역 구성 모드를 시작합니다.

단계 **3** hostname (config)# 프롬프트에서 다음 명령을 입력합니다.

no ssl certificate-authentication interface*interface-name***port 443**

인터페이스 이름은 CDO가 연결하는 인터페이스의 이름입니다.

ASA에서 사용하는 OpenSSL 암호 그룹 확인

이 절차를 사용하여 ASA에서 사용 중인 OpenSSL 암호화 제품군을 식별합니다. 명령 출력에 명명된 암호 제품군이 CDO의 보안 디바이스 커넥터가 지원하는 Cipher Suites에 없는 경우 SDC에서 해당 암호 그룹을 지원하지 않으므로 ASA에서 암호 그룹을 업데이트해야 합니다.

단계 **1** SDC에 연결할 수 있는 컴퓨터에서 콘솔 창을 엽니다.

단계 **2** SSH를 사용하여 SDC에 연결합니다. CDO 또는 SDC와 같은 일반 사용자 또는 생성한 다른 사용자로 로그인할 수 있습니다. 루트로 로그인할 필요가 없습니다.

Tip SDC IP 주소를 찾으려면 다음을 수행합니다.

a. CDO를 엽니다.

b. 사용자 메뉴에서 Secure Connector(보안 커넥터)를 선택합니다.

c. 표에 표시된 SDC를 클릭합니다. SDC의 IP 주소는 디바이스의 세부 정보 창에 표시됩니다.

단계 **3** 명령 프롬프트에 다음을 입력합니다. **openssl s_client -showcerts -connect***ASA_IP_Address***:443**

단계 **4** 명령 출력에서 다음 행을 찾으십시오.

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

이 예에서 ASA에서 사용 중인 암호화 제품군은 `DES-CB3-SHA`입니다.

CDO의 보안 디바이스 커넥터가 지원하는 Cipher Suites

CDO의 보안 디바이스 커넥터는 가장 안전한 최신 암호만 허용하는 node.js를 사용합니다. 결과적으로 CDO의 SDC는 다음 암호 목록만 지원합니다.

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA에서 사용하는 암호 제품군이 이 목록에 없는 경우, SDC에서 지원하지 않으므로 ASA의 암호 그룹 업데이트.

ASA의 암호 그룹 업데이트

ASA에서 **TLS** 암호 그룹을 업데이트하려면 다음을 수행합니다**.**

단계 **1** SSH를 사용하여 ASA에 연결합니다.

단계 **2** ASA에 연결되면 권한을 전역 구성 모드로 승격합니다. 프롬프트는 다음과 같이 표시됩니다. asaname(config)#

단계 **3** 프롬프트에서 다음과 유사한 명령을 입력합니다.

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA256"
```

Note 이 명령이 지원하도록 ASA를 구성하는 암호 그룹은 따옴표 사이에 그리고 custom이라는 단어 뒤에 포함됩니다. 이 명령에서 지정된 암호 그룹은 `ECDHE-RSA-AES128-GCM-SHA256`으로 시작하여 `DHE-RSA-AES256-SHA256`으로 끝납니다. ASA에서 명령을 입력할 때 ASA에서 지원하지 않는 모든 암호 그룹을 제거합니다.

단계 **4** 명령을 제출한 후 프롬프트에서 write memory를 입력하여 로컬 구성을 저장합니다. 예: `asaname(config)#` **`write memory`**

CLI 명령을 사용하여 ASA 문제 해결

이 섹션에서는 ASA 문제를 해결하고 기본 연결을 테스트하는 데 사용할 수 있는 몇 가지 중요한 명령에 대해 설명합니다. 다른 문제 해결 시나리오 및 CLI 명령에 대해 알아보려면 CLI 책 1: Cisco ASA

Series 일반 작업 CLI 구성 가이드를 참조하십시오. '시스템 관리' 섹션에서 '테스트 및 문제 해결' 장으로 이동합니다.

각 ASA 디바이스에서 사용할 수 있는 CDO CLI 인터페이스를 사용하여 이러한 명령을 실행할 수 있습니다. CDO에서 CLI 인터페이스를 사용하는 방법에 대해 알아보려면 CDO 명령줄 인터페이스 사용을 참조하십시오.

NAT 정책 설정

NAT 설정을 결정하는 몇 가지 중요한 명령은 다음과 같습니다.

- NAT 정책 통계를 확인하려면 **show nat**를 사용합니다.
- 할당된 주소와 포트를 포함한 NAT 풀과 할당된 횟수를 확인하려면 **show nat pool**을 사용합니다.

NAT와 관련된 추가 명령은 CLI 책 2: Cisco ASA Series Firewall CLI 구성 가이드를 참조하고 'NAT(Network Address Translation)' 장으로 이동하십시오.

기본 연결 테스트: 주소 **ping**하기

ASA CLI 인터페이스에서 **ping <IP address>** 명령을 사용하여 ASA 디바이스를 ping할 수 있습니다. 기존

라우팅 테이블 표시

라우팅 테이블의 항목을 보려면 **show route** 명령을 사용합니다.

ciscoasa# show route

ASA의 라우팅 테이블에 대한 출력 예:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
마지막 수단의 게이트웨이는 네트워크 0.0.0.0에 대한 192.168.0.254입니다.
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, 관리
C 10.0.0.0 255.0.0.0 직접 연결, 외부
L 10.10.10.1 255.255.255.255 직접 연결, 외부
C 192.168.0.0 255.255.255.0 직접 연결, 관리
L 192.168.0.118 255.255.255.255 직접 연결, 관리
```

스위치 포트 모니터링

- **show interface**

  인터페이스 통계를 표시합니다.

- **show interface ip brief**

  인터페이스 IP 주소와 상태를 표시합니다.

- **show arp**

동적, 정적 및 프록시 ARP 항목을 표시합니다. 동적 ARP 항목에는 ARP 항목의 기간(초)가 포함됩니다.

ARP 항목의 출력 예:

```
관리 10.10.32.129 0050.568a.977b 0
관리 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

ASA 원격 액세스 VPN 문제 해결

이 섹션에서는 ASA 디바이스에서 원격 액세스 VPN을 구성할 때 발생할 수 있는 몇 가지 문제 해결 문제에 대해 설명합니다.

RA VPN 모니터링 페이지에서 누락된 정보

이 문제는 Webvpn에 대해 외부 인터페이스가 활성화되지 않은 경우 발생할 수 있습니다.

해결 방법:

1. 탐색 창에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
2. **Devices(**디바이스**)** 탭을 클릭한 다음 **ASA** 탭을 클릭합니다.
3. 문제가 있는 RA VPN 헤드엔드 ASA 디바이스를 선택합니다.
4. 오른쪽의 관리 창에서 **Configuration(**구성**)**를 클릭합니다.
5. **Edit(**편집**)**를 클릭하고 'webvpn'을 검색합니다.
6. **Enter(**엔터**)**를 누르고 `enable` *interface_name*를 추가합니다. 여기서 interface_name은 원격 액세스 VPN 연결을 만들 때 사용자가 연결하는 외부 인터페이스의 이름입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

   예를 들면 다음과 같습니다.

   ```
   webvpn
   ```

```
enable outside
```

7. **Save(**저장**)**를 클릭합니다.
8. 디바이스에 구성을 미리 보고 배포합니다.

기존 RA VPN 구성에 ASA를 추가할 수 없음

•

시작하기 전에

•

SUMMARY STEPS

1.

DETAILED STEPS

	명령 또는 동작	목적
단계 **1**	예제:	

예

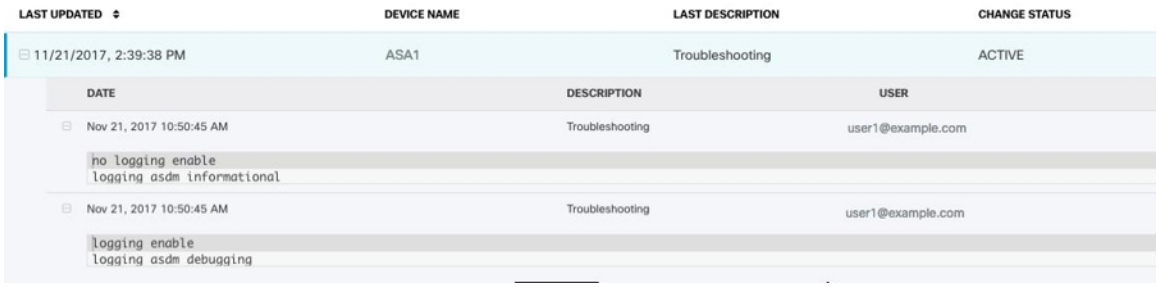
다음에 수행할 작업

•

ASA 실시간 로깅

실시간 로깅을 사용하여 로깅된 데이터의 마지막 20초 또는 로깅된 데이터의 마지막 10KB 중 먼저 도달하는 한계에 도달하는 데이터를 표시합니다. CDO는 실시간 데이터를 검색할 때, ASDM의 기존 로깅 구성을 검토하고, 디버깅 수준 데이터를 요청하도록 변경한 다음, 로깅 구성을 구성으로 반환합니다. 로깅 CDO 디스플레이에는 ASDM에서 설정했을 수 있는 모든 로깅 필터가 반영됩니다.

변경 로그를 검토하면 CDO가 로깅을 수행하기 위해 보내는 명령을 볼 수 있습니다. 다음은 변경 로그 항목의 예입니다. 첫 번째 항목(하단)은 CDO가 로깅 활성화 명령으로 로깅을 "켜고" ASDM 로깅 수준을 디버깅으로 변경했음을 나타냅니다. 두 번째 항목(상단)은 로깅 구성이 이전 상태로 돌아갔음을 보여줍니다. no logging enable 명령으로 로깅이 "꺼지고" ASDM 로깅 수준이 정보로 돌아갔습니다.



ASA 실시간 로그 보기

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 실시간 데이터를 보려는 디바이스를 선택합니다.

단계 **3** **Troubleshoot(**문제 해결**)** Troubleshoot 를 클릭합니다.

단계 **4** (선택 사항) 실시간 로그 보기를 클릭하기 전에 왼쪽 창에서 필터를 정의하여 로그 검색 결과를 구체화할 수 있습니다.

단계 **5** **View Real-time Log(**실시간 로그 보기**)**를 클릭합니다. CDO는 필터링 기준에 따라 실시간 로그 데이터를 검색하여 표시합니다.

단계 **6** 기록된 데이터의 추가 20초 또는 기록된 데이터의 마지막 10KB를 보려면. **View Real-Time Log(**실시간 로그 보기**)**를 다시 클릭합니다.

AT 패킷 트레이서

패킷 트레이서를 사용하면 합성 패킷을 네트워크로 보내고 기존 라우팅 구성, NAT 규칙 및 정책 구성이 해당 패킷에 미치는 영향을 평가할 수 있습니다. 이 도구를 사용하여 다음과 같은 종류의 문제를 해결합니다.

- 사용자가 연결 가능해야 하는 리소스에 연결할 수 없다고 보고합니다.
- 사용자가 연결할 수 없어야 하는 리소스에 연결할 수 있다고 보고합니다.
- 정책을 테스트하여 예상대로 작동하는지 확인합니다.

패킷 트레이서는 실제 또는 가상의 라이브 온라인 ASA 디바이스에서 사용할 수 있습니다. 패킷 트레이서는 ASA 모델 디바이스에서 작동하지 않습니다. 패킷 트레이서는 ASA에 저장된 구성을 기반으로 패킷을 평가합니다. CDO의 준비된 변경 사항은 패킷 트레이서에 의해 평가되지 않습니다.

동기화된 ASA에서 패킷 트레이서를 실행하는 것이 모범 사례라고 생각합니다. 디바이스가 동기화되지 않은 경우 패킷 트레이서가 실행되지만 예기치 않은 결과가 발생할 수 있습니다. 예를 들어 CDO의 준비된 구성에서 규칙을 삭제하고 패킷 추적 중에 ASA에서 동일한 규칙이 트리거된 경우 CDO는 해당 규칙과 패킷의 상호 작용 결과를 표시할 수 없습니다.

ASA 패킷 트레이서 관련 문제 해결

패킷 트레이서는 ASA의 라우팅 구성, NAT 규칙 및 보안 정책을 통해 패킷을 보낼 때 각 단계에서 패킷의 상태를 표시합니다. 정책에서 패킷을 허용하면 녹색 확인 표시가 나타납니다. 패킷이 거부되고 삭제되면 CDO는 빨간색 X를 표시합니다.

패킷 트레이서는 패킷 추적 결과의 실시간 로그도 표시합니다. 아래 예에서 규칙이 tcp 패킷을 거부한 위치를 확인할 수 있습니다.

ASA 디바이스 보안 정책 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **Troubleshoot(**문제 해결**)** Troubleshoot 를 클릭합니다.

단계 **2** Values(값) 창에서 ASA를 통해 가상으로 전송할 인터페이스 및 패킷 유형을 선택합니다.

단계 **3** (선택 사항) Layer 2 CMD 헤더(Trustsec)에 보안 그룹 태그 값이 내장된 패킷을 추적하려면 SGT 번호를 확인하고 보안 그룹 태그 번호 0-65535를 입력합니다.

단계 **4** 소스와 대상을 지정합니다. Cisco Trustsec을 사용하는 경우, IPv4 또는 IPv6 주소, 정규화된 도메인 이름(FQDN) 또는 보안 그룹 이름 또는 태그를 지정할 수 있습니다. 소스 주소의 경우, 또한 형식 Domain\username에 사용자 이름을 지정할 수 있습니다.

단계 **5** 기타 프로토콜 특성 지정:

- ICMP - ICMP 유형, ICMP 코드(0-255) 및 선택사항인 ICMP ID를 입력합니다.
- TCP/UDP/SCTP- 목록에서 선택하거나 포트 콤보 상자에 값을 입력하여 소스 및 대상 포트를 입력합니다.
- IP - 0-255 사이의 프로토콜 번호를 입력합니다.

단계 **6** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **7** 패킷 트레이서 결과 분석를 계속합니다.

액세스 규칙 문제 해결

단계 **1** **Policies(**정책**)** > **Network Policies(**네트워크 정책**)** > 를 선택합니다**.**

단계 **2** ASA와 연결된 정책을 선택합니다.

단계 **3** 네트워크 정책에서 문제를 해결할 규칙을 선택하고 세부 정보 창에서 Troubleshoot 문제 해결를 클릭합니다. 문제 해결 페이지의 값 패널에서 많은 필드가 선택한 규칙의 속성으로 미리 채워져 있습니다.

단계 **4** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **5** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **6** 패킷 트레이서 결과 분석를 계속합니다.

NAT 규칙 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **View NAT Rules(NAT** 규칙 보기**)** View NAT Rules를 클릭합니다.

단계 **2** 문제를 해결할 NAT 규칙 테이블에서 규칙을 선택하고 세부 정보 창에서 문제 해결 Troubleshoot 를 클릭합니다. 문제 해결 페이지의 값 패널에서 많은 필드가 선택한 규칙의 속성으로 미리 채워져 있습니다.

단계 **3** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **4** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

단계 **5** 패킷 트레이서 결과 분석를 계속합니다.

2회 NAT 규칙 문제 해결

단계 **1** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 ASA를 선택하고 Actions 창에서 **View NAT Rules(NAT** 규칙 보기**)** View NAT Rules를 클릭합니다.

단계 **2** 문제를 해결할 NAT 규칙 테이블에서 규칙을 선택하고 세부 정보 창에서 문제 해결 Troubleshoot 를 클릭합니다. 양방향 Twice NAT 규칙의 경우 원본 패킷 변환 또는 대상 패킷 변환의 문제 해결을 선택하는 드롭다운이 열립니다.

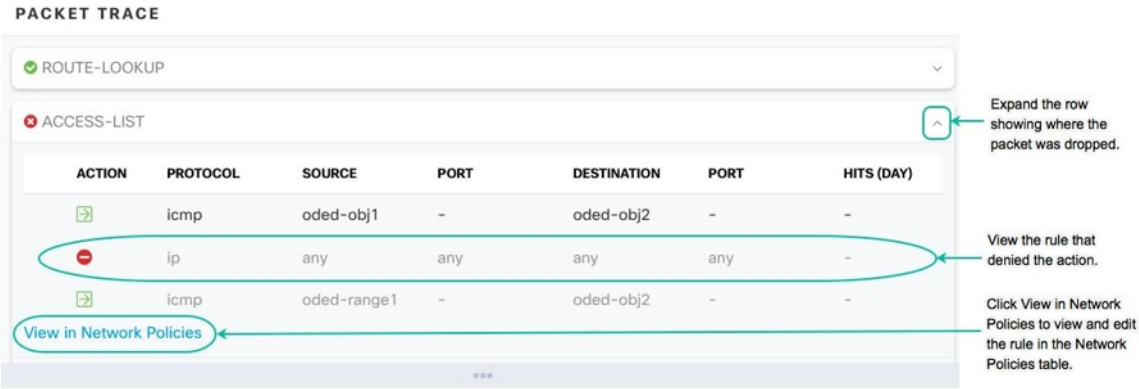
단계 **3** 나머지 필수 필드에 정보를 입력합니다. 모든 필수 필드를 완료하면 Run Packet Tracer(패킷 트레이서 실행)가 활성화됩니다.

단계 **4** **Run Packet Tracer(**패킷 추적기 실행**)**를 클릭합니다.

패킷 트레이서 결과 분석

패킷이 삭제되었는지 또는 허용되었는지 여부는 패킷 추적 테이블의 행을 확장하고 해당 작업과 관련된 규칙 또는 로깅 정보를 읽어 그 이유를 알 수 있습니다. 아래 예에서 패킷 트레이서는 모든 소스에서 수신되고 모든 대상으로 이동하는 IP 패킷을 거부하는 규칙이 포함된 액세스 목록 정책을 식별했습니다. 원하는 작업이 아닌 경우 **View in Network Policies(**네트워크 정책에서 보기**)** 링크를 클릭하고 해당 규칙을 즉시 편집할 수 있습니다. 규칙을 편집한 후에는 구성 변경 사항을 ASA에 배포한 다음 패킷 트레이서를 다시 실행하여 예상한 액세스 결과를 얻습니다.

패킷 트레이서 결과와 함께 CDO는 ASA의 ASA 실시간 로깅를 표시합니다.



Cisco ASA Advisory cisco-sa-20180129-asa1

Cisco PSIRT(Product Security Incident Response Team)은 심각한 심각도의 ASA 및 Firepower 보안 취약점을 설명하는 cisco-sa-20180129-asa1 보안권고를 게시했습니다. 영향을 받는 ASA 및 Firepower 하드웨어, 소프트웨어 및 구성에 대한 자세한 설명은 전체 PSIRT 팀 권고를 읽어보십시오.

ASA가 권고의 영향을 받는다고 판단되면, CDO를 사용하여 ASA를 패치 버전으로 업그레이드할 수 있습니다. 다음 프로세스를 사용합니다.

단계 **1** 영향을 받는 각 ASA에서 DNS 서버를 구성합니다.

단계 **2** 필요한 소프트웨어 패치를 결정하려면 권고로 돌아갑니다.

단계 **3** CDO를 사용하여 ASA를 ASA 권고에 나열된 편집된 릴리스로 업그레이드하는 방법을 설명하는 항목에 대해서는 단일 ASA에서 ASA 및 ASDM 이미지 업그레이드을 참조하십시오. 업그레이드 사전 요구 사항부터 시작한 다음 개별 ASA 업그레이드, 활성-대기 구성에서 ASA 업그레이드 또는 대량 ASA 업그레이드에 대해 읽어보십시오.

편의를 위해 Cisco가 보고한 보안 권고의 요약은 다음과 같습니다.

2018/5/2 업데이트: 추가 조사 후 Cisco는 이 취약점의 영향을 받는 추가 공격 벡터와 기능을 확인했습니다. 또한 원래의 편집이 불완전함을 발견하여 새로운 편집 코드 버전을 사용할 수 있습니다. 자세한 내용은 Fixed Software(수정 소프트웨어) 섹션을 참조하십시오. Cisco ASA(Adaptive Security Appliance) 소프트웨어의 XML 파서에 있는 취약점으로 인해 인증되지 않은 원격 공격자가 영향을 받는 시스템을 다시 로드하거나 코드를 원격으로 실행할 수 있습니다. 메모리 부족 상태로 인해 ASA에서 수신되는 VPN(가상 프라이빗망) 인증 요청 처리를 중지할 수도 있었습니다. 이 취약점은 악성 XML 페이로드를 처리할 때 메모리 할당 및 해제 문제로 인해 발생합니다. 공격자는 조작된 XML 패킷을 영향을 받는 시스템의 취약한 인터페이스로 전송하여 이 취약점을 악용할 수 있습니다. 익스플로잇을 통해 공격자는 임의 코드를 실행하고 시스템을 완전히 제어할 수 있으며, 영향을 받는 디바이스를 다시 로드하거나 들어오는 VPN 인증 요청 처리를 중지할 수 있습니다. 취약하려면 ASA에 SSL(Secure Socket Layer) 서비스 또는 IKEv2 원격 액세스 VPN 서비스가 인터페이스에서 활성화되어 있어야 합니다. 취약점이 악용될 위험은 공격자에 대한 인터페이스의 액세스 가능성에 따라 달라집니다. 취약한 ASA 기능의 전체 목록은 취약한 제품 섹션의 표를 참조하십시오. Cisco는 이 취약점을 해결하는 소프트웨어 업데이트를 출시했습니다. 이 취약점의 영향을 받는 모든 기능을 해결하는 해결 방법은 없습니다. 이 권고는 다음 링크에서 확인할 수 있습니다: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

ASA 실행 구성 크기 확인

실행 중인 구성 파일의 크기를 확인하려면 다음 절차를 수행합니다.

단계 **1** 다음 방법 중 하나로 ASA의 명령줄 인터페이스에 액세스합니다.

- 터미널 창을 열고 SSH를 사용하여 ASA에 로그인합니다. `hostname#`이 포함된 프롬프트가 표시되도록 권한을 "특권 EXEC" 모드로 승격합니다.
- ASA를 온보딩한 경우 **Inventory(**재고 목록**)** 페이지를 열고 연결할 디바이스를 선택한 다음 Device Actions(디바이스 작업) 창에서 **>_ Command Line Interface(**명령줄 인터페이스**)** 버튼을 클릭합니다.

단계 **2** 프롬프트에서 `copy running-config flash`를 입력합니다.

단계 **3** 소스 파일 이름을 묻는 프롬프트가 표시되면 아무 것도 입력하지 않고 <Enter> 키를 누릅니다.

단계 **4** 대상 파일 이름을 입력하라는 메시지가 표시되면 출력 파일의 이름을 입력합니다. ASA는 사용자가 지정한 파일의 실행 중인 구성을 복사한 후 권한 있는 EXEC 프롬프트로 돌아갑니다.

단계 **5** 프롬프트에서 `show flash`를 입력합니다.

단계 **6** 길이 열을 확인합니다. 파일이 4718592바이트를 넘으면 4.5MB보다 큽니다.

다음은 샘플 명령 및 출력 집합입니다.

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 cisco-sa-20190215-runc를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.

CDO-표준 SDC 호스트 업데이트

CDO 이미지를 사용하여 SDC를 배포한 경우 이 지침을 사용합니다.

단계 **1** SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 **2** 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 **3** 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

단계 **4** 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고 Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

단계 **5** docker version 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

단계 **6** 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전(Docker 보안 업데이트 및 컨테이너 보안 모범 사례)을 결정할 수 있습니다.

버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

CSCvo33929-CVE-2019-5736: runc container breakout

대규모 **ASA** 실행 구성 파일

CDO의 동작

ASA가 온보딩에 실패하거나, CDO가 ASA의 실행 중인 구성 파일에 정의된 모든 구성을 표시하지 않거나, CDO가 변경 로그에 쓰지 못하는 등의 동작을 볼 수 있습니다.

가능한 원인

ASA의 실행 중인 구성 파일이 CDO에 대해 "너무 클" 수 있습니다.

ASA를 CDO에 온보딩하면 CDO는 ASA에서 실행 중인 구성 파일의 복사본을 데이터베이스에 저장합니다. 일반적으로 실행 중인 구성 파일이 너무 크거나(4.5MB 이상), 너무 많은 행(약 22,000행)을 포함하거나, 단일 액세스 그룹에 대한 액세스 목록 항목이 너무 많은 경우, CDO는 해당 디바이스를 예측 가능하게 관리할 수 없습니다.

실행 중인 구성 파일의 크기를 확인하려면 ASA 실행 구성 크기 확인을 참조하십시오.

해결방법

보안 정책을 방해하지 않고 구성 파일의 크기를 안전하게 줄이는 데 도움이 필요하면 Cisco 어카운트 팀에 문의하십시오.

보안 디바이스 커넥터 문제 해결

다음 주제를 사용하여 온프레미스 SDC(Secure Device Connector) 문제를 해결합니다.

이러한 시나리오와 일치하지 않는 경우 Cisco 기술 지원 센터에서 케이스를 엽니다.

SDC에 연결할 수 없음

CDO에서 연속으로 두 개의 하트비트 요청에 응답하지 못한 경우 SDC는 "도달할 수 없음" 상태입니다. SDC에 연결할 수 없는 경우 테넌트는 온보딩한 디바이스와 통신할 수 없습니다.

CDO는 다음과 같은 방식으로 SDC에 연결할 수 없음을 나타냅니다.

- "일부 보안 디바이스 커넥터(SDC)에 연결할 수 없습니다."라는 메시지가 표시됩니다. CDO 홈페이지에서 이러한 SDC와 연결된 디바이스와 통신할 수 없습니다.
- Secure Connectors(보안 커넥터) 페이지에서 SDC의 상태는 "연결할 수 없음"입니다.

먼저 이 문제를 해결하려면 SDC를 테넌트에 다시 연결해 봅니다.

1. SDC 가상 머신이 실행 중이고 해당 지역의 CDO IP 주소에 도달할 수 있는지 확인합니다. 매니지드 디바이스에 Cisco Defense Orchestrator 연결을 참조하십시오.
2. 하트비트를 수동으로 요청하여 CDO와 SDC를 다시 연결해 봅니다. SDC가 하트비트 요청에 응답하면 "활성" 상태로 돌아갑니다. 하트비트를 수동으로 요청하려면 다음과 같이 작업합니다.
   1. CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.
   2. 연결할 수 없는 SDC를 클릭합니다.
   3. 작업 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.
   4. **Reconnect(다시 연결)**를 클릭합니다.
3. 테넌트에 수동으로 다시 연결하려고 시도한 후에도 SDC가 활성 상태로 돌아가지 않으면, 배포 후 SDC 상태가 CDO에서 활성화되지 않음, 14 페이지의 지침을 따르십시오.

.

배포 후 SDC 상태가 CDO에서 활성화되지 않음

CDO가 배포 후 약 10분 동안 SDC가 활성 상태임을 나타내지 않으면 SDC를 배포할 때 생성한 `cdo` 사용자 및 암호를 사용하여 SSH를 사용하여 SDC VM에 연결합니다.

단계 **1** `/opt/cdo/configure.log`를 검토합니다. SDC에 대해 입력한 구성 설정과 성공적으로 적용되었는지 여부를 보여줍니다. 설정 프로세스에 오류가 있거나 값이 올바르게 입력되지 않은 경우 sdc-onboard 설정을 다시 실행합니다.

a) `[cdo@localhost cdo]$` 프롬프트에서 `sudo sdc-onboard setup`을 입력합니다.
b) `cdo`user의 암호를 입력합니다.
c) 프롬프트에 따라 수행합니다. 설정 스크립트는 설정 마법사에서 수행한 모든 구성 단계를 안내하고 입력한 값을 변경할 수 있는 기회를 제공합니다.

단계 **2** 로그를 검토하고 `sudo sdc-onboard setup`을 실행한 후에도 CDO가 여전히 SDC가 **Active(활성)** 상태임을 나타내지 않으면, CDO 지원에 문의하십시오.

SDC의 변경된 IP 주소가 CDO에 반영되지 않음

SDC의 IP 주소를 변경한 경우 GMT 오전 3시 이후까지는 CDO에 반영되지 않습니다.

SDC와의 디바이스 연결 문제 해결

이 도구를 사용하여 CDO에서 SDC(보안 디바이스 커넥터)를 통해 디바이스로의 연결을 테스트합니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

단계 **1** CDO 메뉴에서 **Admin(관리)** > **Secure Connector(보안 커넥터)**를 선택합니다.

단계 **2** SDC를 선택합니다.

단계 **3** 오른쪽의 **Troubleshooting(문제 해결)** 창에서 **Device Connectivity(디바이스 연결)**를 클릭합니다.

단계 **4** 문제 해결을 시도하거나 연결을 시도하는 디바이스의 유효한 IP 주소 또는 FQDN 및 포트 번호를 입력하고 **Go(이동)**를 클릭합니다. CDO는 다음 확인을 수행합니다.

a) **DNS** 확인 - IP 주소 대신 FQDN을 제공하는 경우 SDC가 도메인 이름을 확인하고 IP 주소를 가져올 수 있는지 확인합니다.

b) 연결 테스트 - 디바이스에 연결할 수 있는지 확인합니다.

c) **TLS** 지원 - 디바이스와 SDC가 모두 지원하는 TLS 버전 및 암호를 탐지합니다.

- 지원되지 않는 암호 - 디바이스와 SDC에서 모두 지원하는 TLS 버전이 없는 경우 CDO는 디바이스에서 지원하는 TLS 버전 및 암호도 테스트하지만 SDC는 테스트하지 않습니다.

d) SSL 인증서 - 문제 해결에서 인증서 정보를 제공합니다.

단계 **5** 디바이스에 대한 온보딩 또는 연결 문제가 계속 발생하는 경우 Defense Orchestrator 지원에 문의하십시오.

간헐적으로 또는 SDC에 연결되지 않음

이 섹션에서 설명하는 솔루션은 온프레미스 SDC(보안 디바이스 커넥터)에만 적용됩니다.

증상: 간헐적으로 또는 SDC에 연결되지 않음

진단: 이 문제는 디스크 공간이 거의 찼을 때(80% 이상) 발생할 수 있습니다.

디스크 공간 사용량을 확인하려면 다음 단계를 수행합니다.

1. SDC(보안 디바이스 커넥터) VM용 콘솔을 엽니다.
2. 사용자 이름 **cdo**로 로그인합니다.
3. 최초 로그인 시 생성한 비밀번호를 입력합니다.
4. 먼저 **`df -h`**를 입력하여 사용 가능한 디스크 공간이 없는지 확인하여 디스크 여유 공간을 확인합니다.

   Docker에서 디스크 공간을 소비한 것을 확인할 수 있습니다. 정상적인 디스크 사용량은 2GB 미만일 것으로 예상됩니다.
5. **Docker** 폴더의 디스크 사용량을 보려면,

   `sudo du -h /var/lib/docker | sort -h`를 실행합니다.

   Docker 폴더의 디스크 공간 사용량을 볼 수 있습니다.

절차

Docker 폴더의 디스크 공간 사용량이 거의 가득 찬 경우 docker 구성 파일에서 다음을 정의합니다.

- 최대 크기: 현재 파일이 최대 크기에 도달하면 로그 회전을 강제합니다.
- 최대 파일: 최대 한도에 도달했을 때 초과 회전된 로그 파일을 삭제합니다.

다음을 수행하십시오.

1. **sudo vi /etc/docker/daemon.json**를 실행합니다.
2. 파일에 다음 줄을 삽입합니다.

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. **ESC** 키를 누른 다음 **:wq!**를 입력합니다. 변경 사항을 쓰고 파일을 닫습니다.

참고 **sudo cat /etc/docker/daemon.json**을 실행하여 파일의 변경 사항을 확인할 수 있습니다.

4. **sudo systemctl restart docker**를 실행하여 doker 파일을 다시 시작합니다.

   변경 사항이 적용되려면 몇 분 정도 걸립니다. **sudo du -h /var/lib/docker | sort -h**를 실행하여 docker 폴더의 업데이트된 디스크 사용량을 봅니다.
5. **df -h**를 실행하여 사용 가능한 디스크 크기가 증가했는지 확인합니다.
6. SDC 상태를 Unreachable(연결 불가)에서 Active(활성)로 변경하려면 먼저 CDO에서 Secure Connector(보안 커넥터) 페이지로 이동하여 Actions(작업) 메뉴에서 **Request Reconnect(**재연결 요청**)**를 클릭해야 합니다.

보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.
  - CDO-표준 SDC 호스트 업데이트, 12 페이지
  - 사용자 지정 SDC 호스트 업데이트, 12 페이지

• 버그 추적, 13 페이지

CDO-표준 SDC 호스트 업데이트

CDO 이미지를 사용하여 SDC를 배포한 경우 이 지침을 사용합니다.

단계 **1** SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 **2** 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 **3** 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

단계 **4** 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고 Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

단계 **5** docker version 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

단계 **6** 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전(Docker 보안 업데이트 및 컨테이너 보안 모범 사례)을 결정할 수 있습니다.

버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

CSCvo33929-CVE-2019-5736: runc container breakout

보안 이벤트 커넥터 문제 해결

이러한 시나리오와 일치하지 않는 경우 Cisco 기술 지원 센터에서 케이스를 엽니다.

SEC 온보딩 실패 문제 해결

이러한 문제 해결 항목에서는 SEC(보안 이벤트 커넥터) 온보딩 실패와 관련된 여러 가지 증상에 대해 설명합니다.

SEC 온보딩 실패

증상: SEC 온보딩에 실패했습니다.

복구: SEC를 제거하고 다시 온보딩합니다.

이 오류가 표시되는 경우:

1. 가상 머신 컨테이너에서 Secure Event Connector 및 해당 파일을 제거합니다.
2. 보안 디바이스 커넥터 업데이트. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없지만 이 절차는 문제 해결 시 유용합니다.
3. SDC 가상 머신에 SEC(Secure Event Connector) 설치.

팁 SEC를 온보딩할 때는 항상 복사 링크를 사용하여 부트스트랩 데이터를 복사합니다.

참고 이 절차로 문제가 해결되지 않으면 문제 해결 로그 파일 이벤트 로깅하고 관리 서비스 제공자 또는 Cisco 기술 지원 센터에 문의하십시오.

SEC 부트스트랩 데이터가 제공되지 않음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 데이터가 제공되지 않아 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

진단: 프롬프트가 표시될 때 부스트랩 데이터가 설정 스크립트에 입력되지 않았습니다.

복구: 온보딩 시 부트스트랩 데이터 입력에 대한 프롬프트가 표시되면 CDO UI에서 생성된 SEC 부트스트랩 데이터를 제공합니다.

부트스트랩 구성 파일이 없습니다.

메시지: 오류가 발생하여 테넌트 <tenant_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 구성 파일("/usr/local/cdo/es_bootstrapdata")이 없어 종료하는 중입니다.

진단: SEC 부트스트랩 데이터 파일("/usr/local/cdo/es_bootstrapdata")이 없습니다.

복구: CDO UI에서 생성된 SEC 부트스트랩 데이터를 **/usr/local/cdo/es_bootstrapdata** 파일에 배치하고 다시 온보딩을 시도합니다.

1. 온보딩 절차를 반복합니다.
2. 부트스트랩 날짜를 복사합니다.
3. 'sdc' 사용자로 SEC VM에 로그인합니다.
4. CDO UI에서 생성된 SEC 부트스트랩 데이터를 **/usr/local/cdo/es_bootstrapdata** 파일에 배치하고 다시 온보딩을 시도합니다.

부트스트랩 데이터 디코딩 실패

메시지: 오류가 발생하여 테넌트 <tenant_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. SEC 부스트랩 데이터를 디코딩하지 못하여 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

진단: 부트스트랩 데이터 디코딩 실패

복구: SEC 부트스트랩 데이터를 재생성하고 온보딩을 다시 시도합니다.

부트스트랩 데이터에 **SEC**를 온보딩하는 데 필요한 정보가 없습니다.

메시지:

- ERROR는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 FQDN이 설정되지 않았습니다. 종료됩니다.
- ERROR는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 OTP가 설정되지 않았습니다. 종료됩니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.

[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.
```

진단: 부트스트랩 데이터에 SEC를 온보딩하는 데 필요한 정보가 없습니다.

복구: 부트스트랩 데이터를 재생성하고 다시 온보딩을 시도합니다.

툴킷 **cron** 현재 실행 중

메시지: 오류 SEC 툴킷이 이미 실행 중이어서 종료하는 중입니니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

진단: 툴킷 cron이 현재 실행 중입니다.

복구: 온보딩 명령을 다시 시도합니다.

적절한 **CPU** 및 메모리를 사용할 수 없음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 최소 4개의 CPU와 8GB의 RAM이 필요하여 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

진단: 적절한 CPU 및 메모리를 사용할 수 없습니다.

복구: 최소 4개의 CPU 및 8GB RAM이 VM에서 SEC 전용으로 프로비저닝되었는지 확인하고 다시 온보딩을 시도합니다.

SEC가 이미 실행 중

메시지: 오류. 보안 이벤트 커넥터가 이미 실행 중입니다. 새 보안 이벤트 커넥터를 온보딩하기 전에 'cleanup'을 실행하십시오. 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

진단: SEC가 이미 실행 중입니다.

복구: 새 SEC를 온보딩하기 전에 SEC Cleanup 명령을 실행합니다.

SEC 도메인 연결 불가

메시지:

- api-sse.cisco.com:443에 연결 실패; 연결 거부됨
- 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 도메인 api-sse.cisco.com에 연결할 수 없어 종료하는 중입니다.

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

진단: SEC 도메인에 연결할 수 없음

복구: 온프레미스 SDC가 인터넷에 연결되어 있는지 확인하고 다시 온보딩을 시도합니다.

온보딩 **SEC** 명령이 오류 없이 성공했지만 **SEC** 도커 컨테이너가 작동하지 않음

증상: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

진단: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

복구**:**

1. 'sdc' 사용자로 SEC에 로그인합니다.
2. SEC 도커 컨테이너 시작 로그(/usr/local/cdo/data/<tenantDir> /event_streamer/logs/startup.log)에 오류가 있는지 확인합니다.
3. 있는 경우 SEC Cleanup 명령을 실행하고 온보딩을 다시 시도합니다.

CDO 지원 문의

이러한 시나리오와 일치하지 않는 경우 Cisco 기술 지원 센터에서 케이스를 엽니다.

보안 이벤트 커넥터 등록 실패 문제 해결

증상: 클라우드 이벤트 서비스에 대한 Cisco Secure Event Connector 등록이 실패합니다.

진단: SEC가 이벤트 클라우드 서비스에 등록하지 못하는 가장 일반적인 이유입니다.

- **SEC**가 **SEC**에서 **Eventing** 클라우드 서비스에 연결할 수 없습니다**.**

  복구: 포트 443에서 인터넷에 액세스할 수 있고 DNS가 올바르게 구성되어 있는지 확인합니다.

- **SEC** 부트스트랩 데이터의 유효하지 않거나 만료된 일회용 비밀번호로 인한 등록 실패

  복구:

단계 **1** 'sdc' 사용자로 SDC에 로그온합니다.

단계 **2** 커넥터 로그 보기: (/usr/local/cdo/data/<tenantDir> /event_streamer/logs/connector.log)에서 등록 상태를 확인합니다.

유효하지 않은 토큰으로 인해 등록에 실패한 경우 로그 파일에 아래와 유사한 오류 메시지가 표시됩니다.

컨텍스트**:(*contextImpl).handleFailed]** 등록 **- CE2001:** 등록 실패 - 잘못된 토큰으로 인해 디바이스를 등록하지 못했습니다**.** 유효한 새 토큰을 사용하여 다시 시도하십시오**. -** 실패"

단계 **3** SDC VM에서 SEC Cleanup 명령 단계를 실행하여 보안 커넥터 페이지에서 SEC를 제거합니다.

단계 **4** 새 SEC 부트스트랩 데이터를 생성하고 SEC 온보딩 단계를 다시 시도합니다.

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

Note 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다.

단계 **3** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **4** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **5** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **6** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **7** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **8** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

NSEL 데이터 플로우 문제 해결

NSEL(Netflow Secure Event Logging) 구성 및 을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.

Note 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드의 "패킷 캡처" 및 Cisco ASA NetFlow 구현 가이드의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

문제 해결 로그 파일 이벤트 로깅

SEC(Secure Event Connector) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다.

다음 절차를 사용하여 Comparesed.tar.gz 파일을 생성하고 파일의 압축을 풉니다.

1. 문제 해결 스크립트 실행, 23 페이지.
2. sec_troubleshoot.tar.gz 파일 압축 해제, 24 페이지.

문제 해결 스크립트 실행

SEC(보안 이벤트 커넥터) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다. Troubleshooting.sh 스크립트를 실행하려면 다음 절차를 따르십시오.

단계 **1** VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.

단계 **2** 로그인한 다음 **root** 사용자로 전환합니다.

```
[cdo@localhost ~]$sudo su root
```

Note sdc 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

단계 **3** 프롬프트에서 문제 해결 스크립트를 실행하고 테넌트 이름을 지정합니다. 다음은 명령 구문입니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

명령 출력에서 sec_troubleshoot 파일이 SDC의 **/tmp/troubleshoot** 디렉터리에 저장되어 있음을 확인할 수 있습니다. 파일 이름은 sec**_troubleshoot-** ***timestamp*****.tar.gz** 규칙을 따르십시오.

단계 **4** 파일을 검색하려면 CDO 사용자로 로그인하고 SCP 또는 SFTP를 사용하여 파일을 다운로드합니다.

예를 들면 다음과 같습니다.

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

What to do next

sec_troubleshoot.tar.gz 파일 압축 해제, on page 24를 진행합니다.

sec_troubleshoot.tar.gz 파일 압축 해제

SEC(Secure Event Connector) 문제 해결 스크립트 실행 스크립트는 모든 이벤트 스트리머 로그를 수집하여 단일 sec_troubleshoot.tar.gz 파일로 압축합니다. 다음 절차에 따라 sec_troubleshoot.tar.gz 파일의 압축을 풉니다.

1. VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.
2. 로그인한 다음 **root** 사용자로 전환합니다.

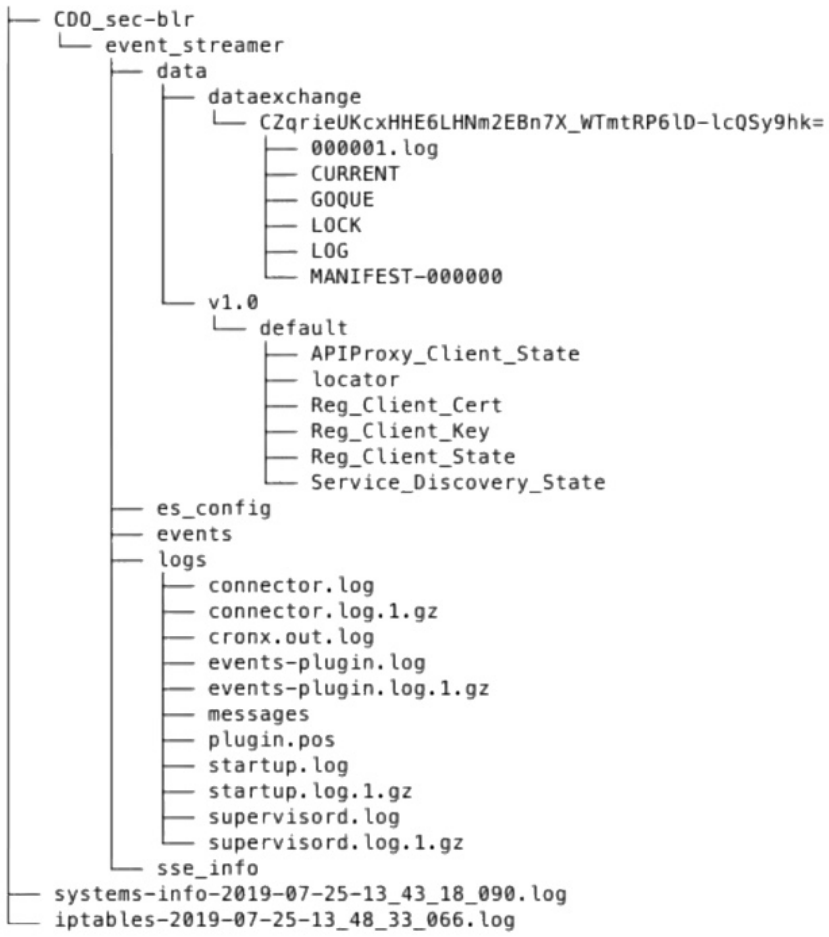
```
[cdo@localhost ~]$sudo su root
```

Note **sdc** 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

3. 프롬프트에서 다음 명령을 입력합니다.

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

로그 파일은 테넌트의 이름을 따서 명명된 디렉터리에 저장됩니다. 이러한 로그는 sec_troubelshoot-timestamp.tar.gz 파일에 저장됩니다. 루트 사용자로 모든 로그 파일을 수집한 경우 iptables 파일이 포함됩니다.



SEC 부트스트랩 데이터를 생성하지 못했습니다.

증상: CDO에서 SEC 부트스트랩 데이터를 생성하는 동안, "부트스트랩 생성" 단계가 "부트스트랩 데이터를 가져오는 중에 오류가 발생했습니다." 오류와 함께 실패합니다. 다시 시도하십시오."

수리: 부트스트랩 데이터 생성을 다시 시도하십시오. 여전히 실패하면 CDO 지원에 문의하십시오.

온보딩 후 CDO 보안 커넥터 페이지에서 SEC 상태가 "비활성"임

Symptom(증상): 보안 이벤트 커넥터 상태가 다음 이유 중 하나로 CDO 보안 커넥터 페이지에서 "비활성"으로 표시됩니다.

- 하트비트 실패
- 커넥터 등록 실패

복구:

- **Heartbeat failed(**하트비트 실패**):** SEC 하트비트를 요청하고 보안 커넥터 페이지를 새로 고쳐 상태가 "활성"으로 변경되는지 확인하고 그렇지 않으면 보안 디바이스 커넥터 등록이 실패했는지 확인합니다.
- **Connector registration failed(**커넥터 등록 실패**):** 보안 이벤트 커넥터 등록 실패 문제 해결을 참조하십시오.

SEC가 "온라인"이지만 CDO 이벤트 로깅 페이지에 이벤트가 없습니다

Symptom(증상**)**: CDO 보안 커넥터 페이지에 보안 이벤트 커넥터가 "활성"으로 표시되지만 CDO 이벤트 뷰어에는 이벤트가 표시되지 않습니다.

Solution or workaround(해결 방법**)**:

단계 **1** 온프레미스 SDC의 VM에 'sdc' 사용자로 로그인합니다. 프롬프트에서 **sudo su - sdc**를 입력합니다.

단계 **2** 다음 확인을 수행합니다.

- SEC 커넥터 로그(/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log)를 확인하고 SEC 등록이 성공했는지 확인합니다. 그렇지 않은 경우 "보안 이벤트 커넥터 등록 실패 문제 해결" 문제를 참조하십시오.
- SEC 이벤트 로그(/usr/local/cdo/data/<tenantDir>/event_streamer/logs/events-plugin.log)를 확인하고 이벤트가 처리되고 있는지 확인합니다. 그렇지 않은 경우 CDO 지원에 문의하십시오.
- SEC 도커 컨테이너에 로그인하고 "supervisorctl -c /opt/cssp/data/conf/supervisord.conf " 명령을 실행하고 출력이 아래와 같고 모든 프로세스가 RUNNING 상태인지 확인합니다. 그렇지 않은 경우 CDO 지원에 문의하십시오.

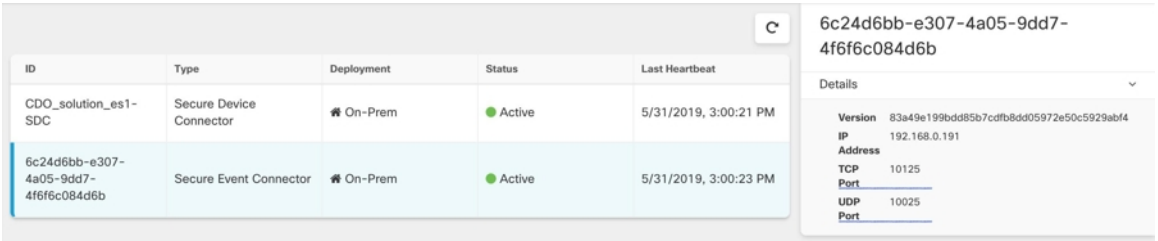
estreamer-connector RUNNING pid 36, 업타임 **5:25:17**

estreamer-cron RUNNING pid 39, 업타임 **5:25:17**

estreamer-plugin RUNNING pid 37, 업타임 **5:25:17**

estreamer-rsyslog RUNNING pid 38, 업타임 **5:25:17**

- 온프레미스 SDC의 방화벽 규칙이 보안 커넥터 페이지에서 SEC에 대해 표시된 UDP 및 TCP 포트를 차단하지 않는지 확인합니다. 어떤 포트를 열어야 하는지 확인하려면 Cisco Security Analytics 및 Logging에 사용되는 장치의 TCP, UDP 및 NSEL 포트 찾기를 참조하십시오.



- 자체 CentOS 7 VM을 사용하여 SDC를 수동으로 설정하고 들어오는 요청을 차단하도록 방화벽을 구성한 경우, 다음 명령을 실행하여 UDP 및 TCP 포트의 차단을 해제할 수 있습니다.

firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent

firewall-cmd --reload

- 선택한 Linux 네트워크 도구를 사용하여 이 포트에서 패킷이 수신되고 있는지 확인합니다. 수신되지 않는 경우 FTD 로그 구성을 다시 확인합니다.

위의 수리 중 어느 것도 작동하지 않으면, CDO 지원에 지원 티켓을 제출하십시오..

SEC Cleanup 명령

SEC(보안 이벤트 커넥터) cleanup 명령은 SDC(보안 디바이스 커넥터) VM에서 SEC 컨테이너 및 관련 파일을 제거합니다. 보안 이벤트 커넥터 등록 실패 문제 해결, on page 21 또는 온보딩에 실패할 경우 이 명령을 실행할 수 있습니다.

명령을 실행하려면 다음을 수행합니다.

Before you begin

이 작업을 수행하려면 테넌트의 이름을 알아야 합니다. 테넌트 이름을 찾으려면 CDO에서 사용자 메뉴를 열고 **Settings(**설정**)**를 클릭합니다. 페이지를 아래로 스크롤하여 테넌트 이름을 찾습니다.

단계 **1** 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 **2** `/usr/local/cdo/toolkit` 디렉터리에 연결합니다.

단계 **3** `sec.sh remove`*`tenant_name`*을 실행하고 SEC를 제거할 의도를 확인합니다.

예:

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

What to do next

이 명령이 SEC를 제거하지 못한 경우 SEC Cleanup 명령 실패, on page 27를 계속하십시오.

SEC Cleanup 명령 실패

SEC Cleanup 명령, on page 27가 실패한 경우 이 절차를 사용합니다.

메시지: SEC를 찾을 수 없습니다. 종료합니다.

증상: Cleanup SEC 명령이 기존 SEC를 정리하지 못합니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

복구: 정리 명령이 실패할 때 보안 이벤트 커넥터를 수동으로 정리합니다.

이미 실행 중인 SEC 도커 컨테이너를 제거합니다.

단계 **1** 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 **2** **docker ps** 명령을 실행하여 SEC 컨테이너의 이름을 찾습니다. SEC 이름은 "es_ *name*" 형식입니다.

단계 **3** **docker stop** 명령을 실행하여 SEC 컨테이너를 중지합니다.

단계 **4** **rm** 명령을 실행하여 SEC 컨테이너를 제거합니다.

예를 들면 다음과 같습니다**.**

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습

SEC(보안 이벤트 커넥터) 상태 확인 스크립트는 SEC의 상태에 대한 정보를 제공합니다.

상태 확인을 실행하려면 다음 절차를 따르십시오.

단계 **1** VM 하이퍼바이저를 열고 SDC(보안 디바이스 커넥터)에 대한 콘솔 세션을 시작합니다.

단계 **2** "cdo" 사용자로 SDC에 로그인합니다.

단계 **3** "sdc" 사용자로 전환합니다.

```
[cdo@tenant]$sudo su sdc
```

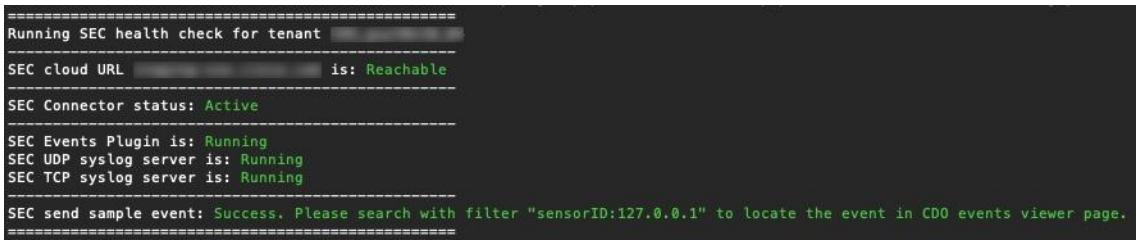
단계 **4** 프롬프트에서 healthcheck.sh 스크립트를 실행하고 테넌트 이름을 지정합니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

스크립트의 출력은 다음과 같은 종류의 정보를 제공합니다.



상태 확인 출력의 값:

- **SEC Cloud URL(SEC** 클라우드 **URL)**: CDO 클라우드 URL 및 SEC가 CDO에 연결할 수 있는지 여부를 표시합니다.
- **SEC** 커넥터: SEC 커넥터가 올바르게 온보딩되고 시작된 경우 "Running(실행 중)"으로 표시됩니다.

- **SEC UDP** 시스템 로그 서버: UDP Syslog 서버가 UDP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC TCP** 시스템 로그 서버: TCP Syslog 서버가 TCP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC** 커넥터 상태: SEC가 실행 중이고 CDO에 온보딩된 경우 Active(활성)로 표시됩니다.
- **SEC Send sample event(SEC** 샘플 이벤트 전송**)**: 상태 확인이 종료될 때 모든 상태 확인이 "녹색"인 경우 툴이 샘플 이벤트를 전송합니다. (프로세스 중 하나라도 "Down" 상태이면 테스트 이벤트 전송을 건너뜁니다.) 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

문제 해결 Cisco Defense Orchestrator

로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다. **CDO**타일을 클릭하여 defenceorchestrator.com에 액세스하거나 **CDO(EU)**를 클릭하여 defenceorchestrator.eu에 액세스합니다.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 계정을 생성하십시오.

- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

액세스 및 인증서 문제 해결

CDO를 사용하여 사용자 액세스 문제 해결

사용자가 액세스 권한이 있어야 하는 리소스에 대한 액세스가 거부되는 경우를 고려하십시오. 다음은 해당 문제를 진단하고 해결하기 위해 취할 수 있는 접근 방식입니다.

단계 **1** 사용자는 리소스에 대한 액세스가 차단되었음을 보안 팀에 알립니다. 일반적으로 리소스에 도달하는 방법을 결정합니다. IP 주소는 무엇입니까? 특정 포트에 도달합니까? 리소스에 정보를 보내는 데 사용되는 프로토콜은 무엇입니까?

단계 **2** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** **FTD** 탭을 클릭하고 ASA를 선택하고 패킷 트레이서를 실행합니다. 자세한 지침은 AT 패킷 트레이서를 참조하십시오.

단계 **4** 리소스에 대한 액세스를 거부했을 수 있는 규칙에 대한 패킷 추적 테이블을 검사합니다.

단계 **5** 액세스를 거부하는 규칙을 식별한 후 CDO에 변경 요청 레이블을 생성하고 활성화합니다. 변경 요청 관리을 참조하십시오. 이렇게 하면 리소스에 대한 액세스를 허용하기 위해 만든 변경 로그 정책 변경 사항을 식별하는 데 도움이 됩니다.

단계 **6** 동작을 편집하려면 CDO에서 규칙을 편집합니다. 이제 ASA가 CDO와 동기화되지 않습니다.

단계 **7** **Devices & Services(**디바이스 및 서비스**)** 페이지에서 변경 사항을 ASA에 배포합니다. CDO는 CDO에 스테이징된 구성이 아닌 ASA에 저장된 구성을 통해 패킷을 추적합니다. CDO에서 준비된 다른 구성 변경 사항도 ASA에 배포하게 됩니다.

단계 **8** 패킷 트레이서를 다시 실행하여 정책 변경이 원하는 결과를 제공하는지 확인합니다. 이제 사용자가 리소스에 액세스할 수 있는지 확인합니다.

단계 **9** 이제 사용자에게 액세스 권한이 있다고 가정하고 CDO에서 변경 요청 레이블을 지웁니다. 이렇게 하면 관련 없는 활동이 이 편집 프로그램과 연결되지 않습니다.

Note 변경해도 문제가 해결되지 않거나 새로운 문제가 발생하여 이전 구성으로 돌아가고 싶은 경우 ASA 구성을 복원할 수 있습니다. ASA 구성 복원을 참조하십시오.

새 지문 탐지 상태 확인

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 새 지문 감지됨 상태에서 디바이스를 선택합니다.

단계 **5** 새 지문 감지됨 창에서 지문 검토를 클릭합니다.

단계 **6** 지문을 검토하고 수락하라는 메시지가 표시되면

a. **Download Fingerprint(**지문 다운로드**)**를 클릭하고 검토합니다.

b. 지문에 만족하면 **Accept(**수락**)**를 클릭합니다. 그렇지 않은 경우 **Cancel(**취소**)**를 클릭합니다.

단계 **7** 새 지문 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. 구성 충돌 해결을 검토하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

Note 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

단계 **1** 탐색창에서 분석 > 이벤트 로깅를 선택합니다.

단계 **2** 기록 탭을 클릭합니다.

단계 **3** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **4** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **5** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **6** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **7** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.

- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **8** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 Firepower Threat Defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 예를 들어 사용자는 Facebook iOS 또는 Android 앱을 사용할 수 없지만 Safari 또는 Chrome을 https://www.facebook.com으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - `SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.`
  - `SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.`
  - `SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.`
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.

- SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
- SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 계정을 생성하십시오.
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

개체 문제 해결

중복 개체 문제 해결

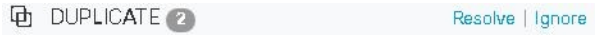
중복 개체 ⧉는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

중복 개체 문제를 해결하려면 다음을 수행합니다.

단계 **1** 왼쪽의 CDO 탐색 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 중복 개체 문제를 찾습니다.

단계 **3** 결과 중 하나를 선택합니다. 개체 세부 정보 패널에 영향을 받는 중복 수가 포함된 DUPLICATE 필드가 표시됩니다.



단계 **4** **Resolve(**해결**)**를 클릭합니다. CDO는 비교할 중복 개체를 표시합니다.

단계 **5** 비교할 두 개체를 선택합니다.

단계 **6** 이제 다음과 같은 옵션이 제공됩니다.

- 개체 중 하나를 다른 개체로 교체하려면 유지할 개체에 대해 **Pick(**선택**)**을 클릭하고 **Resolve(**확인**)**를 클릭하여 영향을 받을 디바이스 및 네트워크 정책을 확인한 다음, 변경 사항이 마음에 들면 **Confirm(**확인**)**를 클릭합니다. CDO는 선택한 개체를 교체로 유지하고 중복 항목을 삭제합니다.
- 목록에 무시할 개체가 있는 경우 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO에 표시되는 중복 개체 목록에서 제거됩니다.
- 개체는 유지하지만 CDO가 중복 개체를 검색할 때 찾지 않도록 하려면 **Ignore All(**모두 무시**)**를 클릭합니다.

단계 **7** 중복 개체 문제가 해결되면 지금 변경 사항을 검토하고 구축하거나, 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

사용되지 않는 개체 문제 해결

사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

관련 정보**:**

- 디바이스 및 서비스 목록 내보내기
- CDO에 디바이스 대량 다시 연결

사용되지 않은 개체 문제 해결

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 하나 이상의 사용되지 않는 개체를 선택합니다.

단계 **4** 이제 다음과 같은 옵션이 제공됩니다.

- Actions(작업) 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 사용되지 않는 개체를 제거합니다.
- Issues(문제) 창에서 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO는 사용되지 않은 개체의 결과에 해당 개체를 표시하지 않습니다.

단계 **5** 사용되지 않는 개체를 제거한 경우, 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축지금 변경한 사항을 수행하거나 대기하고 여러 변경 사항을 한 번에 구축합니다.

Note 사용되지 않는 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참조하십시오.

사용되지 않는 개체 대량 제거

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 삭제하려는 사용되지 않는 개체를 선택합니다.

- 개체 테이블 헤더 행의 확인란을 클릭하여 페이지의 모든 개체를 선택합니다.
- 개체 테이블에서 사용하지 않는 개별 개체를 선택합니다.

단계 **4** 오른쪽의 작업 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 선택한 사용되지 않는 개체를 모두 제거합니다. 한 번에 99개의 개체를 제거할 수 있습니다.

단계 **5** **OK(**확인**)**을 클릭하여 사용하지 않는 개체를 삭제할 것인지 확인합니다.

단계 **6** 이러한 변경 사항을 배포하기 위한 두 가지 선택 사항이 있습니다.

- 지금 변경한 내용을 검토 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.
- **Inventory(**인벤토리**)** 페이지를 열고 변경의 영향을 받은 디바이스를 찾습니다. 변경의 영향을 받는 모든 디바이스를 선택하고 관리 창에서 **Deploy All(**모두 배포**)** 를 클릭합니다. 경고를 읽고 적절한 조치를 취합니다.

불일치 개체 문제 해결

불일치 개체 INCONSISTENT 2 Resolve | Ignore 는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다.

참고: 일관되지 않은 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참고하십시오.

일치하지 않는 개체에 대해 다음을 수행할 수 있습니다.

- **Ignore(**무시**)**: CDO가 개체 간의 불일치를 무시하고 해당 값을 유지합니다. 개체가 더 이상 불일치 범주에 나열되지 않습니다.
- **Merge(**병합**)**: CDO가 선택한 모든 개체와 해당 값을 단일 개체 그룹으로 결합합니다.
- **Rename(**이름 바꾸기**)**: CDO를 사용하면 일치하지 않는 개체 중 하나의 이름을 바꾸고 새 이름을 지정할 수 있습니다.
- **Convert Shared Network Objects to Overrides(**공유 네트워크 개체를 오버라이드로 변환**)**: CDO를 사용하면 일관성이 없는 공유 개체(오버라이드가 있거나 없는)를 오버라이드가 있는 단일 공유 개체로 결합할 수 있습니다. 일치하지 않는 개체의 가장 일반적인 기본값은 새로 형성된 개체의 기본값으로 설정됩니다.

Note 공통 기본값이 여러 개인 경우 그 중 하나가 기본값으로 선택됩니다. 나머지 기본값 및 재정의 값은 해당 개체의 재정의로 설정됩니다.

- **Convert Shared Network Group to Additional Values(**공유 네트워크 그룹을 추가 값으로 변환**):** - CDO를 사용하면 일치하지 않는 공유 네트워크 그룹을 추가 값이 있는 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 이 기능의 기준은 변환할 일관되지 않은 네트워크 그룹에 동일한 값을 가진 공통 개체가 하나 이상 있어야 한다는 것입니다. 이 기준과 일치하는 모든 기본값은 기본값이 되며, 나머지 개체는 새로 형성된 네트워크 그룹의 추가 값으로 할당됩니다.

  예를 들어, 일치하지 않는 두 개의 공유 네트워크 그룹을 고려하십시오. 첫 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)로 구성됩니다. 여기에는 추가 값 'object_3'(192.0.2.a)도 포함됩니다. 두 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 추가 값 'object_4'(192.0.2.b)로 구성됩니다. 공유 네트워크 그룹을 추가 값으로 변환할 때 새로 형성된 그룹 'shared_network_group'에는 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)'가 포함되며, 'object_3'(192.0. 2.a) 및 'object_4'(192.0.2.b)를 추가 값으로 사용합니다.

Note 새 네트워크 개체를 생성하면 CDO는 자동으로 해당 값을 동일한 이름의 기존 공유 네트워크 개체에 오버라이드로 할당합니다. 이는 새 디바이스가 CDO에 온보딩된 경우에도 적용됩니다.

자동 할당은 다음 기준을 충족하는 경우에만 발생합니다.

1. 새 네트워크 개체를 디바이스에 할당해야 합니다.
2. 이름과 유형이 같은 공유 개체는 테넌트에 하나만 있어야 합니다.
3. 공유 개체에 이미 오버라이드가 포함되어 있어야 합니다.

일관성 없는 개체 문제를 해결하려면 다음을 수행합니다.

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 필터링하여 일관성 없는 개체 문제를 찾습니다.

단계 **3** 일치하지 않는 개체를 선택합니다. 개체 세부 정보 패널에 영향을 받는 개체의 수가 포함된 INCONSISTENT 필드가 표시됩니다.

단계 **4** **Resolve(**해결**)**를 클릭합니다. CDO는 비교할 일치하지 않는 개체를 표시합니다.

단계 **5** 이제 다음과 같은 옵션이 제공됩니다.

- 모두 무시**:**

a. 표시된 개체를 비교하고 개체 중 하나에서 **Ignore(**무시**)**를 클릭합니다. 또는 모든 개체를 무시하려면 **Ignore All(**모두 무시**)**을 클릭합니다.

b. **OK(**확인**)**를 클릭하여 확인합니다.

- 개체를 병합하여 해결합니다**.**

a. **Resolve by Merging X Objects(X**개 개체를 병합하여 해결**)**를 클릭합니다.

b. **OK(**확인**)**를 클릭합니다.

- **Rename(**이름 바꾸기**):**

a. **Rename(**이름 변경**)**을 클릭합니다.

b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.

- **Convert to Overrides(**오버라이드로 변환**)(**일치하지 않는 공유 개체의 경우**)**: 공유 개체를 오버라이드와 비교할 때, 비교 패널의 **Inconsistent Values(**일관되지 않는 값**)** 필드에 기본값만 표시됩니다.

a. **Convert to Overrides(**재정의로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 오버라이드가 포함된 단일 공유 개체로 변환됩니다.

b. **OK(**확인**)**를 클릭합니다. **Edit Shared Object(**공유 개체 편집**)**를 클릭하여 새로 형성된 개체의 세부 정보를 볼 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 기본값과 재정의 간에 값을 이동할 수 있습니다.

- **Convert to Additional Values(**추가 값으로 변환**)(**일치하지 않는 네트워크 그룹의 경우**):**

a. **Convert to Additional Values(**추가 값으로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 추가 값이 있는 단일 공유 개체로 변환됩니다.

b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.

단계 **6** 불일치를 해결한 후 변경 사항을 검토하고 지금 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

대량의 개체 문제 해결

사용되지 않는 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결, on page 35 문제가 있는 개체를 해결하는 한 가지 방법은 이러한 개체를 무시하는 것입니다. 개체에 둘 이상의 문제가 있더라도 여러 개체를 선택하고 무시할 수 있습니다. 예를 들어 개체가 일치하지 않고 사용되지 않는 경우 한 번에 하나의 문제 유형만 무시할 수 있습니다.

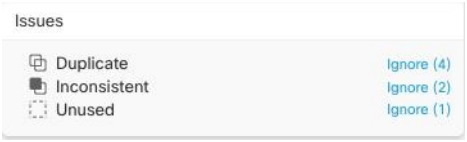
Important 나중에 개체가 다른 문제 유형과 연결될 경우 커밋한 무시 작업은 해당 시점에 선택한 문제에만 영향을 미칩니다. 예를 들어, 개체가 중복되었기 때문에 개체를 무시했고 개체가 나중에 일치하지 않는 것으로 표시되는 경우, 중복 개체로 무시한다고 해서 일치하지 않는 개체로 무시되는 것은 아닙니다.

대량으로 문제를 무시하려면 다음 절차를 수행합니다.

단계 **1** 왼쪽의 CDO 내비게이션 바에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 검색 범위를 좁히기 위해 개체 문제를 필터링할 수 있습니다.

단계 **3** Object(개체) 테이블에서 무시할 적용 가능한 모든 개체를 선택합니다. Issues(문제) 창은 문제 유형별로 개체를 그룹화합니다.



단계 **4** 유형별로 문제를 무시하려면 **Ignore(**무시**)**를 클릭합니다. 각 문제 유형을 개별적으로 무시해야 합니다.

단계 **5** **OK(**확인**)**를 클릭하여 해당 개체를 무시할 것임을 확인합니다.

디바이스 연결 상태

CDO 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Inventory(**인벤토리**)** 페이지에서 **Connectivity(**연결**)** 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 CDO에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는 문제가 두 개 이상 있을 수 있습니다. 다시 연결을 시도하면, CDO는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.

디바이스 연결 상태	가능한 이유	해결 방법
온라인	디바이스의 전원이 켜져 있고 CDO에 연결되어 있습니다.	해당 없음
오프라인	디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다.	디바이스가 오프라인 상태인지 확인합니다.
불충분한 라이선스	디바이스에 충분한 라이선스가 없습니다.	라이선스 부족 문제 해결, on page 39
유효하지 않은 자격 증명	디바이스에 연결하기 위해 CDO에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다.	유효하지 않은 자격 증명 문제 해결, on page 39

디바이스 연결 상태	가능한 이유	해결 방법
새 인증서 탐지됨	디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다.	새 인증서 문제 트러블슈팅, on page 40
온보딩 오류	CDO는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다.	온보딩 오류 문제 해결, on page 49

라이선스 부족 문제 해결

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

단계 **1** Cisco Smart Software Manager에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 스마트 라이선싱 생성 비디오를 참조하십시오.

단계 **2** CDO 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)** 페이지를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License(**라이선스 부족**)** 상태의 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 **Insufficient Licenses(**불충분한 라이선스**)**에 표시되는 **Manage Licenses(**라이선스 관리**)**를 클릭합니다. **Manage Licenses(**라이선스 관리**)** 창이 나타납니다.

단계 **6** 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록를 클릭합니다.

토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

유효하지 않은 자격 증명 문제 해결

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

단계 **1** **Inventory(**재고 목록**)** 페이지를 엽니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials(**유효하지 않은 자격 증명**)** 상태의 디바이스를 선택합니다.

단계 **4** **Device Details(**디바이스 세부 정보**)** 창에서 **Invalid Credentials(**잘못된 자격 증명**)**에 나타나는 **Reconnect(**재연결**)**을 클릭합니다. CDO가 디바이스와의 재연결을 시도합니다.

단계 **5** 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close(**닫기**)**를 클릭합니다.

단계 **8** CDO가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. Resolve Configuration Conflicts(구성 충돌 해결)를 사용하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

새 인증서 문제 트러블슈팅

CDO의 인증서 사용

CDO는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 CDO는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
   - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
   - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 CDO가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 CDO는 도메인 이름 확인을 오버라이드하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- CDO는 아직 내부 CA를 지원하지 않습니다. 현재는 내부 CA가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

  디바이스별로 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. CDO에서 ASA의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는 경우, 디바이스에 대해 지정한 IP 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증

서 검사를 비활성화할 수 있는 방법은 없습니다. 비 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

디바이스에 대한 인증서 확인을 비활성화하면 CDO는 TLS를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 CDO에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

인증서 문제 식별

CDO가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "CDO cannot connect to the device using the certificate presented(CDO가 제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

CDO가 지정된 인증서를 거부하는 이유를 확인하려면 SDC 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 openssl 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 Ctrl-c를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
```

```
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509_V_OK 작업에 성공했습니다.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509_V_ERR_UNABLE_TO_GET_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

9 X509_V_ERR_CERT_NOT_YET_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 반환 코드 확인: 9(인증서가 아직 유효하지 않음)를 참조하십시오.

10 X509_V_ERR_CERT_HAS_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간 이전입니다. 자세한 내용은 아래의 반환 코드 확인: 10(인증서가 만료되었습니다)을 참조하십시오.

11 X509_V_ERR_CRL_NOT_YET_VALID CRL이 아직 유효하지 않습니다.

12 X509_V_ERR_CRL_HAS_EXPIRED CRL이 만료되었습니다.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.

17 X509_V_ERR_OUT_OF_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 배포할 수 있지만 루트를 로컬에서 찾을 수 없습니다.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)을 참조하십시오.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큽니다. 사용되지 않음.

23 X509_V_ERR_CERT_REVOKED 인증서가 해지되었습니다.

24 X509_V_ERR_INVALID_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.

26 X509_V_ERR_INVALID_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.

27 X509_V_ERR_CERT_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.

28 X509_V_ERR_CERT_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

30 X509_V_ERR_AKID_SKID_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509_V_ERR_APPLICATION_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

Note 두 개 이상의 관리 디바이스를 동시에 CDO에 다시 대량으로 다시 연결하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. **Device & Services(**디바이스 및 서비스**)** 페이지로 이동합니다.
2. 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. Action(작업) 창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services(**디바이스 및 서비스**)** 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

인증서 오류 코드

반환 코드 확인**: 0 (ok)** 하지만 **CDO**에서 인증서 오류를 반환합니다**.**

CDO에 인증서가 있으면 "https://<device_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 CDO에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(openssl에서 0 ok 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

```
 # show asp table socket
Protocol         Socket         State         Local Address             Foreign Address
SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

반환 코드 확인**: 9(**인증서가 아직 유효하지 않음**)**

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 notBefore 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

반환 코드 확인**: 10(**인증서가 만료되었습니다**)**

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 openssl이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

반환 코드 확인**: 21(**첫 번째 인증서를 확인할 수 없음**)**

이 오류는 인증서 체인에 문제가 있음을 나타내며, openssl은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체(':'로 시작하는 줄) 및 발급자('i'로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 Organization(조직) 필드도 포함되며, 경우에 따라 Common Name(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

이 인증서가 제공되면 openssl은 ***.example.com**에 대한 ExampleCo 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 openssl의 기본 제공 신뢰 저장소에 있습니다. 확인 후 openssl이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 CA에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 있습니다. OpenSSL은 기본적으로 이러한 중간 CA를 신뢰하지 않으며, 신뢰할 수 있는 CA로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 CA에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 openssl의 출력은 다음과 같습니다.

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C
```

```
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. CDO 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 CA를 포함하려면 아래 링크 중 하나를 따르십시오(CSR이 ASA에서 생성되었는지 여부에 따라).

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

참고 두 개 이상의 관리 디바이스를 CDO에 동시에 CDO에 대량으로 다시 연결하는 경우, CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.

단계 **5** Action(작업) 창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.

단계 **6** Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services(**디바이스 및 서비스**)** 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

온보딩 오류 문제 해결

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

단계 **1** **Inventory(**인벤토리**)** 페이지에서 **Devices(**장치 **)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.

또는

단계 **3** CDO에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

"충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 **CDO**에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  Note CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

Note 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

"동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

단계 **1** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 배포**...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 미리 보고 배포하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

SecureX 문제 해결

SecureX와 함께 CDO를 사용하려고 시도하는 동안 오류, 경고 및 문제가 발생할 수 있습니다. SecureX UI에 표시되는 문제의 경우 SecureX 설명서를 사용해야 합니다. 자세한 내용은 SecureX 지원을 참조하십시오.

CDO 내의 SecureX 리본 기능 또는 SecureX 리본에 대한 테넌트 액세스 가능성에 대한 사례를 열려면 CDO Cisco TAC에서 자세한 내용을 참조하십시오. 테넌트 ID를 제공하라는 요청을 받을 수 있습니다.

SecureX UI 문제 해결

SecureX 대시보드에 중복된 **CDO** 모듈이 표시됩니다**.**

SecureX에서 단일 제품의 여러 모듈을 수동으로 구성할 수 있습니다. 예를 들어 여러 CDO 테넌트가 있는 경우 테넌트당 하나의 CDO 모듈을 생성할 수 있습니다. 중복 모듈은 동일한 CDO 테넌트에서 두 개의 개별 API 토큰이 있음을 의미합니다. 이러한 중복은 혼란을 야기하고 대시보드를 복잡하게 만들 수 있습니다.

SecureX에서 CDO 모듈을 수동으로 구성한 다음 CDO의 일반 설정 페이지에서 **SecureX** 연결을 선택한 경우 이로 인해 하나의 테넌트가 SecureX에 여러 모듈을 가질 수 있습니다.

이 문제를 해결하려면 SecureX에서 원래 CDO 모듈을 제거하고 중복 모듈로 CDO 성능을 계속 모니터링하는 것이 좋습니다. 이 모듈은 더 안전하고 SecureX 리본과 호환되는 더 강력한 API 토큰으로 생성됩니다.

CDO UI 문제 해결

SecureX 내의 CDO 모듈에 대한 사례를 열려면 SecureX 약관, 개인 정보 보호, 지원의 지원 섹션에서 자세한 내용을 참조하십시오.

OAuth 오류

다음 메시지와 함께 oAuth 오류가 발생할 수 있습니다. "사용자가 필요한 모든 범위 또는 충분한 권한을 가지고 있지 않은 것 같습니다." 이 문제가 발생하면 다음 가능성을 고려하십시오.

- 계정이 활성화되지 않았을 수 있습니다. https://visibility.test.iroh.site/에서 등록된 이메일 주소를 사용하여 계정이 활성화되었는지 확인합니다. 계정이 활성화되지 않은 경우 CDO 테넌트가 SecureX와 병합되지 않을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 Cisco TAC에 문의를 참조하십시오.

잘못된 조직 자격 증명으로 SecureX에 로그인했습니다.

일반 설정 페이지의 테넌트 설정 섹션에 있는 **Connect SecureX** 옵션을 사용하여 CDO 이벤트를 SecureX로 보내기로 선택했지만 잘못된 자격 증명을 사용하여 SecureX에 로그인한 경우, 잘못된 테넌트의 이벤트가 SecureX 대시보드에 표시될 수 있습니다.

이 문제를 해결하려면 CDO의 일반 설정 페이지에서 **SecureX** 연결 끊기를 클릭합니다. 이렇게 하면 SecureX 조직과 정보를 주고 받는 데 사용되는 읽기 전용 API 사용자가 종료되고 결과적으로 SecureX 대시보드가 종료됩니다.

그런 다음 **Connect Tenant to SecureX**를 다시 활성화하고 SecureX에 로그인하라는 메시지가 표시되면 올바른 조직 로그인 자격 증명을 사용해야 합니다.

잘못된 계정으로 리본에 로그인했습니다.

이때 잘못된 계정 정보로 리본에 로그인하면 리본에서 로그아웃할 수 없습니다. 리본 로그인을 수동으로 재설정하려면 Support Case Manager에서 사례를 열어야 합니다.

SecureX 리본을 실행할 수 없습니다.

적절한 범위에 대한 액세스 권한이 없을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 Cisco TAC에 문의를 참조하십시오.

SecureX 리본 작동 방식에 대한 자세한 내용은 SecureX 리본 설명서를 참조하십시오.