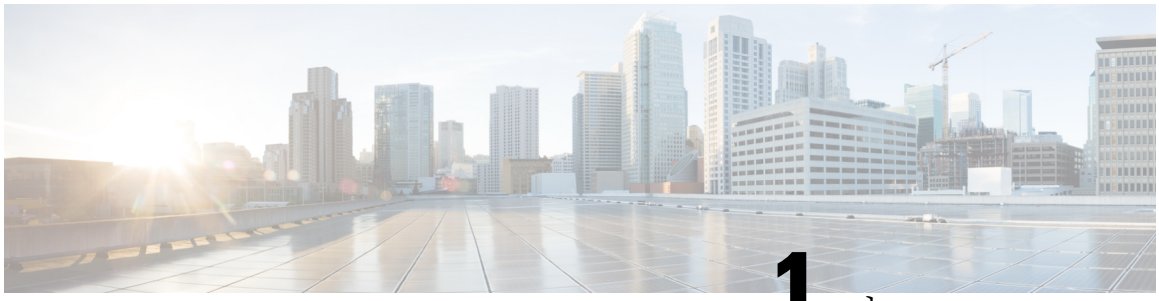
Cisco Security Analytics and Logging (온프레미스) v3.1.0: 방화벽 이벤트 통합 가이드

초판: 2022년 4월 18일

최종 변경: 2022년 5월 24일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



1 장

소개

개요

이 가이드에서는 더 긴 보존 기간에 스토리지를 늘리기 위해 방화벽 이벤트 데이터를 저장하도록 Cisco Security Analytics 및 로깅(온프레미스) 구성을 하는 방법을 설명합니다. Cisco Secure Network Analytics(이전 Stealthwatch) 어플라이언스를 구축하고 방화벽 구축과 통합하면 Secure Network Analytics 어플라이언스로 이벤트 데이터를 내보낼 수 있습니다.

다음을 할 수 있습니다.

- Secure Firewall Management Center에 이벤트를 저장하고 Secure Network Analytics 구축에 이벤트를 저장합니다.
- management center에서 이러한 이벤트를 보려면 이 원격 데이터 소스를 지정합니다.
- 이벤트 뷰어를 사용하여 Cisco Secure Network Analytics Manager(이전 Stealthwatch Management Console) 웹 애플리케이션 UI에서 이벤트 데이터를 검토합니다.
- management center UI에서 이벤트 뷰어로 크로스 실행하여 크로스 실행한 정보에 대한 추가 컨텍스트를 확인합니다.

참고 온프레미스가 아니라 Cisco 클라우드에 방화벽 이벤트 데이터를 저장하려는 경우 Cisco SaaS(Security Analytics and Logging) 설명서에서 자세한 내용을 참조하십시오.

개념 및 아키텍처

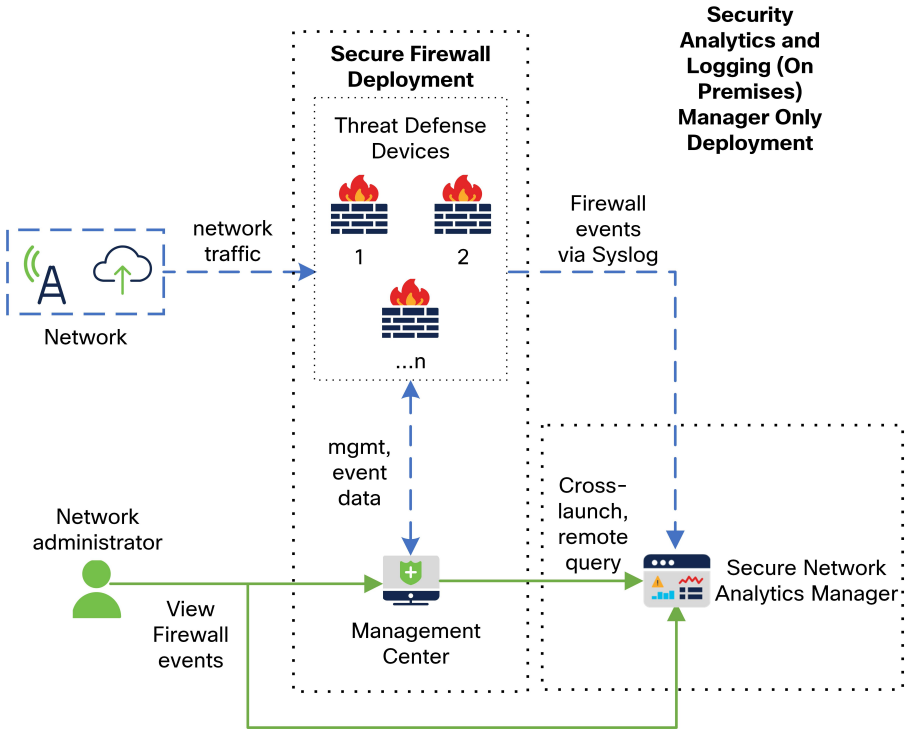
Security Analytics and Logging(온프레미스)구축에서 어플라이언스를 사용Secure Network Analytics하여 다른 Cisco 제품 구축의 데이터를 저장할 수 있습니다. 보안 방화벽 구축의 경우 management center에서 관리하는 Secure Firewall Threat Defense 디바이스에서 보안 이벤트 및 데이터 플레인 이벤트를 관리자에 내보내 해당 정보를 저장할 수 있습니다.

Secure Network Analytics 구축에는 두 가지 옵션이 있습니다.

- 관리자 전용 - 이벤트를 수신 및 저장하는 독립형 관리자 구축, 이벤트의 검토 및 쿼리 가능
- 데이터 저장소 - 이벤트를 수신할 Cisco Secure Network Analytics 플로우 컬렉터(최대 5개), 이벤트를 저장할 Cisco Secure Network Analytics 데이터 노드 1~3개 이상(3개 세트)을 포함하는 Cisco Secure Network Analytics 데이터 저장소 구축 이벤트를 검토하고 쿼리할 수 있는 관리자

관리자 전용

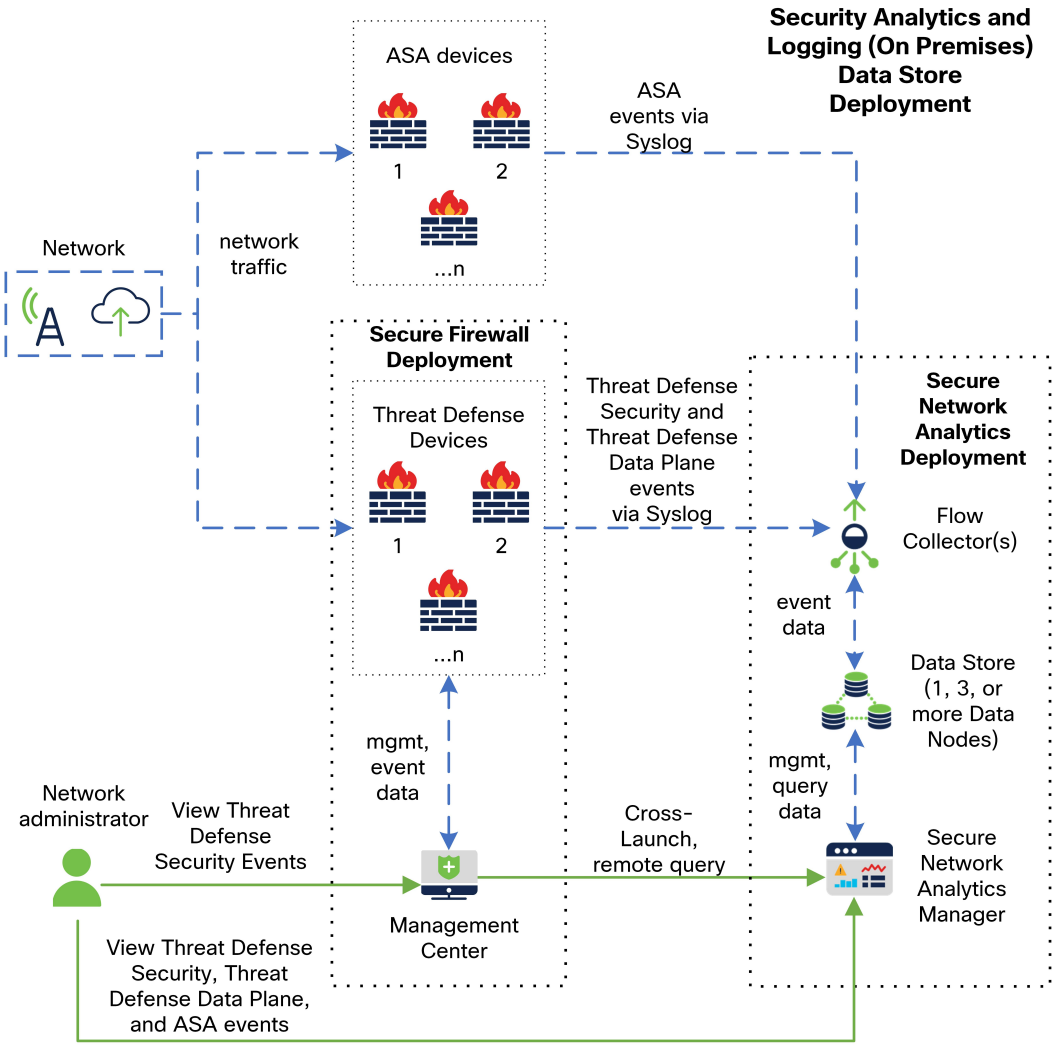
다음 다이어그램에서 관리자 전용 구축의 예를 참조하십시오.



이 구축에서 threat defense 디바이스는 관리자(으)로 보안 방화벽 이벤트를 전송하고, 관리자는 이러한 이벤트를 저장합니다. 사용자는 management center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 또한 management center에서 이벤트를 원격으로 쿼리할 수 있습니다.

데이터 저장소

다음 다이어그램에서 관리자, 데이터 노드 및 플로우 컬렉터가 있는 데이터 저장소 구축의 예를 참조하십시오.

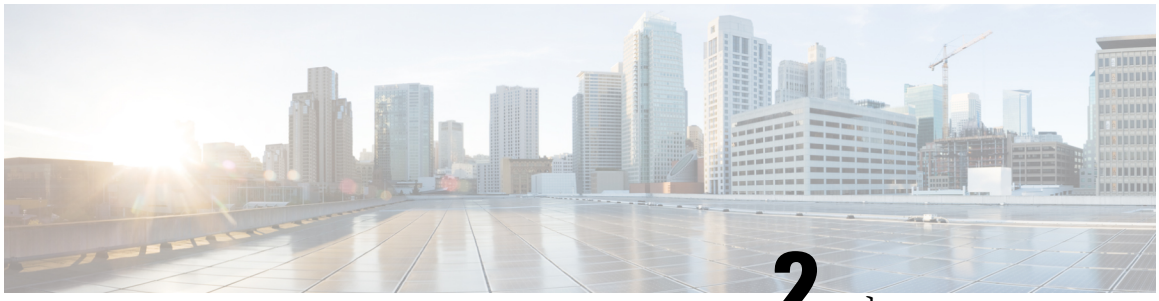


이 구축에서 threat defense 및 보안 방화벽 ASA 디바이스는 플로우 컬렉터로 방화벽 이벤트를 전송합니다. 플로우 컬렉터는 데이터 저장소로 이벤트를 전송하여 저장합니다. 사용자는 management center UI에서 관리자에 교차 실행하여 저장된 이벤트에 대한 세부 정보를 볼 수 있습니다. 또한 management center에서 이벤트를 원격으로 쿼리할 수 있습니다.

지원되는 이벤트 유형

- Threat Defense 보안 이벤트
  - 연결
  - 침입
  - 파일 및 악성코드
- Threat Defense 데이터 플레인 이벤트(데이터 저장소 구축만 해당)

- ASA 이벤트(데이터 저장소 구축만 해당)



2 장

구축

필수조건

다음은 방화벽 이벤트 데이터를 저장하기 위해 Security Analytics and Logging(온프레미스) 구축을 하기 위한 어플라이언스 요구 사항입니다.

방화벽 어플라이언스

다음 방화벽 어플라이언스를 구축해야 합니다.

솔루션 구성 요소	필수 버전	라이선싱: **Cisco Security Analytics** 및 로깅(온프레미스)	참고
Management Center(하드웨어 또는 가상)	v7.2+ https://cisco.com/go/sal-on-prem-docs에서 이전 버전을 실행 중인 management center에 대해 알아보십시오.	없음	• management center 당 하나의 관리자 구축 가능, 선택 사항으로 다중의 플로우 컬렉터 및 데이터 노드 가능

솔루션 구성 요소	필수 버전	라이선싱: **Cisco Security Analytics** 및 로깅(온프레미스)	참고
Secure Firewall 관리 디바이스	마법사를 사용하는 v7.0 이상 시스템 로그를 사용하는 Threat Defense v6.4 이상 시스템 로그를 사용하는 NGIPS v6.4	없음	• threat defense v6.4 이상에서 시스템 로그를 사용하는 방법에 대한 안내를 찾으려면 이전 버전의 위협 대응 디바이스에서 이벤트 전송을 참고하십시오.
ASA 디바이스	v9.12 이상	없음	

Secure Network Analytics Appliances

다음과 같은 Secure Network Analytics 구축 옵션이 있습니다.

- 관리자 전용 - 이벤트를 수집 및 저장하고, 이벤트를 검토 및 쿼리하는 용도로만 관리자 구축
- 데이터 저장소 - 플로우 컬렉터를 구축하여 이벤트를 수집하고, 데이터 저장소를 통해 이벤트를 저장하고, 관리자로 이벤트를 검토 및 쿼리합니다.

표 *1:* 관리자 전용

솔루션 구성 요소	필수 버전	라이선싱: **Security Analytics and Logging**(온프레미스)	참고
관리자	Secure Network Analytics v7.4.0 이상	없음	• 모두 하나의 management center에서 관리하는 경우, 여러 threat defense 디바이스에서 이벤트를 수신할 수 있습니다. • 이벤트 수집을 위해 그리고 관리자 웹 애플리케이션에서 방화벽 이벤트를 보려면 Security Analytics and Logging(온프레미스) 애플리케이션을 설치해야 합니다.

솔루션 구성 요소	필수 버전	라이선싱: **Security Analytics and Logging(**온프레미스**)**	참고
Security Analytics and Logging(온프레미스) 애플리케이션	Security Analytics and Logging(온프레미스) 앱 v3.1 이상	스마트 라이선스 로깅 및 문제 해결(GB/일 기준)	관리자에 이 앱을 설치하고 이벤트 수집을 활성화하도록 구성

표 *2:* 데이터 저장소

솔루션 구성 요소	필수 버전	라이선싱: **Security Analytics and Logging(**온프레미스**)**	참고
관리자	Secure Network Analytics v7.4.0 이상	없음	• 이벤트 수집을 위해 그리고 관리자 웹 애플리케이션에서 방화벽 이벤트를 보려면 Security Analytics and Logging(온프레미스) 애플리케이션을 설치해야 합니다. • 단일 노드 데이터 저장소 및 다중 텔레메트리에는 Secure Network Analytics v7.4.1이 필요합니다.

솔루션 구성 요소	필수 버전	라이선싱: **Security Analytics and Logging**(온프레미스)	참고
Flow Collector	Secure Network Analytics v7.4.0 이상	없음	• 데이터 저장소에 대해 구성된 여러 플로우 컬렉터 구축 가능 • 모두 하나의 management center에서 관리하는 경우, 여러 threat defense 디바이스에서 이벤트를 수신할 수 있습니다. • 여러 ASA 디바이스에서 ASA 이벤트 수신 가능 • 단일 노드 데이터 저장소 및 다중 텔레메트리에는 Secure Network Analytics v7.4.1이 필요합니다.
데이터스토어	Secure Network Analytics v7.4.0 이상	없음	• 1개, 3개 이상(3개 집합)의 데이터 노드 구축 가능 • 플로우 컬렉터에서 수신한 방화벽 이벤트 저장 가능 • 단일 노드 데이터 저장소 및 다중 텔레메트리에는 Secure Network Analytics v7.4.1이 필요합니다.
Security Analytics and Logging(온프레미스) 애플리케이션	Security Analytics and Logging(온프레미스) 앱 v3.1 이상	스마트 라이선스 로깅 및 문제 해결(GB/일 기준)	관리자에 이 앱을 설치하고 이벤트 수집을 활성화하도록 구성

이러한 구성 요소 외에도 모든 어플라이언스가 NTP를 사용하여 시간을 동기화할 수 있는지 확인해야 합니다.

Secure Firewall 또는 Secure Network Analytics 어플라이언스의 콘솔에 원격으로 액세스하려는 경우 SSH를 통한 액세스를 활성화할 수 있습니다.

Secure Network Analytics 라이선싱

라이선스 없이 평가 모드에서 90일 간 Security Analytics and Logging(온프레미스) 사용이 가능합니다. 90일 이후에 Security Analytics and Logging(온프레미스)을(를) 계속 사용하려면 방화벽 구축에서 Secure Network Analytics 어플라이언스로 시스템 로그 데이터를 전송할 것으로 예상되는 일별 GB를 기준으로 스마트 라이선싱용 로깅 및 문제 해결 스마트 라이선스를 얻어야 합니다.

참고 라이선스 계산을 위해 데이터의 양은 가장 가까운 전체 GB 단위로 보고됩니다. 예를 들어 하루에 4.9GB를 전송하는 경우 4GB로 보고됩니다.

Secure Network Analytics Smart Software 라이선싱 가이드에서 Secure Network Analytics 어플라이언스 라이선싱에 대한 세부 내용을 참고하십시오.

Secure Network Analytics 리소스 배정

Secure Network Analytics은(는) Security Analytics and Logging(온프레미스)에 대해 구축된 경우 다음 수집 속도를 제공합니다.

- 하드웨어 또는 VE(가상 에디션) 관리자 전용 구축은 최대 35k EPS의 짧은 버스트로 평균 약 20k 이벤트를 수집할 수 있습니다.
- 데이터 노드 3개가 있는 VE(가상 에디션) 데이터 저장소 구축은 최대 175k EPS의 짧은 버스트를 사용하여 평균 약 50k EPS를 수집할 수 있습니다.
- 데이터 노드 3개가 있는 하드웨어 데이터 저장소 구축은 최대 350k EPS의 짧은 버스트를 사용하여 평균 약 100k EPS를 수집할 수 있습니다.

할당된 하드 드라이브 스토리지에 따라 몇 주 또는 몇 달 동안 데이터를 저장할 수 있습니다. 이러한 예측은 네트워크 로드, 트래픽 급증, 이벤트별로 전송되는 정보 등의 다양한 요인에 따라 달라집니다.

참고 EPS 수집 속도가 높으면 Security Analytics and Logging(온프레미스) 앱에서 데이터를 삭제할 수 있습니다. 또한 연결, 침입, 파일 및 악성코드 이벤트만 전송하는 대신 모든 이벤트 유형을 전송하는 경우, 전체 EPS가 증가할 때 앱에서 데이터를 삭제할 수 있습니다. 이 경우 로그 파일을 검토합니다.

관리자 전용 권장 사항

관리자 **VE** 리소스

최적의 성능을 위해 관리자 VE를 구축하는 경우 다음 리소스를 할당합니다.

리소스	권장 사항
CPU	12
RAM	64GB
하드 드라이브 스토리지	2TB

관리자 **2210** 사양

관리자 2210 사양 시트에서 하드웨어 사양을 참고하십시오.

예측 보존 기간

관리자 VE에 할당한 스토리지 공간을 기반으로 하거나 관리자 2210이 있는 경우 관리자 전용 구축 시 대략 다음 기간에 데이터를 저장할 수 있습니다.

평균 **EPS**	평균 일별 이벤트	**1TB** 스토리지의 예상 보존 기간	**2TB** 스토리지의 예상 보존 기간	**4TB** 스토리지(하드웨어)의 예상 보존 기간
1,000	8,650만	250일	500일	1000일
5,000	4억 3,000만	50일	100일	200일
10,000	8억 6,500만	25일	50일	100일
20,000	17억 3천만	12.5일	25일	50일

관리자은(는) 최대 스토리지 용량에 도달하면 가장 오래된 데이터를 먼저 삭제하여 수신 데이터를 위한 공간을 확보합니다.

참고 이 예상 수집 및 스토리지 기간에 이러한 리소스 할당을 사용하여 관리자 VE를 테스트했습니다. 가상 어플라이언스에 충분한 CPU 또는 RAM을 할당하지 않으면 리소스 할당 부족으로 인해 예기치 않은 오류가 발생할 수 있습니다. 스토리지 할당을 2TB 이상으로 늘리면 리소스 할당 부족으로 인해 예기치 않은 오류가 발생할 수 있습니다.

데이터 저장소 권장 사항

최적의 성능을 위해 관리자 VE, 플로우 컬렉터 VE 및 데이터 저장소 VE를 구축하는 경우 다음 리소스를 할당하십시오.

참고 단일 노드 데이터 저장소를 사용 중이거나 Secure Network Analytics에서 다중 텔레메트리를 활성화한 경우 리소스 할당 및 스토리지 용량이 다음 권장 사항과 다를 수 있습니다. Secure Network Analytics 어플라이언스 설치 가이드(하드웨어 또는 가상 에디션) 및 시스템 구성 가이드 v7.4.1에서 자세한 내용을 참고하십시오.

표 ***3:*** 관리자 ***VE***

리소스	권장 사항
CPU	8
RAM	64GB
하드 드라이브 스토리지	480GB

표 ***4: Flow Collector VE***

리소스	권장 사항
CPU	8
RAM	70GB
하드 드라이브 스토리지	480GB

표 ***5:*** 데이터 노드 ***VE(***데이터 저장소의 일부***)***

리소스	권장 사항
CPU	데이터 노드당 12개
RAM	데이터 노드당 32GB
하드 드라이브 스토리지	데이터 노드 VE당 5TB 또는 3개의 데이터 노드에서 총 15TB

하드웨어 사양

어플라이언스 사양 시트에서 하드웨어 사양을 참고하십시오.

예측 보존 기간**(3** 데이터 노드**)**

데이터 저장소 VE에 할당한 스토리지 공간에 따라 또는 하드웨어 구축이 있는 경우 데이터 저장소구축 시 대략 다음 기간에 데이터를 저장할 수 있습니다.

평균 **EPS**	평균 일별 이벤트	가상	하드웨어
1,000	8,650만	1,500일	3,000일

평균 **EPS**	평균 일별 이벤트	가상	하드웨어
5,000	4억 3,000만	300일	600일
10,000	8억 6,500만	150일	300일
20,000	17억 3천만	75일	150일
25,000	21억 6천만	60일	120일
50,000	43억 2천만	30일	60일
75,000	64억 8000만	지원되지 않음	40일
100,000	86억 4천만	지원되지 않음	30일

데이터 저장소는 최대 스토리지 용량에 도달하면 수신 데이터용 공간을 확보하기 위해 가장 오래된 데이터를 먼저 삭제합니다. 스토리지 용량을 늘리려면 Secure Network Analytics 시스템 구성 가이드를 사용하여 데이터 노드를 더 추가하십시오.

참고 이 예상 수집 및 스토리지 기간에 이러한 리소스 할당을 사용하여 가상 어플라이언스를 테스트했습니다. 가상 어플라이언스에 충분한 CPU 또는 RAM을 할당하지 않으면 리소스 할당 부족으로 인해 예기치 않은 오류가 발생할 수 있습니다. 데이터 노드 스토리지 할당을 5TB 이상으로 늘리면 리소스 할당 부족으로 인해 예기치 않은 오류가 발생할 수 있습니다.

통신 포트

다음 표에는 관리자 전용 구축을 위한 Security Analytics and Logging(온프레미스) 통합을 위해 열어야 하는 통신 포트가 나와 있습니다.

표 ***6:*** 관리자 전용

발신(클라이언트)	수신(서버)	포트	프로토콜 또는 목적
Management Center, Threat Defense 디바이스 및 관리자	외부 인터넷(NTP 서버)	123/UDP	NTP 시간 동기화, 모두 동일한 NTP 서버
사용자 워크스테이션	Management Center 및 관리자	443/TCP	웹 브라우저를 사용하여 HTTPS를 통해 어플라이언스의 웹 인터페이스에 로그인
management center(으)로 관리되는 Threat Defense 디바이스	관리자	8514/UDP	threat defense 디바이스에서 관리자(으)로 시스템 로그 내보내기

발신(클라이언트)	수신(서버)	포트	프로토콜 또는 목적
Management Center	관리자	443/TCP	management center에서 관리자(으)로의 원격 쿼리

다음 표에는 데이터 저장소 구축을 위한 Security Analytics and Logging(온프레미스) 통합을 위해 열어야 하는 통신 포트가 나와 있습니다. 또한 Secure Network Analytics 구축을 위해 열어야 하는 포트에 대해 알아보려면 x2xx 시리즈 하드웨어 어플라이언스 설치 가이드 또는 가상 에디션 어플라이언스 설치 가이드를 참조하십시오.

표 *7:* 데이터 저장소

발신(클라이언트)	수신(서버)	포트	프로토콜 또는 목적
Management Center, Threat Defense 디바이스, 관리자, 플로우 컬렉터 및 데이터 저장소	외부 인터넷(NTP 서버)	123/UDP	NTP 시간 동기화, 모두 동일한 NTP 서버
사용자 워크스테이션	Management Center 및 관리자	443/TCP	웹 브라우저를 사용하여 HTTPS를 통해 어플라이언스의 웹 인터페이스에 로그인
management center(으)로 관리되는 Threat Defense 디바이스	Flow Collector	8514/UDP	threat defense 디바이스에서 플로우 컬렉터로의 시스템 로그 내보내기
ASA 디바이스	Flow Collector	8514/UDP	ASA 디바이스에서 플로우 컬렉터로의 시스템 로그 내보내기
Management Center	관리자	443/TCP	management center에서 관리자(으)로의 원격 쿼리

구성 개요

다음은 이벤트 데이터를 저장하도록 구축을 구성하는 상위 레벨 단계를 설명합니다.

구축을 시작하기 전에 다음 작업을 검토합니다.

구성 요소 및 작업	단계
구축관리자 전용	다음 옵션을 이용할 수 있습니다. • 네트워크에 관리자 2210을 구축하고 eth0 관리 인터페이스 IP 주소 및 기타 정보 할당을 포함하여 초기 구성을 수행합니다. x2xx Series 하드웨어 어플라이언스 설치 가이드 및 Secure Network Analytics 시스템 구성 가이드에서 자세한 내용을 참조하십시오. • 관리자 VE ISO를 다운로드하고 하이퍼바이저에 관리자 VE를 구축합니다. 초기 구성을 수행하고 eth0 관리 인터페이스 IP 주소 및 기타 정보를 할당합니다. Secure Network Analytics 가상 에디션 어플라이언스 설치 가이드에서 자세한 내용을 참고하십시오.
구축데이터 저장소	• 1개의 관리자, 플로우 컬렉터 및 1개, 3개 이상(3개 세트)의 데이터 노드를 네트워크에 구축합니다. 각 어플라이언스에 대한 초기 구성을 수행하고 데이터 저장소를 초기화합니다. x2xx Series 하드웨어 어플라이언스 설치 가이드 또는 Virtual Edition 어플라이언스 설치 가이드 및 Secure Network Analytics 시스템 구성 가이드에서 자세한 내용을 참고하십시오.
관리자에 Security Analytics and Logging(온프레미스) 앱을 다운로드하여 설치하고 방화벽 이벤트를 수신 및 저장하도록 Secure Network Analytics 구축을 구성합니다.	• https://software.cisco.com에서 앱 파일 app-smc-sal-3.1.0-v2.swu를 다운로드합니다. • 관리자에서 Central Management의 App Manager(앱 관리자)로 이동하여 앱을 설치합니다. 앱에 대해 자세히 알아보려면 Security Analytics and Logging(온프레미스) 릴리스 노트 및 앱 도움말을 참조하십시오.
Security Analytics and Logging(온프레미스)에 이벤트를 전송하도록 management center 구성	다음 옵션을 이용할 수 있습니다. • Secure Firewall Management Center 구성, 17 페이지 섹션을 사용하여 Secure Network Analytics 어플라이언스에 이벤트를 전송하도록 management center을(를) 구성합니다. • 시스템 로그를 사용하여 Secure Network Analytics에 데이터 플레인 이벤트 로그를 전송하도록 Secure Firewall Management Center 구성 섹션을 사용하여 데이터 플레인 이벤트 로깅을 구성합니다. • 우선순위가 낮은 연결 이벤트 저장 중지 Management Center를 사용하여 management center의 로깅 로드를 줄입니다.
이벤트를 Security Analytics and Logging(온프레미스)에 전송할 ASA 디바이스 구성	• ASA 디바이스 구성, 24 페이지 섹션을 사용하여 Secure Network Analytics 어플라이언스에 이벤트를 전송하도록 ASA 디바이스를 구성합니다.

구성 요소 및 작업	단계
다음 단계 검토	다음 단계를 검토합니다. • 보안 방화벽 온라인 도움말에서 자세한 내용을 참고하십시오. Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Management Center에서 작업을 참조하십시오.. • 관리자 웹 애플리케이션 온라인 도움말에서 Secure Network Analytics 사용 방법에 대한 세부 내용을 참고하십시오.

Secure Network Analytics 구축 및 구성

Security Analytics and Logging(온프레미스)에 대해 Secure Network Analytics 구축을 하고 구성하려면 다음과 같이 합니다.

1. Secure Network Analytics 구축에 대한 지침을 따릅니다.
   - 관리자 전용 구축 및 구성, 15 페이지
   - 데이터 저장소 구축 및 구성, 16 페이지
2. Security Analytics and Logging(온프레미스) 앱을 설치합니다., 16 페이지.

관리자 전용 구축 및 구성

시작하기 전에

- 네트워크에 관리자 구축을 했으며, management center의 관리 IP 주소와 threat defense 디바이스의 관리 IP 주소 모두에서 관리 IP 주소에 연결할 수 있는지 확인합니다. 추가 구성을 위해 관리 IP 주소를 적어 둡니다. Secure Network Analytics 가상 에디션 어플라이언스 설치 가이드에서 자세한 내용을 참고하십시오.
- Secure Network Analytics 제품 인스턴스 등록을 확인합니다. 관리자 VE 라이선스는 등록 후 어카운트에 자동으로 추가됩니다. Secure Network Analytics Smart Software 라이선싱 가이드에서 자세한 내용을 참고하십시오.

Secure Network Analytics가상 에디션 어플라이언스 설치 가이드의 지침에 따라 관리자 VE를 구축하거나, x2xx 시리즈 하드웨어 어플라이언스 설치 가이드에 따라 관리자 2210을 구축하고, Secure Network Analytics시스템 구성 가이드에 따라 관리자을(를) 구성합니다.

데이터 저장소 구축 및 구성

중요 어플라이언스 최초 시간 설정 중에 방화벽 로그를 수집하고 저장하려면 플로우 컬렉터를 활성화해야 합니다. 이 설정은 Security Analytics and Logging(온프레미스)에 사용할 플로우 컬렉터를 구성합니다. 어플라이언스를 구성한 후 플로우 컬렉터 고급 설정을 사용하여 수집 설정을 업데이트할 수 있습니다. 플로우 컬렉터 고급 설정을 사용한 Security Analytics and Logging(온프레미스) 구성 섹션에서 자세한 내용을 참조하십시오.

시작하기 전에

- 관리자, 플로우 컬렉터 및 데이터 노드를 네트워크에 구축했는지, threat defense 디바이스의 관리 IP 주소로 플로우 컬렉터 관리 IP 주소에 연결할 수 있는지, management center의 관리 IP 주소를 기준으로 관리자 관리 IP 주소에 연결할 수 있는지 확인합니다. 추가 구성을 위해 관리 IP 주소를 적어 둡니다.
- Secure Network Analytics 제품 인스턴스 등록을 확인합니다. 관리자 VE 라이선스는 등록 후 어카운트에 자동으로 추가됩니다. Secure Network Analytics Smart Software 라이선싱 가이드에서 자세한 내용을 참고하십시오.

단계 **1** x2xx 시리즈 하드웨어 어플라이언스 설치 가이드의 지침에 따라 Secure Network Analytics 하드웨어 어플라이언스를 구축하거나 가상 에디션 어플라이언스 설치 가이드에 따라 Secure Network Analytics 가상 어플라이언스를 구축합니다.

단계 **2** Secure Network Analytics 시스템 구성 가이드를 사용하여 어플라이언스를 구성합니다. 플로우 컬렉터에서 최초 설정을 구성할 때 다음을 선택해야 합니다.

- 데이터 저장소의 일부로 플로우 컬렉터를 구축할지 묻는 메시지가 표시되면 예를 선택합니다. 아니요를 선택하면 새 가상 어플라이언스를 구축하거나 어플라이언스를 RFD해야 합니다.
- 텔레메트리 유형 선택 화면에서 방화벽 로그를 선택합니다. 그런 다음 UDP 포트를 입력합니다. 기본적으로 8514가 사용됩니다. 예를 클릭하여 설정을 확인합니다.

Security Analytics and Logging(온프레미스) 앱을 설치합니다.

관리자에 Security Analytics and Logging(온프레미스) 앱을 설치합니다. Security Analytics and Logging(온프레미스) 릴리스 노트에서 자세한 내용을 참고하십시오.

단계 **1** https://software.cisco.com에서 Cisco 스마트 어카운트에 로그인하거나 관리자에게 문의하여 Security Analytics and Logging(온프레미스) 앱을 다운로드합니다.

단계 **2** 관리자에 로그인합니다.

단계 **3** 전역 설정 아이콘을 클릭합니다.
단계 **4** **Central Management**를 선택합니다.
단계 **5** 앱 관리자 탭을 클릭합니다.
단계 **6** **Browse(**찾아보기**)**를 클릭합니다.
단계 **7** 화면에 표시되는 프롬프트에 따라 앱 파일을 업로드합니다.

다음에 수행할 작업

- Secure Network Analytics 어플라이언스에 이벤트를 전송하도록 management center 구성을 합니다.
- Secure Network Analytics 어플라이언스에 이벤트를 전송하도록 ASA 디바이스를 구성합니다. ASA 디바이스 구성, 24 페이지의 내용을 참조하십시오.

주의 관리자 전용 구축이 있는 경우 Security Analytics and Logging(온프레미스) 앱을 제거하면 방화벽 이벤트 데이터를 비롯한 모든 관련 정보가 관리자에서 삭제됩니다. 또한 독립형 관리자 제한을 제거합니다. Security Analytics and Logging(온프레미스) 애플리케이션을 제거한 후에는 트래픽을 검사하기 위해 기존 Secure Network Analytics 구축의 일부로 독립형 관리자이(가) 있는 하나 이상의 플로우 컬렉터를 관리할 수 있습니다.

Secure Firewall Management Center 구성

Security Analytics and Logging(온프레미스)에 대해 Secure Firewall Management Center 구성을 할 때 Secure Network Analytics에 이벤트를 전송할 수 있는 다음 옵션이 있습니다.

- 이벤트를 Secure Network Analytics 구축에 직접 전송하도록 Secure Firewall Management Center에서 마법사 구성.
- 시스템 로그를 사용하여 Secure Network Analytics에 데이터 플레인 이벤트 로그를 전송하도록 Secure Firewall Management Center 구성.

Secure Firewall Management Center에서 마법사 구성

다음은 모든 Secure Firewall Management Center 사용자가 방화벽 이벤트를 보내고 저장할 수 있게 하는 Security Analytics and Logging(온프레미스) 구축 마법사에 대한 설명입니다.

- 관리자 전용: 이벤트를 전송 및 저장하며, 이벤트를 검토하고 쿼리할 수 있는 독립형 관리자을(를) 구축합니다. 이벤트 데이터를 관리자 전용 구축에 전송하도록 Secure Firewall Management Center 구성에서 관리자 전용 구축 구성에 대한 세부 내용을 참고하십시오.
- 데이터 저장소: 이벤트를 수신하는 플로우 컬렉터, 이벤트를 저장하는 데이터 저장소, 이벤트를 검토하고 쿼리할 수 있는 관리자을(를) 구축합니다. 이벤트 데이터를 데이터 저장소 구축에 전송

하도록 Secure Firewall Management Center 구성에서 데이터 저장소 구축 구성에 대한 세부 내용을 참고하십시오.

Secure Firewall 통합을 위한 사전 요건

- Secure Firewall 시스템이 예상대로 작동하고 전송하려는 이벤트를 생성해야 합니다.
- 방화벽 이벤트 데이터를 수신할 수 있도록 Secure Network Analytics및 Security Analytics and Logging(온프레미스) 제품을 설정합니다.
- 다음 Secure Firewall 사용자 역할 중 하나가 있어야 합니다.
  - 관리자
  - 애널리스트
  - 보안 분석가
- 현재 시스템 로그를 사용하여 이벤트를 직접 전송하는 것을 지원하는 디바이스 버전에서 Secure Network Analytics에 이벤트를 전송하는 경우, 원격 볼륨에서 이벤트가 중복되지 않도록 해당 디바이스에 대해 시스템 로그를 비활성화합니다(또는 시스템 로그 구성을 포함하지 않는 액세스 제어 정책을 해당 디바이스에 할당).
- 다음과 같은 세부 정보가 있습니다.
  - 관리자의 호스트 이름이나 IP 주소.
  - (플로우 컬렉터를 사용하여 확장된 스토리지 용량을 위해 여러 Secure Network Analytics 어플라이언스를 집계하는 경우) 플로우 컬렉터의 IP 주소입니다. (이 설정에는 호스트 이름을 사용할 수 없습니다.)
  - 관리자 권한이 있는 Secure Network Analytics 어플라이언스의 계정에 대한 자격 증명.

    이러한 자격 증명은 management center에 저장되지 않습니다. 관리자에서 management center에 대한 읽기 전용 Analyst API 계정을 설정하는 데 한 번만 사용됩니다. 이를 위해서는 전용 계정이 필요하지 않습니다. 고유한 관리자 자격 증명을 사용할 수 있습니다.

    등록 프로세스 중에 관리자에서 로그아웃될 수 있습니다. 이 마법사를 시작하기 전에 진행 중인 작업을 완료하십시오.
  - "처음 사용 시 신뢰" 옵션을 관리자에서 사용하지 않으려는 경우 SSL 인증서.

이벤트 데이터를 관리자 전용 구축에 전송하도록 **Secure Firewall Management Center** 구성

시작하기 전에

Secure Firewall Management Center에서 마법사 구성에 나와 있는 모든 요구 사항을 충족하는지 확인합니다.

단계 **1** Secure Firewall Management Center에서 통합 > **Security Analytics & Logging**으로 이동합니다.

단계 **2** 관리자 전용 위젯에서 시작을 클릭합니다.

단계 **3** Secure Network Analytics Manager의 호스트 이름 또는 IP 주소와 포트를 입력하고 다음을 클릭합니다.

단계 **4** 찾은 검색을 확인합니다.

1. 로깅을 위해 IP 주소 및 포트를 확인하고 필요한 경우 수정합니다.
2. 교차 실행 URL 및 포트를 확인하고 필요한 경우 수정합니다.
3. "처음 사용 시 신뢰" 옵션을 사용하지 않으려면 관리자에서 SSL 인증서를 업로드합니다.
4. **Next(**다음**)**를 클릭합니다.

단계 **5** 쿼리에 대한 보안 통신을 설정하기 위해 관리자에 로그인할 자격 증명을 입력하고 완료를 클릭합니다.

이러한 자격 증명은 management center에 저장되지 않습니다. Secure Network Analytics Manager에서 management center에 대한 읽기 전용 Analyst API 계정을 설정하는 데 한 번 사용됩니다. 이를 위해서는 전용 계정이 필요하지 않습니다. 고유한 관리자 자격 증명을 사용할 수 있습니다.

다음에 수행할 작업

- Secure Network Analytics 어플라이언스에 이벤트가 성공적으로 저장되었음을 확인한 후에는 management center에 저장된 모든 이벤트를 원격으로 사용 가능한지 확인될 때까지 기다립니다. 그런 다음 우선순위가 낮은 연결 이벤트 저장 중지 Management Center를 참조하십시오.

참고 이러한 구성을 변경해야 하는 경우 마법사를 다시 실행합니다. 구성을 비활성화하거나 마법사를 다시 실행하면 계정 자격 증명을 제외한 모든 설정이 유지됩니다.

이벤트 데이터를 데이터 저장소 구축에 전송하도록 **Secure Firewall Management Center** 구성

시작하기 전에

- Secure Firewall Management Center에서 마법사 구성에 나와 있는 모든 요구 사항을 충족하는지 확인합니다.
- 관리 디바이스 버전이 7.0 이상입니다.

단계 **1** management center에서통합 > **Security Analytics & Logging**으로 이동합니다.

단계 **2** 데이터 저장소 위젯에서 시작을 클릭합니다.

단계 **3** 관리자의 호스트 이름이나 IP 주소, 포트를 입력합니다.

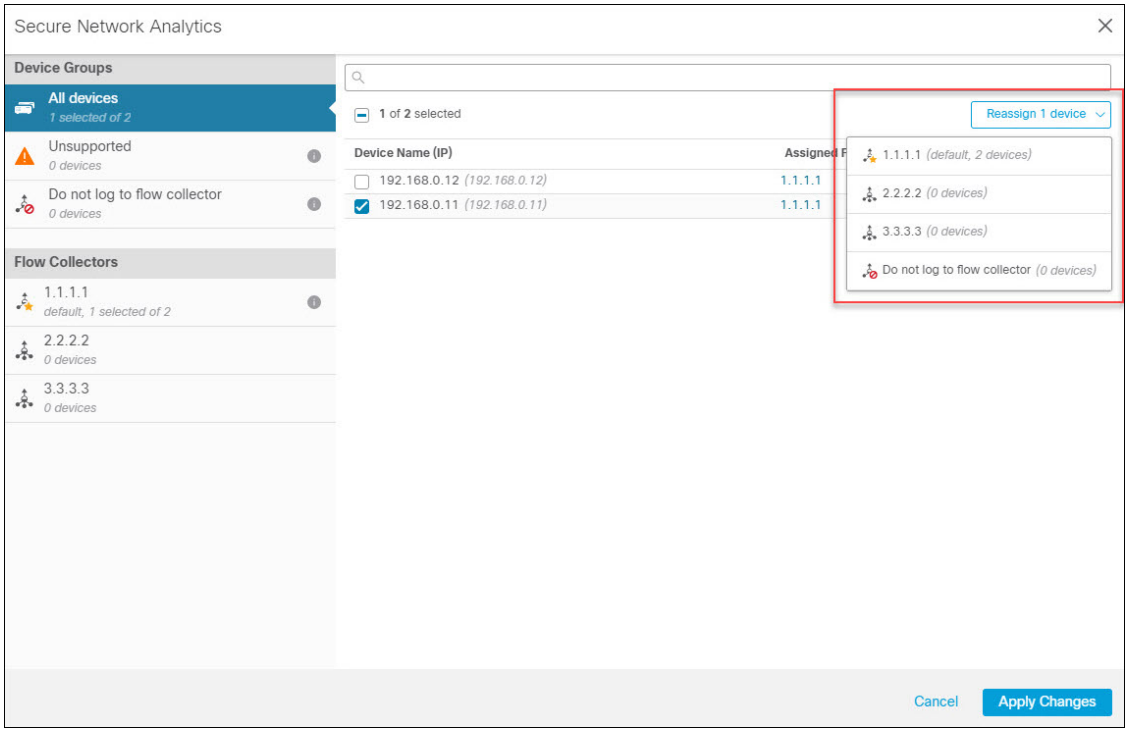
단계 **4** 플로우 컬렉터의 호스트 이름 또는 IP 주소 및 포트를 입력합니다.

플로우 컬렉터를 더 추가하려면 + 다른 플로우 컬렉터 추가를 클릭합니다.

단계 **5** (선택 사항) 둘 이상의 플로우 컬렉터를 구성한 경우 다른 플로우 컬렉터와 관리 디바이스를 연결합니다.

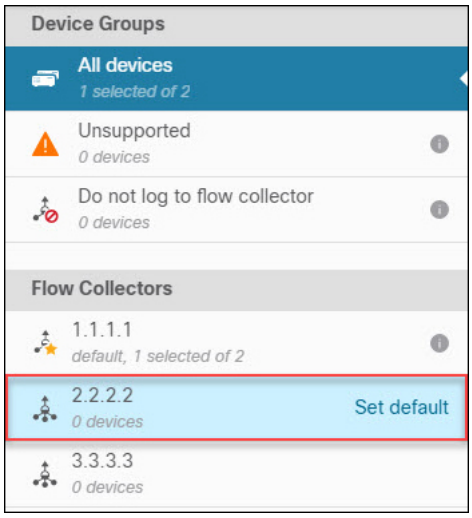
기본적으로 모든 관리 디바이스는 기본 플로우 컬렉터에 할당됩니다.

1. 디바이스 할당을 클릭합니다.
2. 재할당할 관리 디바이스를 선택합니다.
3. 디바이스 재할당 드롭다운 목록에서 플로우 컬렉터를 선택합니다.



관리 디바이스가 플로우 컬렉터에 이벤트 데이터를 전송하지 않도록 하려면 해당 디바이스를 선택하고, 디바이스 재할당 드롭다운 목록에서 플로우 컬렉터에 로깅하지 않음을 선택합니다.

참고 원하는 플로우 컬렉터 위로 마우스를 이동하고 기본값 설정을 클릭하여 기본 플로우 컬렉터를 변경할 수 있습니다.



4. **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 찾은 검색을 확인합니다.

1. 교차 실행 URL 및 포트를 확인하고 필요한 경우 수정합니다.
2. "처음 사용 시 신뢰" 옵션을 사용하지 않으려면 관리자에서 SSL 인증서를 업로드합니다.

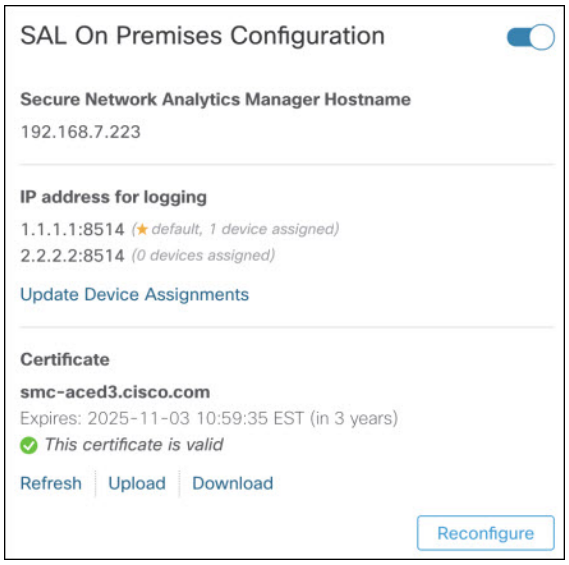
   참고 Cisco Secure Network Analytics: 관리 어플라이언스용 SSL/TLS 인증서에서 SSL 인증서를 획득하고 업로드하는 방법을 자세히 알아보십시오.

3. **Next(**다음**)**를 클릭합니다.

단계 **8** 쿼리에 대한 보안 통신을 설정하기 위해 관리자에 로그인할 자격 증명을 입력하고 완료를 클릭합니다.

이러한 자격 증명은 management center에 저장되지 않습니다. 관리자에서 management center에 대한 읽기 전용 Analyst API 계정을 설정하는 데 한 번 사용됩니다. 이를 위해서는 전용 계정이 필요하지 않습니다. 고유한 관리자 자격 증명을 사용할 수 있습니다.

구성을 저장한 후 **Security Analytics & Logging** 페이지에서 디바이스 할당 업데이트를 클릭하여 디바이스 할당을 업데이트할 수 있습니다.



다음에 수행할 작업

- 시스템 로그를 사용하여 Secure Network Analytics에 데이터 플레인 이벤트 로그를 전송하도록 Secure Firewall Management Center 구성, 22 페이지을(를) 사용하여 데이터 플레인 이벤트 로그 전송을 활성화합니다.
- Secure Network Analytics 어플라이언스에 이벤트가 성공적으로 저장되었음을 확인한 후에는 management center에 저장된 모든 이벤트를 원격으로 사용 가능한지 확인될 때까지 기다립니다. 그런 다음 우선순위가 낮은 연결 이벤트 저장 중지 Management Center를 참조하십시오.

참고 이러한 구성을 변경해야 하는 경우 마법사를 다시 실행합니다. 구성을 비활성화하거나 마법사를 다시 실행하면 계정 자격 증명을 제외한 모든 설정이 유지됩니다.

시스템 로그를 사용하여 **Secure Network Analytics**에 데이터 플레인 이벤트 로그를 전송하도록 **Secure Firewall Management Center** 구성

다음은 어플라이언스 플랫폼 설정 정책의 UI 옵션에서 시스템 로그를 사용하여 데이터 플레인 이벤트 로그를 Secure Network Analytics에 전송하도록 management center을(를) 구성하는 방법을 설명합니다.

참고 데이터 플레인 이벤트는 Security Analytics and Logging(온프레미스) 데이터 저장소 구축에서 지원됩니다.

시작하기 전에

management center에서 Secure Firewall Management Center에서 마법사 구성를 사용하여 Secure Network Analytics에 데이터 플레인 이벤트 로깅 전송을 활성화해야 합니다.

단계 **1** 로깅을 활성화합니다.

a) 시스템 로그 > 로그 설정 > 기본 로그 설정으로 이동합니다.

b) **Enable Logging(**로깅 활성화**)** 확인란을 선택합니다.

단계 **2** 로그 트랩을 구성합니다.

a) 시스템 로그 > 로그 대상으로 이동합니다.

b) + 로그 대상 추가를 클릭합니다.

c) 로그 대상에서 시스템 로그 서버를 선택합니다.

d) 이벤트 클래스에서 심각도에 대한 필터를 선택합니다.

e) 한 가지 심각도를 선택합니다.

단계 **3** 로그 기능을 구성합니다.

a) 시스템 로그 > 시스템 로그 설정 > 기능으로 이동합니다.

b) 기능에서, **default = LOCAL4(20)**을 선택합니다.

우선순위가 낮은 연결 이벤트 저장 중지 **Management Center**

대부분의 연결 이벤트는 식별된 위협과 관련이 없습니다. 이렇게 많은 양의 이벤트를 management center에 저장하지 않도록 선택할 수 있습니다.

management center에 저장되지 않은 이벤트는 https://www.cisco.com/c/en/us/products/collateral/security/%20firesight-management-center/datasheet-c78-736775.html의 데이터 시트에 지정된 대로 management center 어플라이언스의 최대 플로우 속도에 포함되지 않습니다.

다음 연결 이벤트는 높은 우선순위로 간주되며, 연결 이벤트의 스토리지를 비활성화한 경우에도 항상 management center에 저장됩니다.

- 보안 이벤트
- 침입 이벤트와 연관된 연결 이벤트
- 파일 이벤트와 연관된 연결 이벤트
- 악성코드 이벤트와 연관된 연결 이벤트

management center에 우선순위가 낮은 연결 이벤트를 저장하지 않으면 다른 이벤트 유형에 더 많은 스토리지 공간을 할당할 수 있으므로 위협을 조사할 시간이 늘어납니다. 이 설정은 통계 수집에 영향을 주지 않습니다.

이 설정은 management center에서 관리하는 모든 디바이스의 이벤트에 적용됩니다.

시작하기 전에

주의 이 절차를 실행하면 즉시 현재 management center에 저장된 모든 연결 이벤트가 영구적으로 삭제됩니다.

이 절차를 실행하기 전에 유지하려는 모든 낮은 우선순위 연결 이벤트가 Secure Network Analytics 어플라이언스에 있는지 확인합니다. 일반적으로 management center이(가) Secure Network Analytics에 이벤트를 성공적으로 전송하고 있음을 확인한 후 이 옵션을 활성화하는 것이 좋습니다.

단계 **1** management center에서 낮은 우선순위 연결 이벤트의 저장을 중지하는 방법에는 두 가지가 있습니다.

두 방법 모두 동일한 효과를 갖습니다.

- 이벤트를 Security Analytics and Logging(온프레미스)에 전송할 대상 마법사를 완료한 후 **System(**시스템**) > Logging(**기록**) > Security Analytics and Logging(**보안 분석 및 기록**)**으로 이동하여 **FMC**에 더 적은 이벤트를 저장하는 옵션을 활성화합니다.
- **System(**시스템**) > Configuration(**구성**) > Database(**데이터베이스**)**로 이동하여 **Connection Database(**연결 데이터베이스**)** 섹션에서 **Maximum Connection Events(**최대 연결 이벤트**)**를 `0`으로 설정합니다.

  이 값을 0 이외의 값으로 설정하면 낮은 우선순위 연결 이벤트가 모두 최대 플로우 속도에 포함됩니다. 이 설정은 연결 요약에 영향을 주지 않습니다.

단계 **2** 변경 내용을 저장합니다.

다음에 수행할 작업

System(시스템**) > Configuration(**구성**) > Database(**데이터베이스**)** 페이지에서 다른 모든 이벤트 유형에 대한 스토리지 제한을 늘립니다.

ASA 디바이스 구성

ASA 시스템 로그는 ASA 디바이스의 모니터링 및 문제 해결에 필요한 정보를 제공합니다. Cisco ASA Series 시스템 로그 메시지에서 ASA 이벤트 유형 목록을 참고하십시오.

참고 ASA 이벤트 스토리지는 Security Analytics and Logging(온프레미스) 데이터 저장소 구축에서 지원됩니다.

ASA에서 시스템 로그 이벤트를 Security Analytics and Logging(온프레미스)에 전송하게 하려면 ASA 디바이스에 로깅을 설정해야 합니다.

- 로깅 활성화

- Secure Network Analytics 플로우 컬렉터로 출력 대상 설정

참고 Security Analytics and Logging(온프레미스)에 대한 보안 로깅은 지원되지 않습니다.

ASA 디바이스에서 시스템 로그 이벤트를 전송하는 CLI 명령

다음 구성 명령을 사용하여 ASA 장치에서 Security Analytics and Logging(온프레미스)(으)로 보안 이벤트에 대한 시스템 로그 메시지를 보냅니다.

시작하기 전에

- 요구 사항 및 사전 요건 섹션을 검토합니다.
- ASA 디바이스가 플로우 컬렉터에 연결할 수 있는지 확인합니다.
- 관리자의 Central Management에서 플로우 컬렉터 IP 주소 및 포트 번호를 가져옵니다.

단계 **1** 로깅을 활성화합니다.

logging enable

예제**:**

```
ciscoasa(config)# logging enable
```

단계 **2** 어떤 시스템 로그 메시지를 시스템 로그 서버(플로우 컬렉터)에 전송할지 지정합니다.

logging trap {*severity_level* | *message_list*}

예제**:**

플로우 컬렉터로 보낼 시스템 로그 메시지의 심각도 레벨 숫자(1~7) 또는 이름을 지정할 수 있습니다.

```
ciscoasa(config)# logging trap errors
```

예제**:**

또는 플로우 컬렉터로 보낼 시스템 로그 메시지를 식별하는 사용자 정의 메시지 목록을 지정할 수도 있습니다.

```
ciscoasa(config)# logging list specific_event_list message 106100
ciscoasa(config)# logging list specific_event_list message 302013-302018
ciscoasa(config)# logging trap specific_event_list
```

단계 **3** 플로우 컬렉터로 메시지를 전송하도록 ASA를 구성합니다.

logging host *interface_name syslog_ip* [**protocol**/*port*]

예제**:**

```
ciscoasa(config)# logging host management 209.165.201.3 17/8514
```

참고
1. 시스템 로그 IP 및 포트의 경우 플로우 컬렉터 IP 및 해당 시스템 로그 포트 번호를 지정합니다(시작하기 전에 섹션의 해당 지침 참조).
2. UDP 프로토콜을 나타내려면 *17*을 지정합니다.

단계 **4** (선택 사항) 시스템 로그 메시지에서 타임스탬프 형식을 설정합니다.

logging timestamp *{rfc5424}*

예제**:**

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# logging timestamp rfc5424
```

RFC5424에 지정된 타임스탬프 형식은 yyyy-MM-THH:mm:ssZ입니다. 여기서 Z는 UTC 표준 시간대를 나타냅니다.

참고 RFC5424는 ASA 9.10(1)에서만 지원됩니다.

단계 **5** (선택 사항) 디바이스 ID와 함께 시스템 로그 메시지를 표시하도록 ASA를 설정합니다.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

예제**:**

```
ciscoasa(config)# logging device-id context-name
```

syslog 서버는 디바이스 ID를 사용하여 syslog 생성기를 식별합니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다.

ASA 디바이스에서 시스템 로그 이벤트를 전송하는 ASDM 설정

이 절차에서는 Security Analytics and Logging(온프레미스)에 보안 이벤트에 대한 ASA 시스템 로그 메시지를 전송하는 ASDM 설정을 설명합니다.

시작하기 전에

- 요구 사항 및 사전 요건 섹션을 검토합니다.
- ASA 디바이스가 플로우 컬렉터에 연결할 수 있는지 확인합니다.
- 관리자의 Central Management에서 플로우 컬렉터 IP 주소 및 포트 번호를 가져옵니다.

단계 **1** ASDM에 로그인합니다.

단계 **2** 로깅을 활성화합니다.

a) **Configuration(**설정**)** > **Device Management(**디바이스 관리**)** > **Logging(**기록**)** > **Logging Setup(**기록 설정**)** 을 클릭합니다.

b) **Enable logging(**로깅 활성화**)** 확인란을 선택하여 로깅을 켭니다.

c) (선택 사항) **Send syslogs in EMBLEM(EMBLEM**으로 **syslogs** 전송**)** 확인란을 선택하여 EMBLEM 로깅 형식을 활성화합니다.

단계 **3** 시스템 로그 서버(플로우 컬렉터)의 로깅 필터 설정을 구성합니다.

a) **Configuration(**설정**)** > **Device Management(**디바이스 관리**)** > **Logging(**기록**)** > **Logging Filters(**필터 기록**)**를 선택합니다.

b) 테이블에서 **Syslog Servers(**시스템 로그 서버**)**를 선택한 다음 **Edit(**편집**)**를 클릭합니다.

c) **Edit Logging Filters(**로깅 필터 편집**)** 대화 상자에서 다음 로깅 필터 설정 중 하나를 선택합니다.

시스템 로그 메시지를 심각도 레벨을 기준으로 필터링하려면 **Filter on severity(**심각도에 따라 필터링**)**를 클릭한 다음 심각도 레벨을 선택합니다.

참고 ASA는 심각도 레벨이 지정된 레벨 이하인 시스템 로그 메시지를 생성합니다.

또는

시스템 로그 메시지를 메시지 ID를 기준으로 필터링하려면 **Use event list(**이벤트 목록 사용**)**를 클릭합니다. 필수 시스템 로그 메시지 ID를 사용하여 생성한 이벤트 목록을 선택하거나 **New(**새로 만들기**)**를 클릭하여 시스템 로그 메시지 ID 또는 ID 범위로 목록을 생성할 수 있습니다.

d) 설정을 저장합니다.

단계 **4** 플로우 컬렉터 주소 및 포트를 사용하여 외부 시스템 로그 서버를 설정합니다.

a) **Configuration(**설정**)** > **Device Management(**디바이스 관리**)** > **Logging(**기록**)** > **Syslog Server(**시스템 로그 서버**)**를 선택합니다.

b) **Add(**추가**)**를 클릭하여 새 syslog 서버를 추가합니다.

c) **Add Syslog Server(**시스템 로그 서버 추가**)** 대화 상자에서 다음을 지정합니다.

- 인터페이스 - 시스템 로그 서버와 통신하는 데 사용할 인터페이스입니다.
- **IP Address(IP** 주소**)** - 관리자의 Central Management에서 가져온 플로우 컬렉터 IP입니다.
- 프로토콜 - UDP를 선택합니다.
- 포트 - 해당 플로우 컬렉터 시스템 로그 포트(기본값: 8514)입니다.
- (선택 사항) **Log messages in Cisco EMBLEM format(Cisco EMBLEM** 형식으로 메시지 로깅**)** 확인란을 선택하여 EMBLEM 로깅 형식을 활성화합니다.

단계 **5** **Save(**저장**)**를 클릭하여 설정 변경 사항을 저장합니다.

ASA 디바이스에서 시스템 로그 이벤트를 전송하도록 CSM 설정

보안 이벤트에 대한 ASA 시스템 로그 메시지를 Security Analytics and Logging(온프레미스)에 전송하려면 아래의 CSM(Cisco Security Manager) 구성 절차를 사용합니다.

시작하기 전에

- 요구 사항 및 사전 요건 섹션을 검토합니다.
- ASA 디바이스가 플로우 컬렉터에 연결할 수 있는지 확인합니다.
- 관리자의 Central Management에서 플로우 컬렉터 IP 주소 및 포트 번호를 가져옵니다.
- 이 통합에 대한 보안 로깅은 지원되지 않습니다.

단계 **1** Cisco Security Manager의 **Configuration Manager** 창에 로그인합니다.

단계 **2** 시스템 로그 로깅을 활성화합니다.

a) Syslog Logging Setup(시스템 로그 기록 설정) 페이지에 액세스하려면 다음 중 하나를 수행합니다.

- (디바이스 보기) 정책 선택기에서 **Policy(**정책**)** > **Logging(**기록**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**을 선택합니다.
- (정책 보기) 정책 유형 선택기에서 **Router Platform(**라우터 플랫폼**)** > **Logging(**기록**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**을 선택합니다. 기존 정책을 선택하거나 새 정책을 생성합니다.

b) Syslog Logging Setup(시스템 로그 기록 설정) 페이지에서 **Enable Logging(**기록 활성화**)** 체크 박스를 선택하여 시스템 로그 기록 기능을 켭니다.

c) (선택 사항) **Send syslogs in EMBLEM(EMBLEM**으로 **syslogs** 전송**)** 확인란을 선택하여 EMBLEM 로깅 형식을 활성화합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **3** 시스템 로그 서버(플로우 컬렉터)의 로깅 필터 설정을 구성합니다.

a) 정책 선택기에서 **Platform(**플랫폼**)** > **Logging(**기록**)** > **Syslog(**시스템 로그**)** > **Logging Filters(**기록 필터**)**를 선택합니다.

b) 테이블의 **Logging Destination(**기록 대상**)**에서 **Syslog Servers(**시스템 로그 서버**)**를 선택한 다음 **Edit(**편집**)**를 클릭합니다. 시스템 로그 서버 개체가 없으면 **Add Row(**행추가**)**를 클릭합니다.

c) **Add/Edit Logging Filters(**로깅 필터 추가/편집**)** 대화 상자에서 다음 로깅 필터 설정 중 하나를 선택합니다.

- 시스템 로그 메시지를 심각도 레벨을 기준으로 필터링하려면 **Filter on severity(**심각도에 따라 필터링**)**를 클릭한 다음 심각도 레벨을 선택합니다.

  참고 ASA는 심각도 레벨이 지정된 레벨 이하인 시스템 로그 메시지를 생성합니다.

- 메시지 ID에 따라 시스템 로그 메시지를 필터링하려면 드롭다운 목록에서 **Use event list(**이벤트 목록 사용**)**를 클릭하고 선택한 이벤트 목록을 선택합니다.

참고 이벤트 목록을 정의하지 않은 경우 드롭다운 목록이 비어 있습니다. 이벤트 목록을 한 개 이상 정의해야 합니다(**Platform(**플랫폼**)** > **Logging(**로깅**)** > **Syslog(**시스템 로그**)** > **Event Lists(**이벤트 목록**)**).

d) 설정을 저장합니다.

단계 **4** (선택 사항) 로깅 매개변수를 설정합니다.

a) (디바이스보기) **Platform(**플랫폼**)** > **Logging(**기록**)** > **Syslog(**시스템 로그**)** > **Server Setup(**서버 설정**)**을 선택합니다.

b) 시스템 로그 메시지에 타임스탬프 형식을 설정하려면 **Enable Timestamp on each Syslog Message(**각 시스템 로그 메시지에서 타임스탬프 활성화**)** 체크 박스를 선택한 다음 **Enable Timestamp Format(rfc5424)(**타임스탬프 형식 활성화**(rfc5424))** 체크 박스를 선택합니다.

참고 RFC5424는 ASA 9.10(1)에서만 지원됩니다.

c) (선택 사항) 디바이스 ID와 함께 시스템 로그 메시지를 표시하도록 ASA를 설정합니다.

- **Interface(**인터페이스**)** - 이 라디오 버튼을 클릭하고 ASA 디바이스의 인터페이스를 선택합니다.
- **User Defined ID(**사용자 정의 **ID)** - 이 라디오 버튼을 클릭하고 ASA 디바이스의 모든 시스템 로그 메시지에 추가할 원하는 이름을 입력합니다.
- **Host Name(**호스트 이름**)** - 디바이스 호스트네임과 함께 시스템 로그 메시지를 표시하려면 이 라디오 버튼을 클릭합니다.

참고 syslog 서버는 디바이스 ID를 사용하여 syslog 생성기를 식별합니다. syslog 메시지에 대해 1가지 디바이스 ID 유형만 지정할 수 있습니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **5** 시스템 로그 메시지를 전송할 외부 로그 서버를 설정합니다.

a) 시스템 로그 서버 페이지에 액세스하려면 다음 중 하나를 수행합니다.

- (디바이스 보기) 정책 선택기에서 **Platform(**플랫폼**)** > **Logging(**기록**)** > **Syslog Servers(**시스템 로그 서버**)**를 선택합니다.
- (정책 보기) 정책 유형 선택기에서 **Router Platform(**라우터 플랫폼**)** > **Logging(**기록**)** > **Syslog Servers(**시스템 로그 서버**)**를 선택합니다. 기존 정책을 선택하거나 새 정책을 생성합니다.

b) **Add(**추가**)**를 클릭하여 새 syslog 서버를 추가합니다.

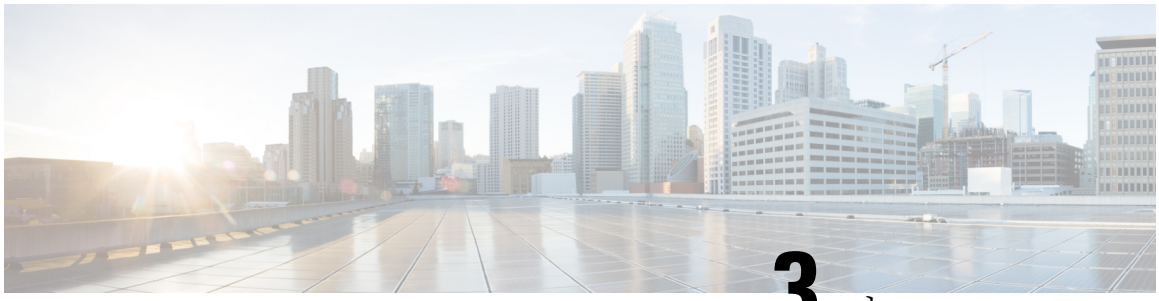
c) **Add/Edit Syslog Server(**시스템 로그 서버 추가/편집**)** 대화 상자에서 다음을 지정합니다.

- 인터페이스 - 시스템 로그 서버와 통신하는 데 사용하는 인터페이스입니다.
- **IP Address(IP** 주소**)** - 관리자의 Central Management에서 가져온 플로우 컬렉터 IP입니다.
- 프로토콜 - UDP를 선택합니다.
- 포트 - 해당 플로우 컬렉터 시스템 로그 포트(기본값: 8514)입니다.

- (선택 사항) **Log messages in Cisco EMBLEM format(Cisco EMBLEM** 형식으로 메시지 로깅**)** 확인란을 선택하여 EMBLEM 로깅 형식을 활성화합니다.

d) **OK(**확인**)**를 클릭하여 설정을 저장하고 대화 상자를 닫습니다. 정의한 시스템 로그 서버가 테이블에 표시됩니다.

단계 **6** 설정 변경 사항을 제출 및 구축합니다.



3 장

다음 단계

다음 단계

Security Analytics and Logging(온프레미스)의 일부로 Secure Network Analytics 어플라이언스에 이벤트 데이터를 전송하도록 방화벽 디바이스를 구성한 후 다음 단계를 수행할 수 있습니다.

- management center 온라인 도움말을 검토합니다.
- 관리자웹 애플리케이션 온라인 도움말Secure Network Analytics에서 자세한 내용을 참고하십시오.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Management Center에서 작업

디바이스가 Security Analytics and Logging(온프레미스)을(를) 사용하여 Secure Network Analytics 어플라이언스에 연결 이벤트를 전송하는 경우, management center의 이벤트 뷰어 및 상황 탐색기에서 원격으로 저장된 이벤트를 확인하고 작업을 수행하고 보고서를 생성할 때 해당 이벤트를 포함할 수 있습니다. management center의 이벤트에서 교차 실행하여 Secure Network Analytics 어플라이언스의 관련 데이터를 볼 수도 있습니다.

기본적으로 시스템은 사용자가 지정한 시간 범위에 따라 적절한 데이터 소스를 자동으로 선택합니다. 데이터 소스를 재정의하려는 경우 이 절차를 사용합니다.

중요 데이터 소스를 변경하는 경우 로그아웃한 후에도 변경 사항이 있을 때까지 보고서를 포함하여 이벤트 데이터 소스를 사용하는 모든 관련 분석 기능에서 선택 사항이 유지됩니다. 다른 management center 사용자에게는 선택 항목이 적용되지 않습니다.

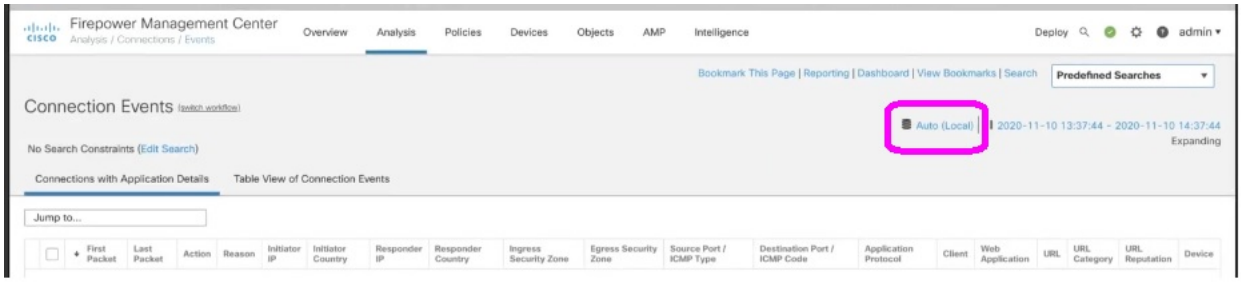
선택한 데이터 소스는 우선순위가 낮은 연결 이벤트에만 사용됩니다. 기타 모든 이벤트 유형(침입, 파일 및 악성 코드 이벤트, 해당 이벤트와 연결된 연결 이벤트, 보안 인텔리전스 이벤트)은 데이터 소스에 관계 없이 표시됩니다.

시작하기 전에

마법사를 사용하여 연결 이벤트를 Security Analytics and Logging(온프레미스)에 보냈습니다.

단계 **1** management center 웹 인터페이스에서 **Analysis(분석) > Connections(연결) > Events(이벤트)**와 같은 연결 이벤트 데이터를 표시하는 페이지로 이동합니다.

단계 **2** 여기에 표시된 데이터 소스를 클릭하고 옵션을 선택합니다.



주의 **Local(로컬)**을 선택하면 선택한 전체 시간 범위에 대해 로컬 데이터를 사용할 수 없는 경우에도 management center에서 사용 가능한 데이터만 표시됩니다. 이러한 상황이 발생했다는 알림이 표시되지 않습니다.

단계 **3** (선택 사항) Secure Network Analytics 어플라이언스에서 관련 데이터를 직접 보려면 IP 주소 또는 도메인과 같은 값을 마우스 오른쪽 버튼으로 클릭(통합 이벤트 뷰어에서 클릭)하고 교차 실행 옵션을 선택합니다.

교차 실행을 이용한 이벤트 조사

management center에서 이벤트를 볼 때 특정 이벤트 데이터(예: IP 주소)를 마우스 오른쪽 버튼으로 클릭하고 관리자에서 관련 데이터를 볼 수 있습니다.

단계 **1** 이벤트를 표시하는 management center의 다음 페이지 중 하나로 이동합니다.

- 대시보드(**Overview(개요) > Dashboards(대시보드)**) 또는
- 이벤트 뷰어 페이지(이벤트의 테이블을 포함하는 분석 메뉴에서 아무 메뉴 옵션).

단계 **2** 관심 있는 이벤트를 오른쪽으로 클릭하고 사용할 Security Analytics and Logging(온프레미스) 교차 실행 리소스를 선택합니다. 별도의 브라우저 창에 관리자이(가) 열립니다. 아직 로그인하지 않은 경우 사용자 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다. 쿼리하는 데이터의 양, 관리자의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

단계 **3** 관리자에 로그인합니다.

A 부록

문제 해결

문제 해결

Security Analytics and Logging(온프레미스**)** 일반 문제 해결

관리자의 다음 로그 파일에는 Security Analytics and Logging(온프레미스)와 관련된 문제 해결 정보가 포함되어 있습니다.

- `/lancope/var/logs/containers/sal.log` - 일반 애플리케이션 로깅 정보(관리자 전용 구축 전용)
- `/lancope/var/logs/sal_preinstall.log` - 애플리케이션 설치 프로세스와 관련된 정보

플로우 컬렉터에서 다음 로그 파일에는 Security Analytics and Logging(온프레미스) 데이터 저장소 구축과 관련된 문제 해결 정보가 포함되어 있습니다.

- `lancope/var/sw/today/logs/sw.log` - 텔레메트리 로깅 관련 정보
- `/lancope/var/logs/containers/svc-db-ingest.log` - 이벤트 수집 및 데이터베이스 관련 정보

플로우 컬렉터 고급 설정을 사용하는 **Security Analytics and Logging(**온프레미스**)** 구성**(**데이터 저장소에만 해당**)**

최초 설정 중에 방화벽 로그를 저장하지 않도록 플로우 컬렉터를 구성한 경우, 플로우 컬렉터 고급 설정 페이지를 사용하여 수집 설정을 업데이트할 수 있습니다. 고급 설정에 액세스하려면 다음과 같이 합니다.

1. 플로우 컬렉터(이전의 어플라이언스 관리(Admin) 인터페이스)에 로그인합니다.
2. 지원 > 고급 설정을 클릭합니다.
3. 방화벽 이벤트 로그 수집을 활성화하려면 **enable_sal** 필드에 1을 입력합니다.
4. 방화벽 로그에 대한 포트를 변경하려면 **sal_syslog_port** 필드에 새 값을 입력합니다(기본 포트는 8514).
5. 적용 을 클릭한 다음 확인을 클릭합니다.

관리자 전용 구축 시 **Security Analytics and Logging**(온프레미스) 앱 설치 실패

독립형 어플라이언스(관리자 전용)인 관리자에 또는 플로우 컬렉터 및 데이터 노드(데이터 저장소)를 관리하는 관리자에 애플리케이션 설치를 지원합니다. 하나 이상의 플로우 컬렉터를 관리하고 데이터 저장소를 관리하지 않는 경우 관리자에 앱을 설치할 수 없습니다. 이 상황에서 앱을 설치하려고 하면 설치에 실패합니다. 이것이 원인인지 확인하려면 `/lancope/var/logs/sal_preinstall.log`에서 로그 파일을 검토합니다. 다음 메시지 또는 이와 유사한 메시지가 표시되면 설치에서 관리되는 플로우 컬렉터를 탐지한 것입니다.

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

앱을 설치하려면 Central 관리자 어플라이언스 인벤토리에서 관리되는 플로우 컬렉터를 모두 제거한 다음 다시 시도하십시오.

⚠

주의 관리자 전용 구축이 있는 경우 Security Analytics and Logging(온프레미스) 앱을 제거하면 관리자에서 이벤트 데이터를 비롯한 모든 관련 정보가 삭제되고 독립형 관리자 제한이 제거됩니다. Security Analytics and Logging(온프레미스) 애플리케이션을 제거한 후에는 트래픽을 검사하기 위해 기존 Secure Network Analytics 구축의 일부로 관리자을(를) 사용하여 하나 이상의 플로우 컬렉터를 관리할 수 있습니다.

Security Analytics and Logging(온프레미스) 앱 삭제 이벤트

앱은 다음과 같은 상황에서 이벤트를 삭제할 수 있습니다.

- 연결, 파일, 악성코드 및 침입 이벤트만이 아니라 모든 이벤트 유형을 시스템 로그로 내보냅니다.
- EPS(average events per second) 수집 속도 또는 버스트 EPS 수집 속도가 Secure Network Analytics 리소스 배정 섹션의 권장 사양을 초과합니다.

관리자 전용 구축의 경우 관리자에서 `/lancope/var/logs/containers/sal.log` 로그 파일의 정보를 검토하여 앱이 이벤트를 삭제하는지 확인합니다. "`events_dropped:`"를 포함하는 항목에 대한 파일을 검색합니다.

데이터 저장소 구축의 경우 플로우 컬렉터에서 `lancope/var/sw/today/logs/sw.log` 로그 파일의 정보를 검토하여 애플리케이션이 이벤트를 삭제하는지 확인합니다. 파일에서 "`sal_event`"를 포함하는 항목을 검색합니다.

이러한 작동이 계속될 경우 Cisco 지원팀에 문의하십시오.

Security Analytics and Logging(온프레미스) 앱 충돌

Security Analytics and Logging(온프레미스) 앱이 충돌하는 경우(예: 과도한 수집 속도로 인해) 관리자을(를) 다시 시작합니다. 이렇게 하면 앱도 다시 시작됩니다.

⚠

주의 앱을 제거하지 마십시오. 관리자 전용 구축이 있는 경우 Security Analytics and Logging(온프레미스) 앱을 제거하면 이벤트 데이터를 비롯한 모든 관련 정보가 관리자에서 삭제됩니다.