Cisco Secure Network Analytics

시스템 설정 가이드 7.4.2

목차

소개

개요

이 가이드를 사용하여 v7.4.2에서 다음의 Cisco Secure Network Analytics(이전 Stealthwatch) 하드웨어 및 Virtual Edition 어플라이언스를 하나의 매니지드 시스템에 구성합니다.

- Cisco Secure Network Analytics 관리자 (이전 Stealthwatch 관리 콘솔)
- Cisco Secure Network Analytics 데이터 노드
- Cisco Secure Network Analytics 플로우 컬렉터
- Cisco Secure Network Analytics 플로우 센서
- Cisco Secure Network Analytics UDP 디렉터

Secure Network Analytics에 대한 자세한 내용은 다음 온라인 리소스를 참조하십시오.

- **개요:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **어플라이언스:** https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html
- **릴리스 노트:** 자세한 내용은 릴리스 노트를 참조하십시오.

대상

이 가이드는 네트워크 관리자와 Secure Network Analytics 제품 설치 및 구성을 담당하는 기타 직원을 대상으로 합니다.

전문 설치자의 도움을 받길 원하는 경우 로컬 Cisco 파트너 또는 Cisco 지원팀에 문의하십시오.

설치 요구 사항

이 가이드를 사용하여 관리되는 시스템에 Secure Network Analytics를 구성하기 전에 다음 가이드를 사용하여 하드웨어 및 가상 어플라이언스를 설치합니다.

하드웨어

- **하드웨어 설치:** 이 구성을 시작하기 전에 Secure Network Analyticsx2xx Series 하드웨어 설치 가이드 또는 Secure Network Analyticsx3xx Series 하드웨어 설치 가이드를 사용하여 어플라이언스 하드웨어(물리적 어플라이언스)를 설치합니다.
- **사양:** 하드웨어 사양은 Cisco.com에서 확인할 수 있습니다.
- **지원되는 플랫폼:** 각 시스템 버전에 대해 지원되는 하드웨어 플랫폼을 보려면 Cisco.com의 하드웨어 및 소프트웨어 버전 지원 매트릭스를 참조하십시오.

VE(Virtual Edition) 어플라이언스

- **Virtual Edition 설치:** 이 구성을 시작하기 전에 Secure Network AnalyticsVirtual Edition 설치 가이드를 사용하여 가상 어플라이언스를 설치합니다.

빠른 참조 개요

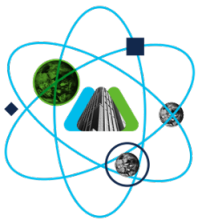
성공적으로 설치하려면 다음 절차를 순서대로 수행합니다. 자세한 지침을 보려면 절차 링크를 클릭합니다.

시작하기 전에 및 시스템 구성 계획

어플라이언스를 구성하고 데이터 저장소와 함께 또는 데이터 저장소 없이 구축하려면 필요한 모든 정보가 있어야 합니다.Secure Network Analytics

1. 최초 설정을 사용하여 환경 구성

- **로그인:** 콘솔을 통해 각 어플라이언스에 sysadmin으로 로그인합니다 (비밀번호: lan1cope). 명령 프롬프트에서 `SystemConfig`를 입력합니다.
- 데이터 저장소가 있는 플로우 컬렉터: root로 로그인(비밀번호: lan1cope)
- **필수 어플라이언스:**관리자이며 플로우 컬렉터은 모든 구축에 필요합니다. 데이터 저장소가 있는 구축의 경우에는 (상호 데이터 노드 통신이 있는) 데이터 노드를 구성해야 합니다.



2. 매니지드 시스템 구성

어플라이언스 설정 도구를 사용하여 매니저에서 관리할 수 있도록 각 어플라이언스를 순서대로 구성합니다. 어플라이언스에 대해 데이터 저장소 도메인 또는 비데이터 저장소 도메인도 생성합니다.

- **어플라이언스 설정 도구:**브라우저의 주소 필드에 **https://** 를 입력한 후 어플라이언스의 IP 주소를 입력합니다.
- **로그인:** admin
- **비밀번호:** lan411cope
- **Sysadmin 및 Root 비밀번호 기본값:** lan1cope

어플라이언스를 순서대로 구성합니다. Central Management 인벤토리를 확인하고 각 어플라이언스 상태가 **Connected(연결됨)**(또는 **데이터 저장소가 초기화되지 않음**)인지 확인한 다음 클러스터의 다음 어플라이언스 구성을 시작합니다.

1. 기본 매니저(Central Management)
2. 데이터 노드

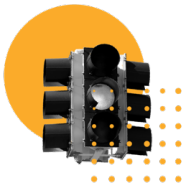
3. Flow Collector 5000 Series 데이터베이스
4. Flow Collector 5000 Series 엔진
5. 기타 모든 플로우 컬렉터
6. UDP Director
7. Flow Sensor
8. 보조 매니저

3. 매니저 페일오버 관계

- 이 절차는 기본 매니저 및 보조 매니저를 구성한 경우에 필요합니다.
- 페일오버가 두 개의 매니저 간 페일오버 쌍을 설정하여 그 중 하나가 다른 하나의 백업 콘솔로 사용되도록 할 수 있습니다.
- Secure Network Analytics페일오버 구성 가이드의 지침을 따르십시오.

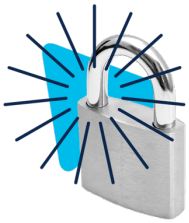
4. 사이트 이중화 구성

- 이 절차는 선택 사항이며 데이터스토어이 있어야 합니다.
- 사이트 이중화를 사용하면 유사한 어플라이언스로 별도 구축된 두 Cisco Secure Network Analytics 사이트의 클러스터에서 이중화에 가까운 방식을 설정할 수 있습니다.



5. v7.4.2 패치 설치

- https://software.cisco.com에서 Cisco Software Central의 Cisco 스마트 어카운트에서 최신 **v7.4.2 패치**를 다운로드합니다.
- 패치 readme 파일의 지침에 따라 각 패치를 설치합니다.



6. 초기화 데이터스토어

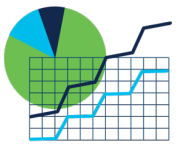
구축에만 필요합니다.데이터스토어

1. 매니저 어플라이언스 콘솔(SystemConfig)에 root로 로그인합니다.
2. **Data Store(데이터 저장소)** > **SSH**를 선택합니다.
3. 데이터 저장소 - 초기화를 선택합니다.

7. 데스크톱 클라이언트 설치

비데이터 저장소 구축에만 필요합니다.

- 데스크톱 클라이언트에는 64비트 운영 체제가 필요합니다. 32비트 운영 체제 또는 Linux에서 실행할 수 없습니다.
- 매니저다음에 로그인합니다. (**다운로드**) 아이콘를 클릭합니다.



8. 통신 확인

- 매니저다음에 로그인합니다. 플로우 수집 트렌드 검토
- 데이터스토어 데이터베이스 상태를 검토하여 작동 상태인지 확인합니다. (구성 > 전역 Central Management > 데이터 저장소 탭)
- 보고서 작성기에서 보고서를 실행하여 플로우 컬렉터 및 데이터 저장소에 플로우가 수신되는지 확인합니다. (보고서 > 보고서 작성기 > 플로우 컬렉터별 플로우 수집 트렌드 보고서, 플로우 데이터베이스 수집 트렌드 보고서)

9. 어플라이언스 구성 종료

- 플로우 센서 애플리케이션 ID 및 페이로드(모든 플로우 센서에 필요)
- UDP Director 고가용성
- 기타 선택적 어플라이언스 설정

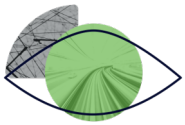
10. 텔레메트리 구성

추가 텔레메트리 유형이 활성화된 데이터스토어 구축에 필요합니다.

- **NVM 플로우:** 엔드포인트 라이선스 및 NVM(Network Visibility Module) 구성 가이드의 지침을 따르십시오.
- **방화벽 로그:** 보안 분석 및 로깅: 방화벽 이벤트 통합 가이드의 지침을 따르고 매니저에 앱을 설치합니다.

11. 라이선싱 Secure Network Analytics

- 90일 평가 기간이 만료되기 전에 https://software.cisco.com에서 Cisco 스마트 어카운트에 제품 인스턴스를 등록하십시오.
- Secure Network Analytics스마트 소프트웨어 라이선싱 가이드의 지침을 따르십시오.



12. 관리 Secure Network Analytics

매니저에 로그인하고 다음을 선택합니다.

- **호스트 그룹:** 구성 > 호스트 그룹 관리 탐지
- **정책:** 구성 > 정책 관리 탐지
- **플로우 검색**: Investigate(조사) > Flow Search(플로우 검색)
- **보고서:** Dashboards(대시보드) > Report Builder(보고서 작성기)
- **사용자 관리:** Configure(구성) > GLOBAL User Management(전역 사용자 관리)
- **지침:** 아무 페이지에서 ? (**도움말**) 아이콘 > **Help(도움말)**을 선택합니다. 또한 환경 관리, 동작 조사, 위협에 대응을 참조하십시오.

다음을 포함한 추가 설정, 유지 보수, 문제 해결에 대해 알아보려면 이 가이드를 참조하십시오.

- 분석
- 애플리케이션
- 인증/권한 부여
- 도메인
- 비밀번호
- SSL/TLS 어플라이언스 ID 및 추가 SSL/TLS 클라이언트 ID
- 위협 피드
- Central Management(어플라이언스 관리)
- 데이터 저장소 데이터베이스
- 데이터 저장소 유지 관리
- 비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터
- 문제 해결

시작하기 전에

구성 프로세스를 시작하기 전에 이 가이드를 검토하여 구성 계획에 필요한 프로세스와 준비 사항, 시간 및 리소스를 파악합니다.

용어

이 가이드에서는 플로우 센서 VE(Virtual Edition)과 같은 가상 제품을 포함하여 모든 Secure Network Analytics 제품에 대해 "**어플라이언스**"라는 용어를 사용합니다.

"**클러스터**"는 매니저에서 관리하는 Secure Network Analytics 어플라이언스의 그룹입니다.

약어

이 가이드에는 다음 약어가 나와 있습니다.

약어	정의
DNS	Domain Name System(서비스 또는 서버)
dvPort	Distributed Virtual Port(분산된 가상 포트)
ESX	엔터프라이즈 서버 X
GB	Gigabyte(기가바이트)
IDS	Intrusion Detection System(침입 탐지 시스템)
IPS	Intrusion Prevention System(침입 방지 시스템)
ISO	국제 표준화 기구(ISO, International Standards Organization)
IT	Information Technology(정보 기술)
KVM	KVM(Kernel-based Virtual Machine)
MTU	Maximum Transmission Unit(최대 전송 단위)
NTP	Network Time Protocol(네트워크 타이밍 프로토콜)
TB	Terabyte(테라바이트)
UUID	Universally Unique Identifier(범용 고유 식별자)
VDS	vNetwork Distributed Switch(vNetwork 분산형 스위치)

약어	정의
VE	Virtual Edition(가상 버전)
VLAN	Virtual Local Area Network
VM	Virtual Machine(가상 머신)

컨피그레이션 세부사항

Secure Network Analytics 시스템 구성에는 다음이 포함됩니다.

- **요구 사항:** 데이터 저장소가 있거나 데이터 저장소가 없는 경우, 또는 하이브리드 구축(데이터 저장소 및 비데이터 저장소 도메인 모두)으로 Secure Network Analytics를 구성할 수 있습니다. 어플라이언스 구성 및 도메인 요구 사항을 검토하려면 **시스템 구성 계획**을 참조하십시오.
- **구성 순서:** 이 가이드의 다음 지침에 따라 어플라이언스 설정 도구에 지정된 순서로 어플라이언스를 구성해야 합니다.
- **인증서:** 어플라이언스는 고유한 자체 서명 어플라이언스 ID 인증서를 사용해 설치됩니다.
- **Central Management:** 기본 매니저/Central Manager에서 어플라이언스를 관리할 수 있습니다.

소프트웨어 다운로드

Cisco Software Central을 사용하여 VE(Virtual Appliance) 설치 파일, 패치 및 소프트웨어 업데이트 파일을 다운로드합니다. https://software.cisco.com에서 Cisco Smart Account에 로그인하거나 관리자에 문의합니다.

비밀번호 요구 사항

시스템 구성 중에 기본 비밀번호를 대체하고 다음에 대해 새 비밀번호를 생성합니다.

사용자	기본 비밀번호
관리자	lan411cope
root	lan1cope
sysadmin	lan1cope
dbadmin	데이터스토어를 초기화할 때 비밀번호를 할당합니다.

readonlyuser	데이터스토어를 초기화할 때 비밀번호를 할당합니다.
CIMC admin	하드웨어 어플라이언스에 대한 원격 액세스를 위해 CIMC다음에 로그인합니다. CIMC를 아직 구성하지 않은 경우 Cisco UCS C Series 통합 관리 컨트롤러 GUI 구성 가이드의 지침을 따르십시오. 기본 비밀번호는 **password**입니다. 처음 로그인할 때 비밀번호를 변경하십시오.

라이선싱

Secure Network Analytics 라이선싱을 위해 Smart Account를 사용해 제품 인스턴스를 등록하고, 라이선스를 관리하고, 보고서를 실행하고 알림을 구성할 수 있습니다. https://software.cisco.com에서 Cisco Smart Account에 로그인하거나 관리자에 문의합니다.

Secure Network Analytics 평가 모드를 사용할 경우 선택한 기능을 90일간 사용할 수 있습니다. Secure Network Analytics의 최대 기본 기능을 사용하고 계정에 라이선스 및 기능을 추가하려면 제품 인스턴스를 Smart Software 라이선싱에 등록하십시오. 자세한 내용은 **11. 라이선싱 Secure Network Analytics**을 참조하십시오.

> 90일 평가 기간이 만료되기 전 제품 인스턴스를 등록했는지 확인하십시오. 평가 기간이 만료되면 플로우 수집이 중지됩니다. 플로우 수집을 다시 시작하려면 제품 인스턴스를 등록하십시오.

TLS

Secure Network Analytics v1.2가 필요합니다.

타사 애플리케이션

Secure Network Analytics 은 어플라이언스에 서드파티 애플리케이션 설치를 지원하지 않습니다.

브라우저

Secure Network Analytics 는 최신 버전의 Chrome, Firefox, Edge를 지원합니다.

호스트 이름

각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.

도메인 이름

각 어플라이언스에는 정규화된 도메인 이름이 필요합니다. 빈 도메인을 사용하여 어플라이언스를 설치할 수 없습니다.

NTP 서버

- **설정:** 각 어플라이언스에 최소 1개의 NTP 서버가 필요합니다.
- **문제가 있는 NTP:** 서버 목록에 있는 경우 130.126.24.53 NTP 서버를 제거합니다. 이 서버는 문제가 있는 것으로 알려져 있으며 기본 NTP 서버 목록에서 더 이상 지원되지 않습니다.

시간대

모든 Secure Network Analytics 어플라이언스는 UTC(협정 세계시)를 사용합니다.

- **가상 호스트 서버:** 가상 호스트 서버가 올바른 시간으로 설정되어 있는지 확인합니다.

> 가상 어플라이언스를 설치할 가상 호스트 서버에 설정한 시간이 정확한지 확인하십시오. 시간이 정확하지 않을 경우, 어플라이언스가 부팅을 하지 못할 수 있습니다.

시스템 구성 계획

구성을 시작하기 전에 지침을 검토하여 최초 설정에서 어플라이언스를 구성하고 어플라이언스 설정 도구에서 하나의 매니지드 시스템으로 구성하기 위한 계획, 시간, 요구 사항을 파악합니다.

시스템 구성 요구 사항

v7.4.2 구축에 대한 세부사항을 확인하려면 네트워크 설계자 및 관리자에게 문의하십시오.Secure Network Analytics 설정 요구 사항은 각 섹션을 참조하십시오.

- **Secure Network Analytics 포함 데이터스토어**
- **Secure Network Analytics 다음 없이 데이터스토어**
- **Secure Network Analytics 하이브리드 구축**
- **시스템 구성 계획**

Secure Network Analytics 포함 데이터스토어

Secure Network Analytics에서 데이터 저장소를 사용하는 경우 플로우 컬렉터는 스토리지를 위해 데이터 저장소 데이터 노드로 텔레메트리를 보냅니다.

- **데이터 노드의 수:** 데이터 저장소에는 1개의 데이터 노드(단일 데이터 노드 구축) 또는 3개 이상의 데이터 노드(다중 데이터 노드 구축)를 포함할 수 있습니다. 데이터 노드가 2개뿐인 데이터스토어은 지원되지 않습니다.
- **하드웨어 또는 가상:** 데이터 노드이 모두 하드웨어 또는 모두 Virtual Edition으로 같은 유형인지 확인합니다.
- **크기**: 데이터 노드 Virtual Edition의 프로필 크기가 동일한지 확인하여 동일한 RAM, CPU 및 디스크 공간을 확보합니다. 자세한 내용은 가상 어플라이언스 설치 가이드를 참조하십시오.
- **텔레메트리 수집**: NetFlow 외에도 NVM 플로우(Network Visibility Module) 및 방화벽 로그에 대한 텔레메트리 수집을 구성할 수 있습니다.

올바른 설정을 위해 다음 사항을 참고하십시오.

1. 최초 설정에서 데이터 저장소 구성에 대한 어플라이언스를 구성합니다. 다음 어플라이언스를 구성합니다.

    - **관리자: 구성 매니저**
    - 플로우 컬렉터: 데이터 저장소를 사용한 플로우 컬렉터 구성 참조 **데이터 저장소가 있는 플로우 컬렉터구성**
    - **데이터 노드**: **구성 데이터 노드**

2. 매니저 Appliance Setup Tool(어플라이언스 설정 도구)에서 Secure Network Analytics 어플라이언스에 대한 데이터 저장소 도메인을 생성합니다.
3. NVM 플로우 및 방화벽 로그에 대한 텔레메트리 수집을 활성화하려면 **10. 텔레메트리 구성**

Secure Network Analytics 다음 없이 데이터스토어

데이터스토어가 없는 Secure Network Analytics에서 플로우 컬렉터는 텔레메트리를 플로우 컬렉터 또는 플로우 컬렉터 데이터베이스에 로컬로 저장합니다(5000 Series만 해당).

올바른 설정을 위해 다음 사항을 참고하십시오.

1. 최초 설정에서 다음 어플라이언스를 구성합니다.

   - **관리자: 구성 매니저**
   - **플로우 컬렉터: 데이터스토어** 참조

2. 매니저 Appliance Setup Tool(어플라이언스 설정 도구)에서 Secure Network Analytics 어플라이언스에 대한 비데이터 저장소 도메인을 생성합니다.

매니지드 시스템 구성을 완료한 후 향후 구축에 데이터스토어를 추가할 수 있습니다(지침은 **비데이터 저장소 구축에 데이터 저장소 추가** 참조).

또한, 전환 전 데이터 또는 가시성을 손실하지 않고 데이터 저장소 데이터베이스를 사용하도록 기존 플로우 컬렉터를 전환할 수 있습니다. 이렇게 하면 데이터 저장소에서만 사용 가능한 기능을 활용할 수 있습니다. 자세한 내용은 **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**을 참조하십시오.

Secure Network Analytics 하이브리드 구축

하이브리드로 구성한 Secure Network Analytics에서 스토리지용 데이터 저장소 데이터 노드에 텔레메트리를 전송하고, 플로우 컬렉터 또는 플로우 컬렉터 데이터베이스에서 로컬로 텔레메트리를 저장하도록 다른 플로우 컬렉터를 설정할 수 있습니다(5000 Series만 해당).

정상적으로 설정하려면 다음 순서로 어플라이언스와 도메인을 구성합니다.

1. 최초 설정에서 데이터 저장소 없이 어플라이언스를 구성합니다. 다음 어플라이언스를 구성합니다.

   - **관리자: 구성 매니저**
   - **플로우 컬렉터: 데이터스토어** 참조

2. 매니저 Appliance Setup Tool(어플라이언스 설정 도구)에서 Secure Network Analytics 어플라이언스에 대한 비데이터 저장소 도메인을 생성합니다.
3. **9. 어플라이언스 구성 종료**까지 모든 절차를 완료하여 비데이터 저장소 도메인의 초기 시스템 설정을 완료합니다.

4. **비데이터 저장소 구축에 데이터 저장소 추가**의 지침을 따르십시오. 데이터 저장소 도메인을 생성하고 플로우 컬렉터 및 데이터 노드를 도메인에 추가합니다.

어플라이언스 구성 요구 사항

최초 설정에서 각 어플라이언스를 구성하려면 다음 정보가 필요합니다. 또한 이 정보를 사용하여 어플라이언스 설정 도구로 어플라이언스를 매니지드 시스템으로 구성합니다.

설정 요구 사항	세부 정보	어플라이언스
IP Address(IP 주소)	`eth0` 관리 포트에 라우팅 가능한 IP 주소를 할당합니다.	
넷마스크		
게이트웨이		
호스트 이름	각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.	
도메인 이름	각 어플라이언스에는 정규화된 도메인 이름이 필요합니다. 빈 도메인을 사용하여 어플라이언스를 설치할 수 없습니다.	
DNS 서버	이름 확인용 내부 DNS 서버	
NTP 서버	서버 간 동기화를 위한 내부 시간 서버입니다. 각 어플라이언스에 최소 1개의 NTP 서버가 필요합니다. 서버 목록에 있는 경우 130.126.24.53 NTP 서버를 제거합니다. 이 서버는 문제가 있는 것으로 알려져 있으며 기본 NTP 서버 목록에서 더 이상 지원되지 않습니다.	
메일 릴레이 서버	알림을 보낼 SMTP 메일 서버	
플로우 컬렉터 내보내기 포트	플로우 컬렉터에만 필요합니다. NetFlow 기본값: 2055	
프라이빗 LAN 또는 VLAN	데이터 노드에만 필요합니다.	

내에서 라우팅할 수 없는 IP 주소(상호 데이터 노드통신용)	• 하드웨어 eth2 또는 eth2와 eth3의 결합 최대 20G 처리량을 지원하는 LACP `eth2/eth3` 결합 포트 채널을 생성하면 데이터 노드간의 통신이 더 빨라지고 데이터스토어에 데이터 노드 추가 또는 교체가 더 빨라집니다. LACP 포트 결합은 하드웨어 데이터 노드에 사용할 수 있는 유일한 결합 옵션입니다. • 가상 eth1 **IP 주소:** 제공된 IP 주소를 사용하거나 상호 데이터 노드통신에 대한 다음 요구 사항을 충족하는 값을 입력할 수 있습니다. • 169.254.42.2와 169.254.42.254 사이의 **169.254.42.0/24 CIDR 블록**의 **라우팅할 수 없는 IP 주소**. • **처음 3개의 옥텟:** 169.254.42 • **서브넷:** /24 • **순차**: 유지 관리의 편의를 위해 순차 IP 주소(예: 169.254.42.10, 169.254.42.11, 169.254.42.12)를 선택합니다. **넷마스크:** 넷마스크는 255.255.255.0으로 하드 코딩되어 있으며 수정할 수 없습니다.	
eth0 하드웨어 연결 포트	데이터스토어 하드웨어 어플라이언스가 있는 Secure Network Analytics의 경우에만 필요합니다. • 매니저 2210 • 플로우 컬렉터 4210 • 데이터 노드s eth0 하드웨어 연결 포트 옵션: • **SFP+**: SFP+: 10G SFP+/DAC 파이버 포트(eth0용).	

	• **BASE-T**: 100Mbs/1GbE/10GbE eth0에 대한 BASE-T 구리 포트입니다. BASE-T가 기본값입니다.	

하드웨어(물리적) 어플라이언스에 연결

CIMC(Cisco Integrated Management Controller), 키보드와 모니터, 시리얼 케이블이나 시리얼 콘솔을 사용하여 어플라이언스에 연결합니다. 지침은 x2xx Series 하드웨어 설치 가이드 또는 Secure Network Analyticsx3xx Series 하드웨어 설치 가이드를 참조하십시오.

CIMC 액세스

원격 액세스를 위해 CIMC에 로그인합니다. CIMC를 아직 구성하지 않은 경우 Cisco UCS C Series 통합 관리 컨트롤러 GUI 구성 가이드의 지침을 따르십시오.

기본 비밀번호는 **password**입니다. 처음 로그인할 때 비밀번호를 변경하십시오.

Virtual Edition 어플라이언스에 연결

1. Hypervisor 호스트(가상 머신 호스트)에 연결합니다.
2. Hypervisor 호스트에서 가상 머신을 찾습니다.
3. 가상 머신의 전원이 켜져 있는지 확인합니다.

   가상 머신의 전원이 켜지지 않았고 사용 가능한 메모리가 부족하다는 오류 메시지를 받은 경우, 다음 작업 중 하나를 수행하십시오.

   - **리소스:** 어플라이언스가 설치된 시스템에서 사용 가능한 리소스를 늘립니다. 자세한 내용은 Virtual Edition 어플라이언스 설치 가이드의 **리소스 요구 사항**을 참조하십시오.
   - **VMware 환경:** 어플라이언스 및 해당 리소스 풀의 메모리 예약 한도를 늘립니다.

> 충분한 리소스를 할당하려면 리소스 요구 사항을 검토합니다. 이 단계는 시스템 성능에 중요합니다.
>
> 필요한 리소스 없이 Cisco Secure Network Analytics 어플라이언스를 구축하기로 선택한 경우, 어플라이언스 리소스 사용을 면밀히 모니터링하고 필요에 따라 리소스를 늘려 구축의 적절한 상태와 기능을 보장해야 할 책임이 있습니다.

4. 가상 머신 콘솔에 액세스합니다. 가상 어플라이언스에서 부팅을 완료하도록 허용합니다.

> VM 호스트의 속도에 따라 모든 서비스가 부팅되는 데 약 30분 정도 걸릴 수 있습니다.

1. 최초 설정을 사용하여 환경 구성

다음 지침에 따라 각 어플라이언스의 기본 환경을 구성합니다. 하드웨어(물리적) 어플라이언스든 VE(Virtual Edition) 어플라이언스든 관계없이 최초 설정에서 순서에 상관없이 어플라이언스를 구성할 수 있습니다.

> 이러한 구성 절차를 시작하기 전에 **시스템 구성 계획**을 검토합니다.

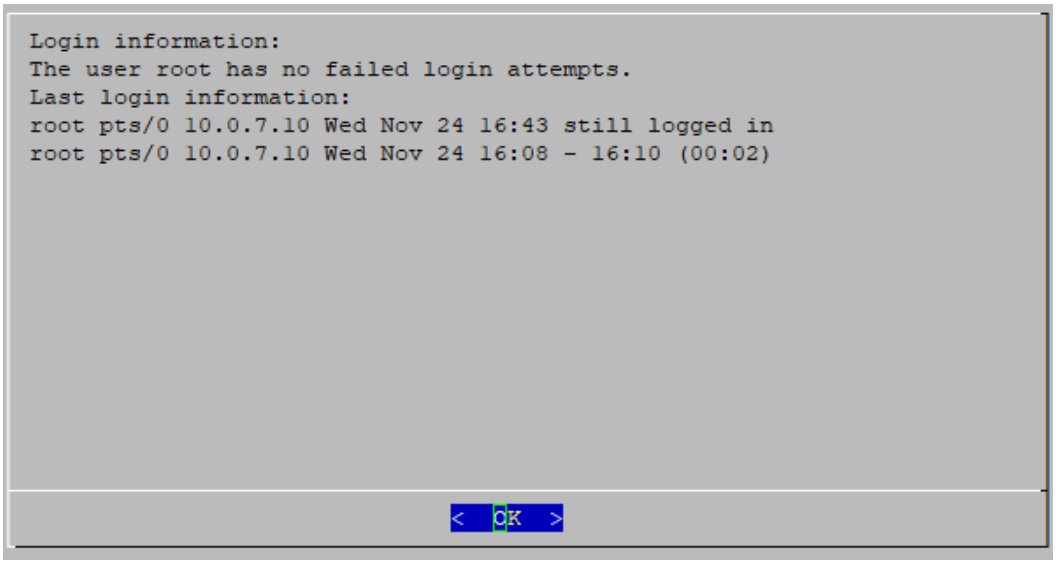
어플라이언스 구성 개요

어플라이언스 지침	데이터 저장소에 필수	참고
구성 매니저	예	매니저은 데이터 저장소가 있거나 없는 구축에 필요합니다.
구성 데이터 노드	예	1개 데이터 노드(단일 데이터 노드 구축) 또는 3개 이상의 데이터 노드(멀티 데이터 노드 구축)를 구축할 수 있습니다. 2 데이터 노드를 구축하는 것은 지원되지 않습니다. 데이터 노드는 모두 하드웨어 또는 모두 가상 버전이어야 합니다. 또한 데이터 노드 Virtual Edition의 프로필 크기가 동일한지 확인하여 동일한 RAM, CPU 및 디스크 공간을 확보합니다. 자세한 내용은 가상 어플라이언스 설치 가이드를 참조하십시오.
데이터 저장소가 있는 플로우 컬렉터구성	예	플로우 컬렉터는 텔레메트리를 저장할 수 있도록 데이터스토어 데이터 노드로 전송합니다. 또한 수집할 텔레메트리 유형을 확인합니다.
데이터스토어		플로우 컬렉터는 텔레메트리를 플로우 컬렉터 또는 플로우 컬렉터 데이터베이스에 로컬로 저장합니다(5000 Series만 해당).
플로우 센서 또는 UDP Director		플로우 센서과 UDP Director는 선택 사항입니다.

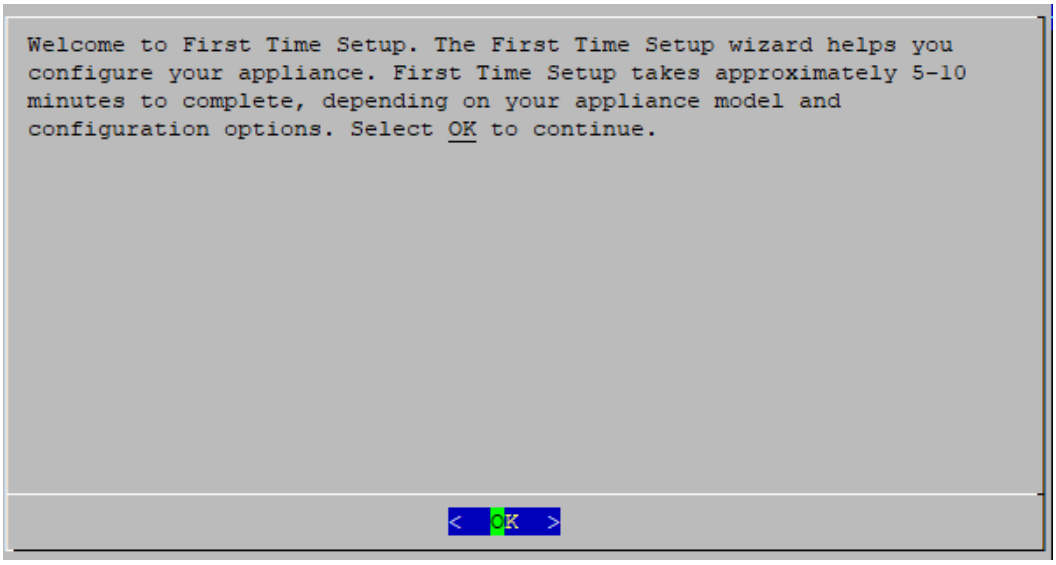
		UDP Director 대신 Cisco Telemetry Broker를 설치하려면 이 가이드의 지침을 완료하여 시스템 구성을 완료합니다. 그런 다음 Cisco Telemetry Broker 가상 어플라이언스 구축 및 구성 가이드의 지침을 따르십시오.

구성 매니저

1. 콘솔을 통해 매니저에 로그인합니다.
    - **로그인:** sysadmin
    - **기본 비밀번호**: lan1cope
    - 시스템을 구성할 때 기본 비밀번호를 변경합니다.
2. 시스템 구성(`SystemConfig`)이 열립니다.
3. 실패한 로그인 시도 정보를 검토합니다. **OK(확인)**를 선택하여 계속합니다.

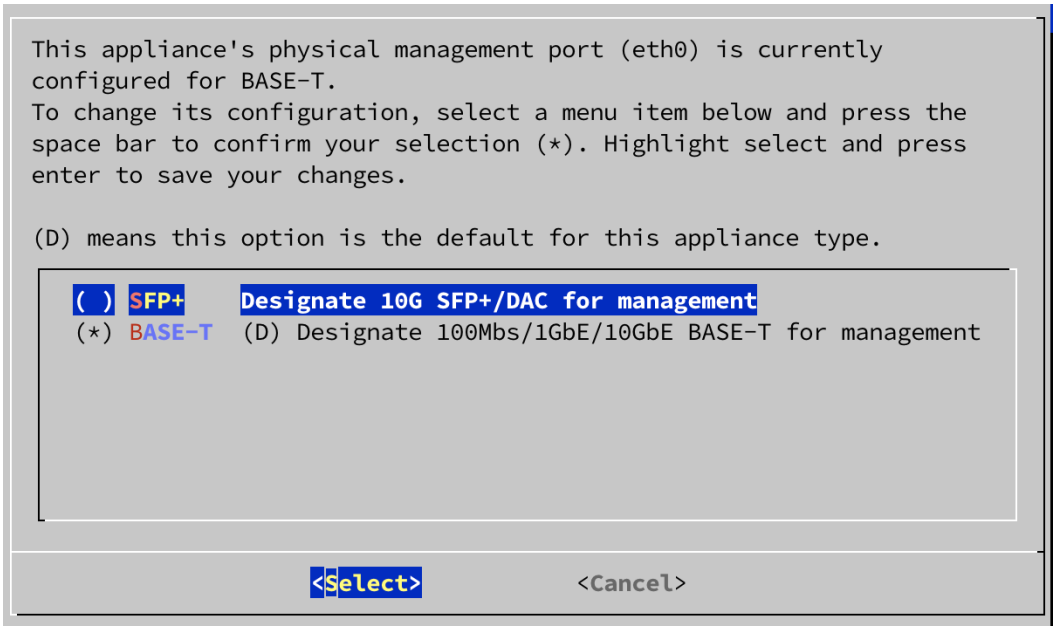


4. 최초 설정 소개를 검토합니다. **OK(확인)**를 선택하여 계속합니다.



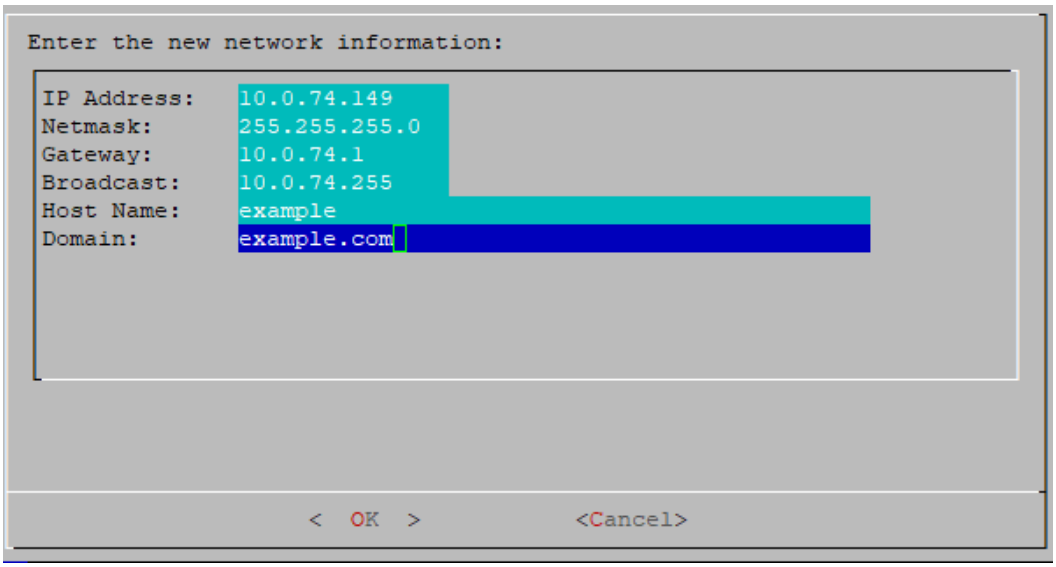
5. **eth0에 대한 포트 순서 설정(매니저 2210 하드웨어 전용):** 다음 중 하나를 선택합니다.

   - **SFP+**: eth0에 대해 10G SFP+/DAC 파이버 포트를 사용하도록 어플라이언스를 구성합니다.
   - **BASE-T**: eth0에 대해 100Mbs/1GbE/10GbE BASE-T 구리 포트를 사용하도록 어플라이언스를 구성합니다. BASE-T가 기본값입니다.

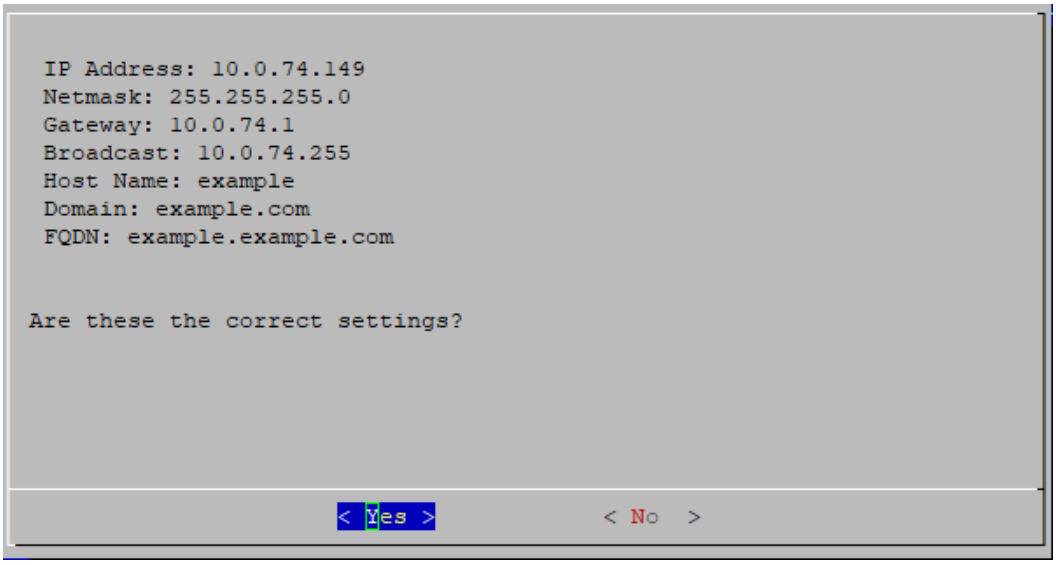


6. 관리 인터페이스에 **IP 주소**(eth0), **넷마스크**, **게이트웨이**, **브로드캐스트**, **호스트 이름** 및 **도메인**을 입력하고 **OK(확인)**을 선택하여 계속합니다.

> 각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.



7. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.



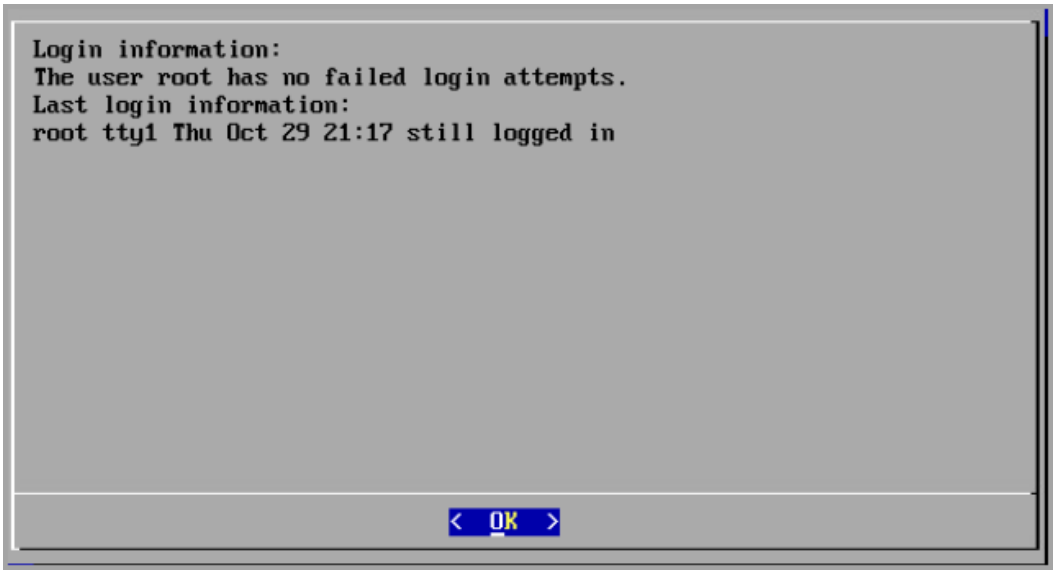
8. **OK(확인)**을 선택하여 선택을 확인합니다. 화면에 표시 되는 프롬프트에 따라 가상 환경을 종료하고 어플라이언스를 재시작합니다.
9. **Ctrl + Alt**를 눌러 콘솔을 종료합니다.
10. 시스템에서 다음 매니저에 대한 **구성 매니저** 구성의 모든 단계를 반복합니다.

    최초 설정에서 매니저을 모두 구성한 경우 **어플라이언스 구성 개요**로 돌아가 플로우 컬렉터 및 다른 어플라이언스를 구성합니다.

구성 데이터 노드

1개 데이터 노드(단일 데이터 노드 구축) 또는 3개 이상의 데이터 노드(멀티 데이터 노드 구축)를 구축할 수 있습니다. 2 데이터 노드를 구축하는 것은 지원되지 않습니다.

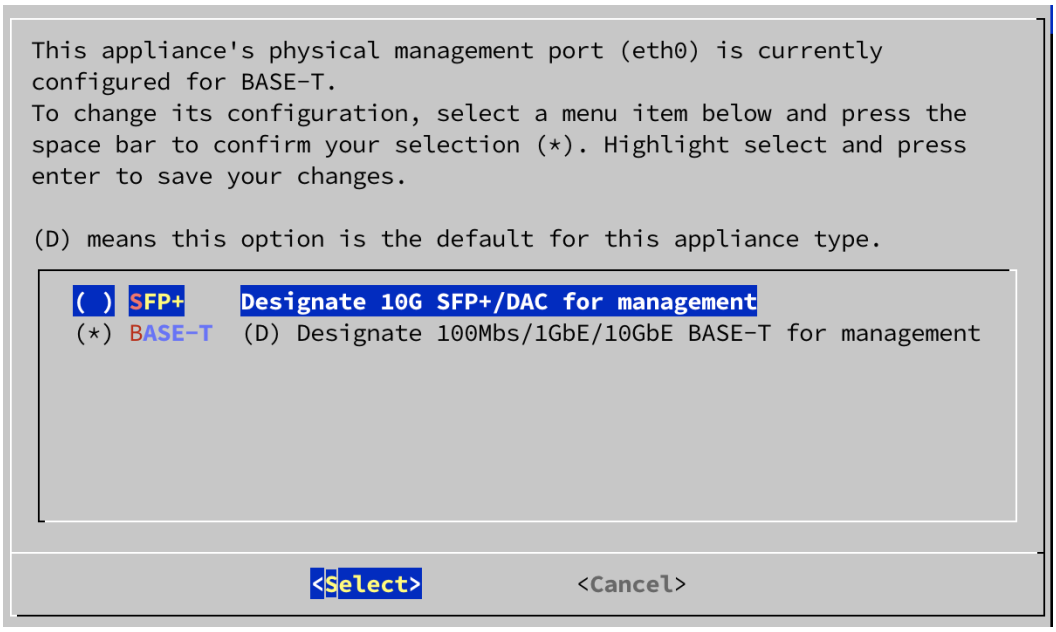
1. 콘솔로 데이터 노드에 로그인합니다.
   - **로그인:** sysadmin
   - **기본 비밀번호**: lan1cope
   - 시스템을 구성할 때 기본 비밀번호를 변경합니다.
2. 시스템 구성(`SystemConfig`)이 열립니다.
3. 실패한 로그인 시도 정보를 검토합니다. **OK(확인)**를 선택하여 계속합니다.



4. 최초 설정 소개를 검토합니다. **OK(확인)**를 선택하여 계속합니다.

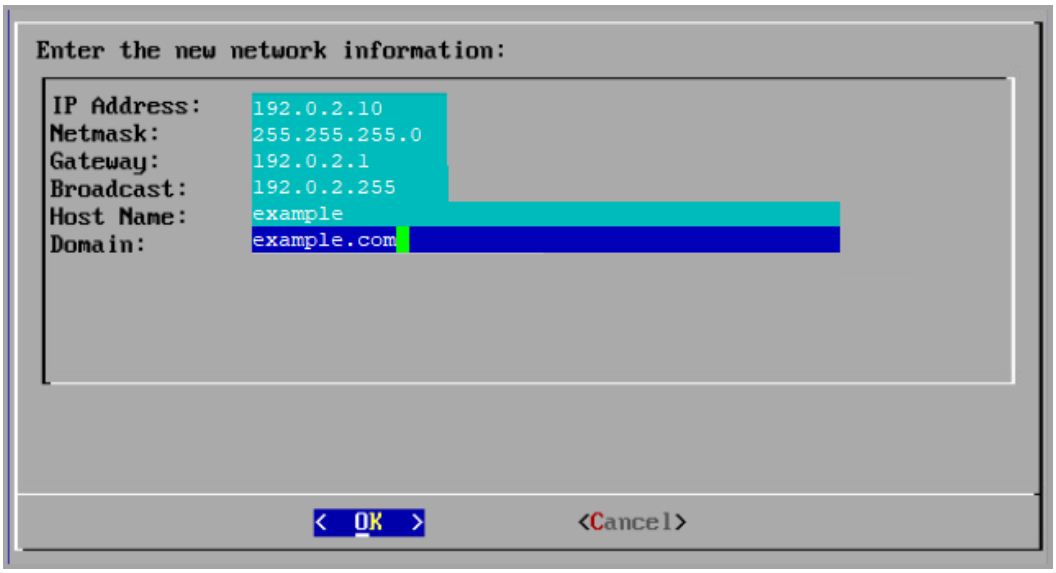
5. **eth0의 포트 순서 설정(데이터 저장소 6200 하드웨어 전용):** 다음 중 하나를 선택합니다.

   - **SFP+**: eth0에 대해 10G SFP+/DAC 파이버 포트를 사용하도록 어플라이언스를 구성합니다.
   - BASE-T: eth0에 대해 100Mbs/1GbE/10GbE BASE-T 구리 포트를 사용하도록 어플라이언스를 구성합니다.
     BASE-T가 기본값입니다.

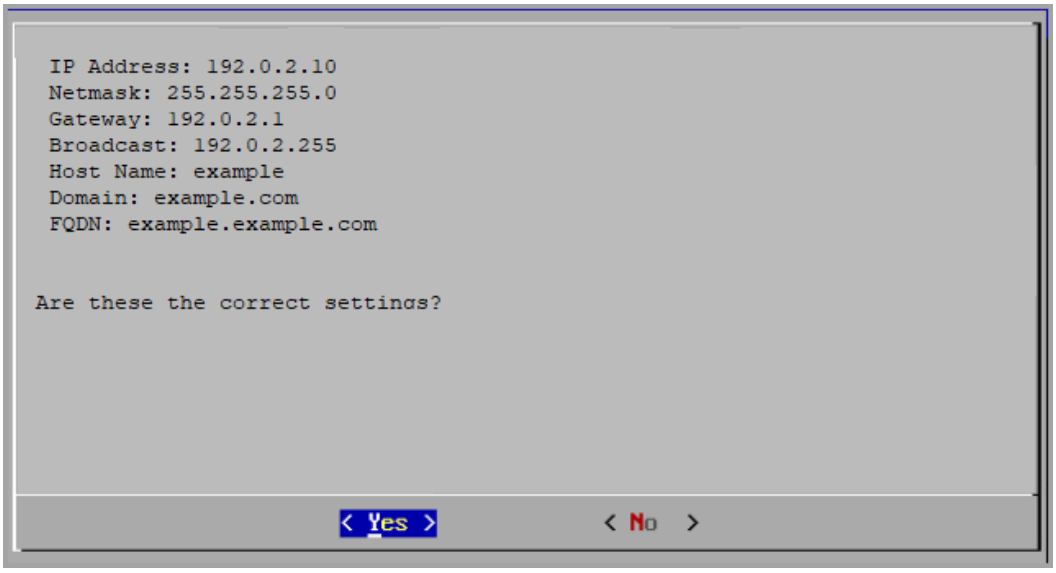


6. 관리 인터페이스에 **IP 주소**, **넷마스크**, **게이트웨이**, **브로드캐스트**, **호스트 이름** 및 **도메인**을 입력하고, **OK(확인)**을 선택하여 계속합니다.

> 각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.



7. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.



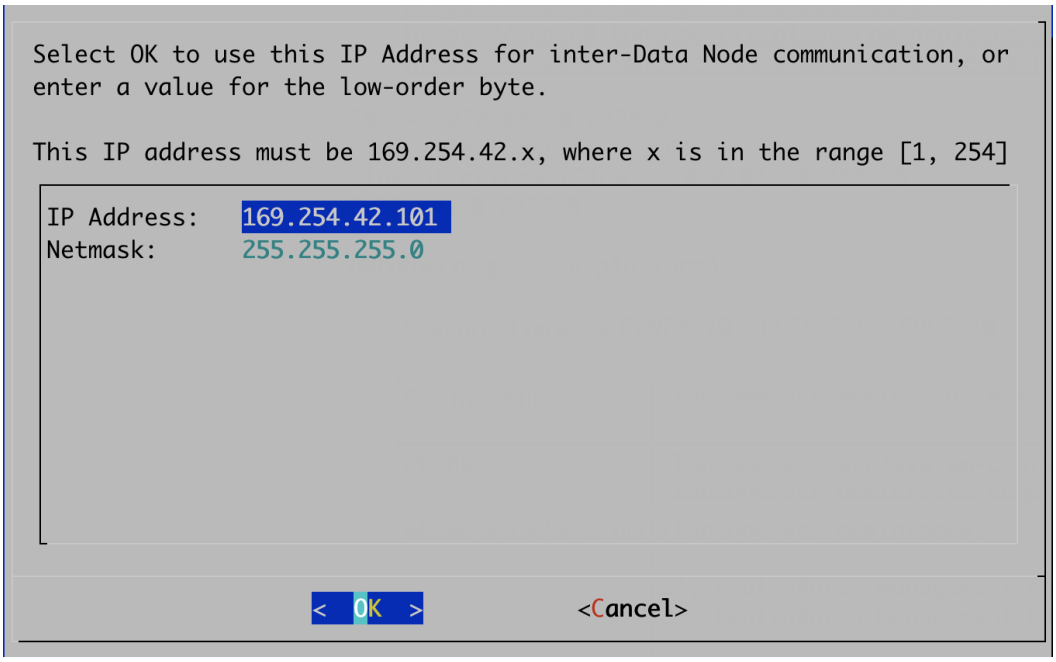
8. **OK(확인)**을 선택하여 선택을 확인합니다. 화면의 프롬프트를 따르십시오.

9. **상호 데이터 노드 통신을 위한 물리적 포트(eth2) 또는 포트 채널(eth2 및 eth3)을 구성합니다.**

> 하드웨어 데이터 노드의 경우, 10G 처리량에 대해 `eth2` 포트를 구성하면 정상적인 데이터 노드간 통신에 충분합니다. 최대 20G 처리량을 지원하는 LACP `eth2/eth3` 결합 포트 채널을 생성하면 데이터 노드간의 통신이 더 빨라지고 데이터스토어에 데이터 노드 추가 또는 교체가 더 빨라집니다. 각각의 새 데이터 노드는 인접 데이터 노드에서 트래픽을 수신하여 데이터를 채우기 때문입니다. LACP 포트 결합은 하드웨어 데이터 노드에 사용할 수 있는 유일한 결합 옵션입니다.

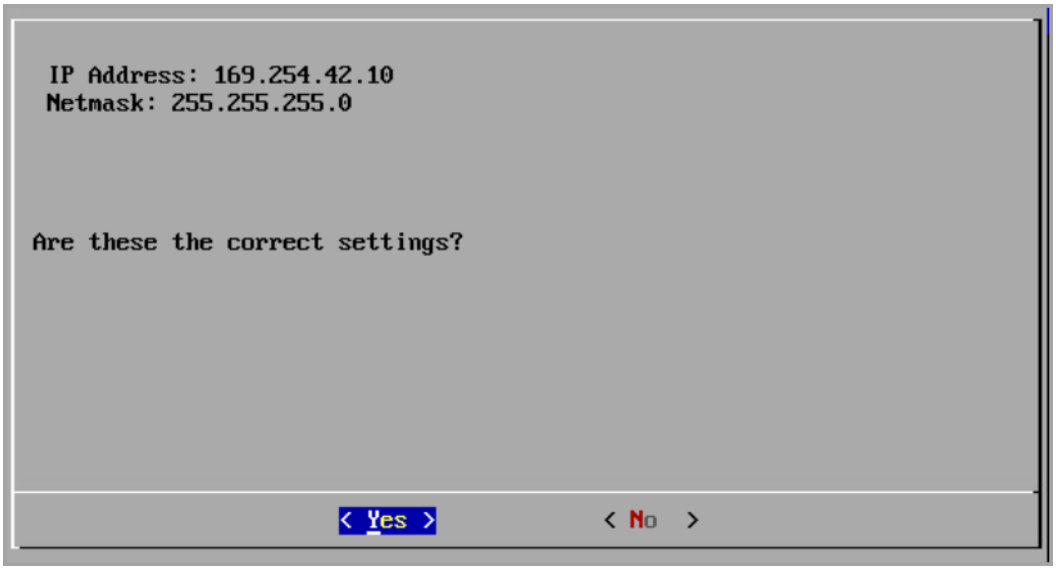
다음을 입력합니다.

필드	요구 사항
IP Address (IP 주소)	**제공된 IP 주소**를 사용하거나 상호 데이터 노드 통신을 위한 eth2 및 eth3 인터페이스에 대해 다음 요구 사항을 충족하는 **값을 입력합니다.** • 169.254.42.2와 169.254.42.254 사이의 **169.254.42.0/24 CIDR 블록**의 **라우팅할 수 없는 IP 주소**. • **처음 3개의 옥텟:** 169.254.42 • **서브넷:** /24 • **순차**: 유지 관리의 편의를 위해 순차 IP 주소(예: 169.254.42.10, 169.254.42.11, 169.254.42.12)를 선택합니다.
넷마스크	255.255.255.0



10. **OK(확인)**를 선택하여 계속합니다.

11. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.



12. 화면의 프롬프트에 따라 환경을 완료하고 어플라이언스를 다시 시작합니다.
13. **Ctrl + Alt**를 눌러 콘솔을 종료합니다.
14. 시스템에서 다음 데이터 노드에 대한 **구성 데이터 노드** 구성의 모든 단계를 반복합니다.

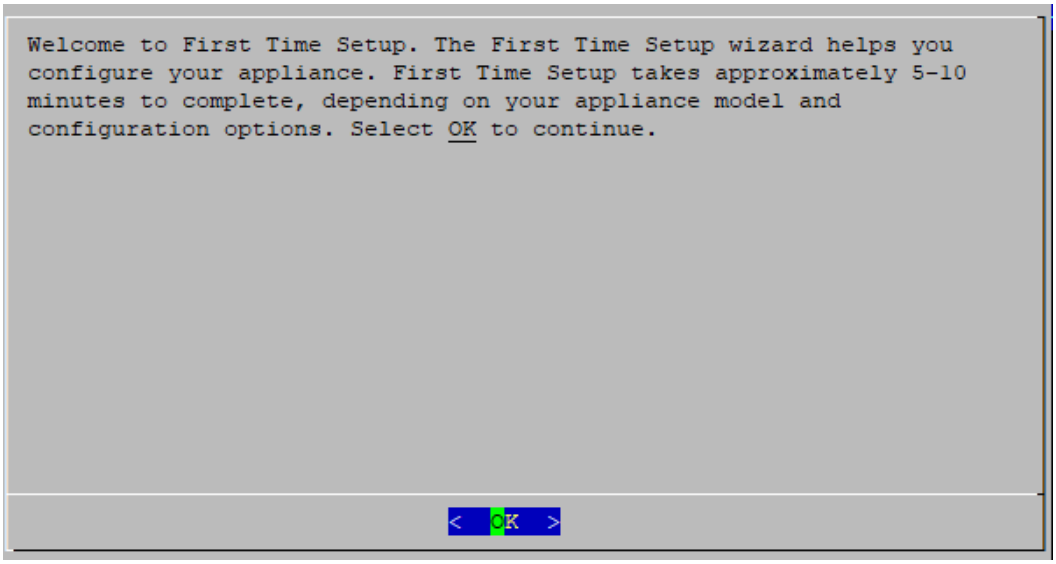
    - 최초 설정에서 모든 데이터 노드를 구성한 경우, 다음 섹션으로 이동하여 데이터 저장소가 있는 플로우 컬렉터를 구성하거나 **어플라이언스 구성 개요**로 돌아가 다른 어플라이언스를 구성합니다.
    - 최초 설정에서 모든 어플라이언스를 구성한 경우 **2. 매니지드 시스템 구성**

데이터 저장소가 있는 플로우 컬렉터구성

플로우 컬렉터을 데이터스토어에서 사용하도록 구성하는 경우, 플로우 컬렉터는 텔레메트리를 데이터 저장소 데이터 노드로 전송하여 저장합니다. 또한 수집할 텔레메트리 유형을 확인합니다.

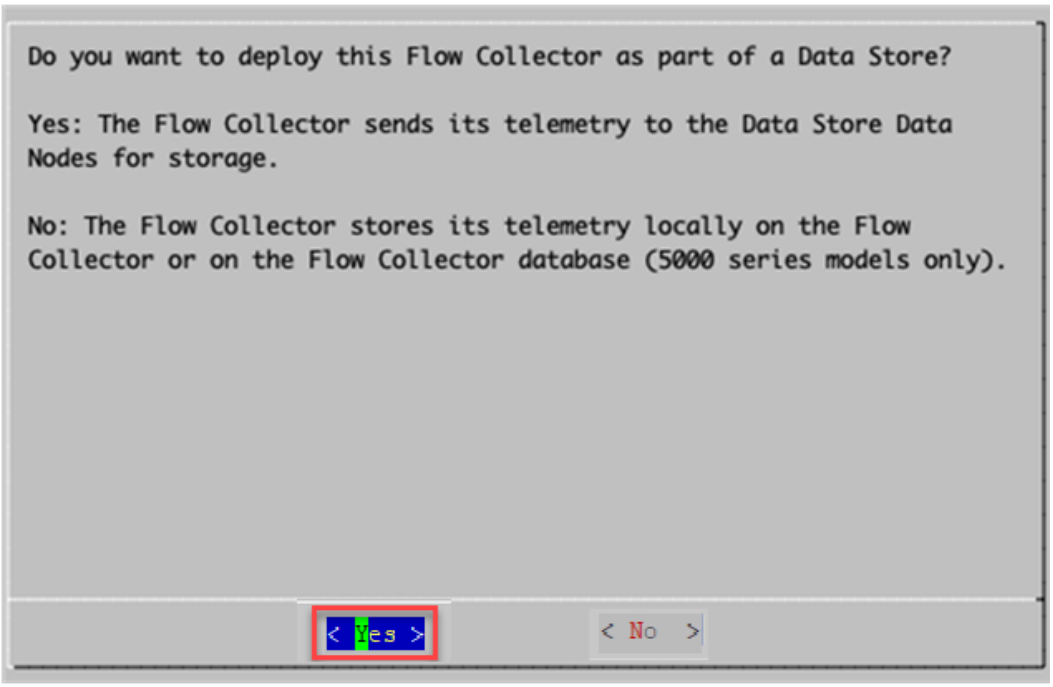
> v7.4.2부터는 비-데이터스토어 플로우 컬렉터 를 데이터스토어 플로우 컬렉터로 전환할 수 있습니다. 자세한 내용은 **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**을 참조하십시오.

1. 콘솔을 통해 플로우 컬렉터에 로그인합니다.
   - **로그인:** root
   - **기본 비밀번호**: lan1cope
   - 시스템을 구성할 때 기본 비밀번호를 변경합니다.
2. 명령 프롬프트에서 `SystemConfig`를 입력합니다. Enter를 누릅니다.
3. 실패한 로그인 시도 정보를 검토합니다. **OK(확인)**를 선택하여 계속합니다.
4. 최초 설정 소개를 검토합니다. OK(확인)를 선택하여 계속합니다.

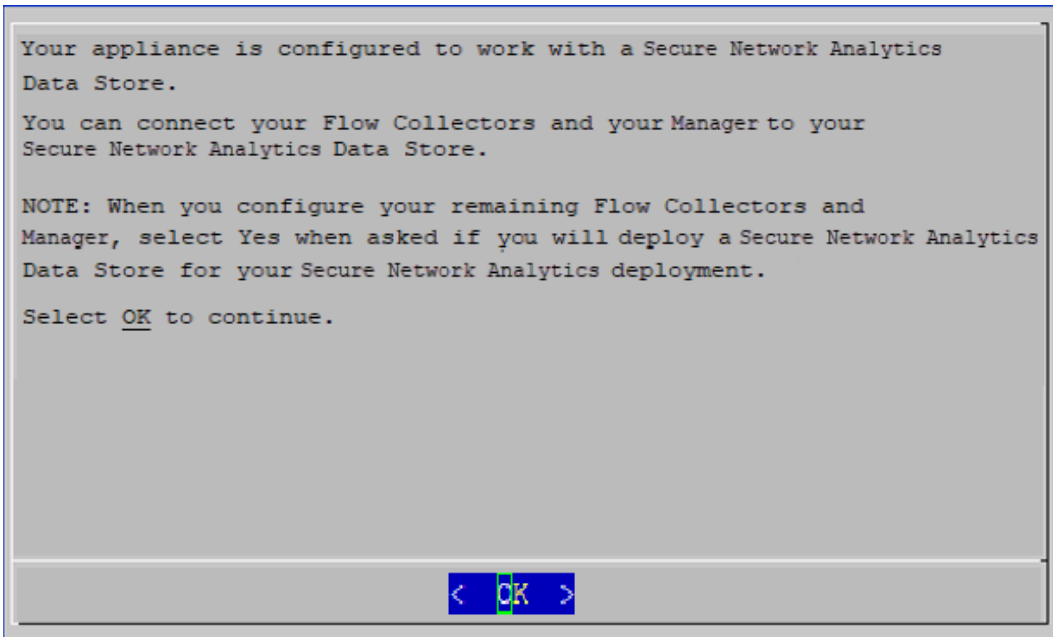


5. 이 플로우 컬렉터를 데이터스토어의 일부로 구축하시겠습니까? **Yes(예)**를 선택합니다.

> 플로우 컬렉터를 데이터스토어와 함께 사용하도록 구성한 후에는 이 구성을 변경할 수 없습니다. 데이터스토어를 네트워크에 구축하려는 경우에만 Yes(예)를 선택합니다.
>
> Secure Network Analytics를 데이터스토어 없이 구축해야 하는 경우 이 섹션의 지침을 따르지 마십시오. **데이터스토어**의 지침을 따릅니다.
>
> 잘못된 선택을 한 경우 새 가상 어플라이언스를 구축하거나 어플라이언스를 RFD 합니다.



6. **OK(확인)**를 선택하여 계속합니다.



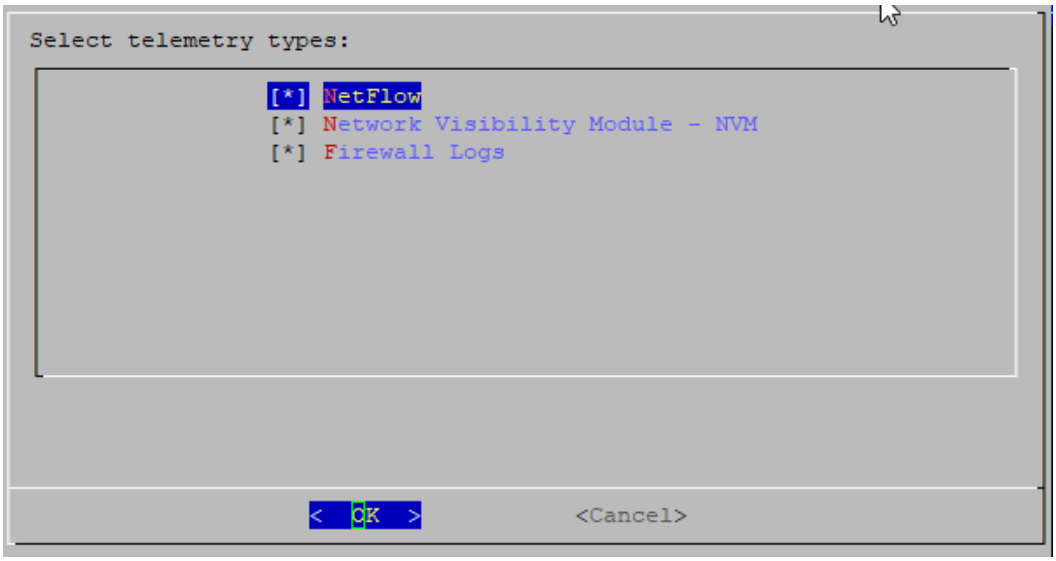
7. 수집할 텔레메트리 유형을 선택합니다.

   - **기본값:** 모든 텔레메트리 유형이 기본값으로 선택됩니다. 별표(*)는 선택된 텔레메트리를 표시합니다.
   - **선택 해제:** 텔레메트리를 선택 해제하려면 텔레메트리 유형을 선택하고 클릭합니다(또는 키보드의 스페이스 키를 누름).

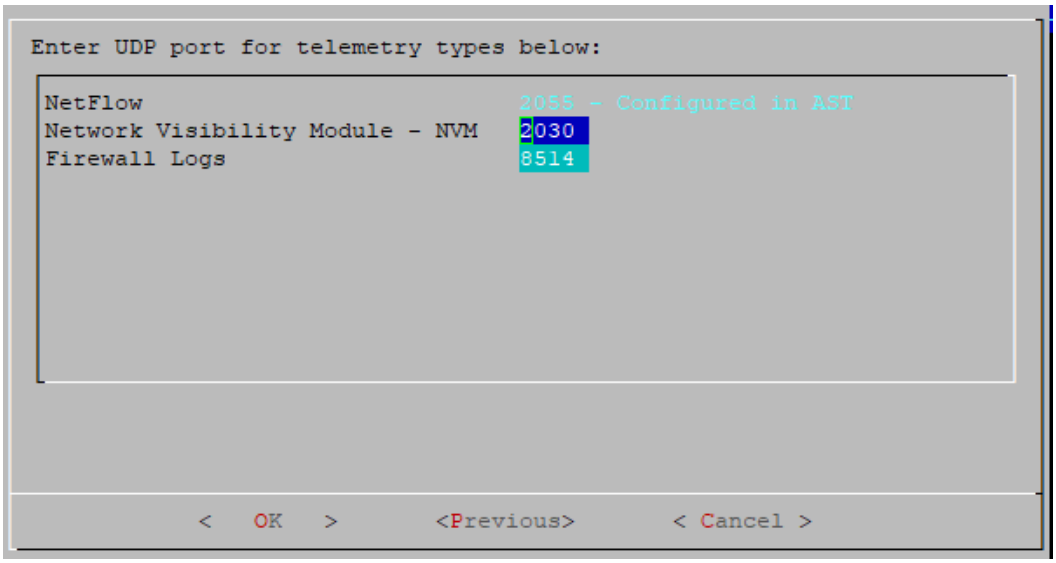
추가 정보:

- **Network Visibility Module(NVM):** Network Visibility Module(NVM)을 선택하면, 플로우 컬렉터가 NVM 플로우를 수집하고 저장합니다. 자세한 내용은 Cisco 보안 네트워크 분석 엔드포인트 라이센스 및 Network Visibility Module (NVM) 구성 가이드를 참조하세요.
- **Firewall Logs(방화벽 로그)**: Firewall Logs(방화벽 로그)를 선택하면 플로우 컬렉터에서 Cisco Security Analytics and Logging(온프레미스)에 대한 방화벽 이벤트 로그를 수집하고 저장합니다. 자세한 내용은 보안 분석 및 로깅: 방화벽 이벤트 통합 가이드를 참조하십시오.

> NetFlow를 비활성화하도록 플로우 수집기를 구성하는 경우 내보내기, 호스트 그룹, 보안 이벤트, 호스트 보고서 등의 구성 옵션을 업데이트해도 아무런 효과가 없습니다.

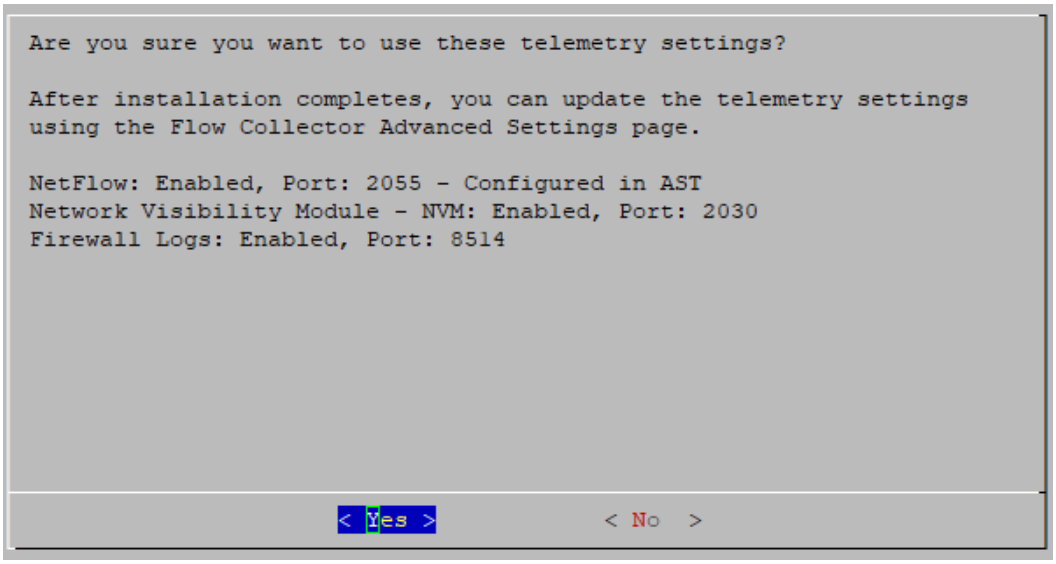


8. 선택한 텔레메트리 유형에 대한 UDP 포트를 입력합니다. **OK(확인)**를 선택합니다.



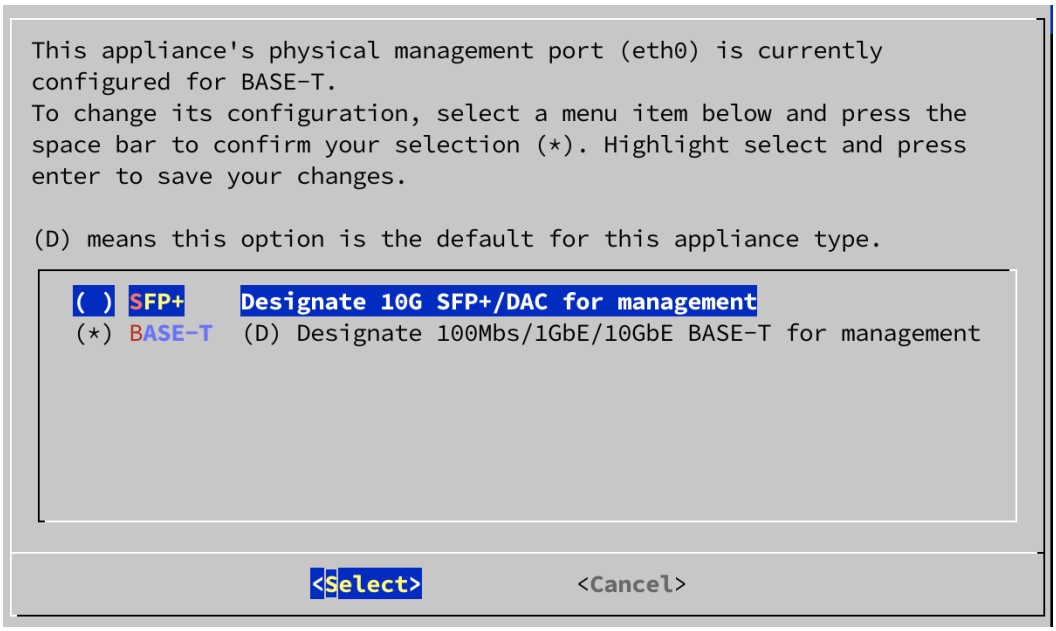
> 텔레메트리 포트가 고유한지 확인합니다. 텔레메트리 포트를 중복으로 구성하면 플로우 데이터 손실을 방지하기 위해 포트가 내부 기본값으로 재설정됩니다. 예를 들어, NetFlow와 NVM을 동일한 텔레메트리 포트로 내보내는 경우, NVM 데이터를 내보내는 각 디바이스는 플로우 컬렉터에 내보내기를 생성하고 플로우 컬렉터 엔진의 내보내기 리소스를 소진하여 플로우 데이터가 손실됩니다.

9. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.



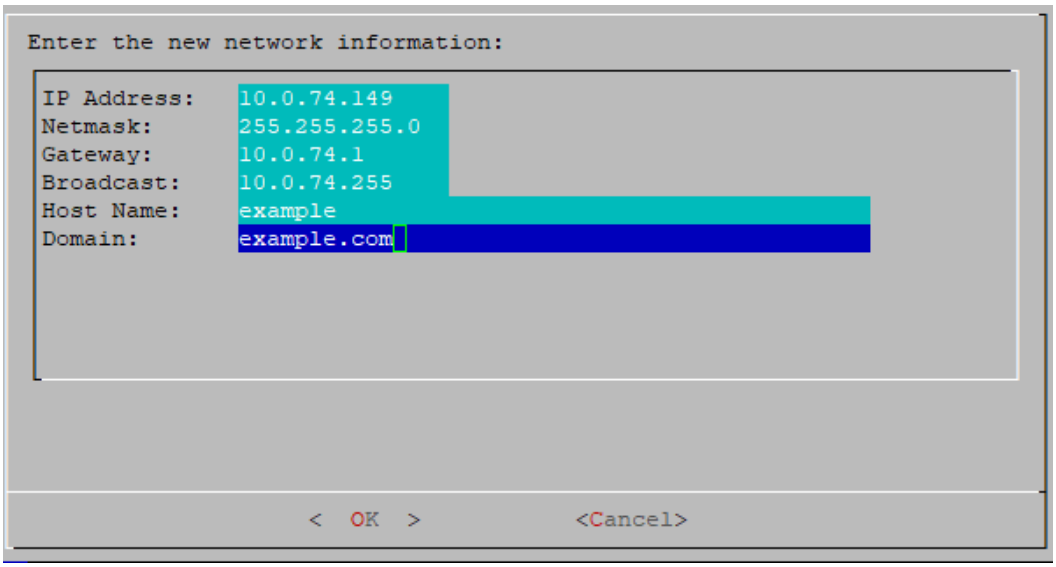
10. **eth0의 포트 순서 설정(플로우 컬렉터 4210 하드웨어만 해당):** 다음 중 하나를 선택합니다.

- **SFP+**: eth0에 대해 10G SFP+/DAC 파이버 포트를 사용하도록 어플라이언스를 구성합니다.
- **BASE-T**: eth0에 대해 100Mbs/1GbE/10GbE BASE-T 구리 포트를 사용하도록 어플라이언스를 구성합니다. BASE-T가 기본값입니다.

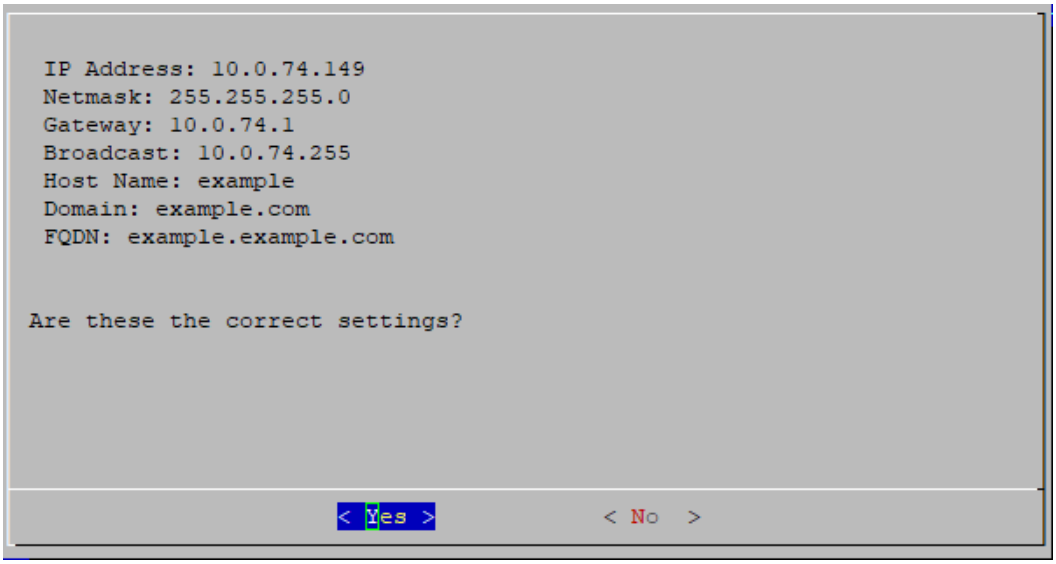


11. 관리 인터페이스에 **IP 주소**, **넷마스크**, **게이트웨이**, **브로드캐스트**, **호스트 이름** 및 **도메인**을 입력하고, **OK(확인)**을 선택하여 계속합니다.

> 각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.



12. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.



13. **OK(확인)**을 선택하여 선택을 확인합니다. 화면에 표시 되는 프롬프트에 따라 가상 환경을 종료하고 어플라이언스를 재시작합니다.
14. **Ctrl + Alt**를 눌러 콘솔을 종료합니다.

15. 시스템에서 다음 플로우 컬렉터에 대한 **데이터 저장소가 있는 플로우 컬렉터구성** 구성의 모든 단계를 반복합니다.

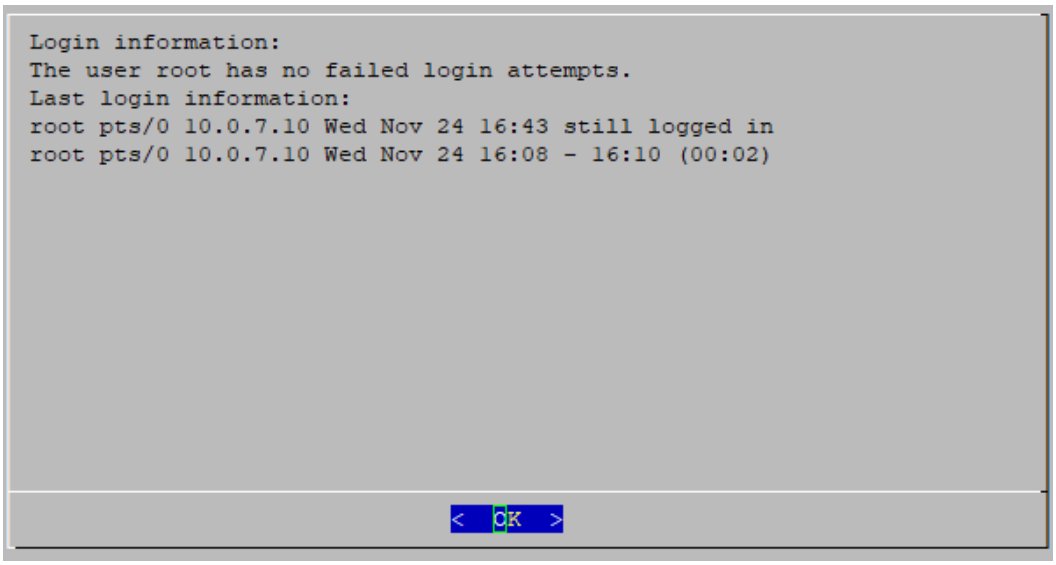
    최초 설정에서 데이터 저장소에 대한 모든 플로우 컬렉터를 구성한 경우, **어플라이언스 구성 개요**로 돌아가 다른 어플라이언스를 구성합니다.

데이터스토어

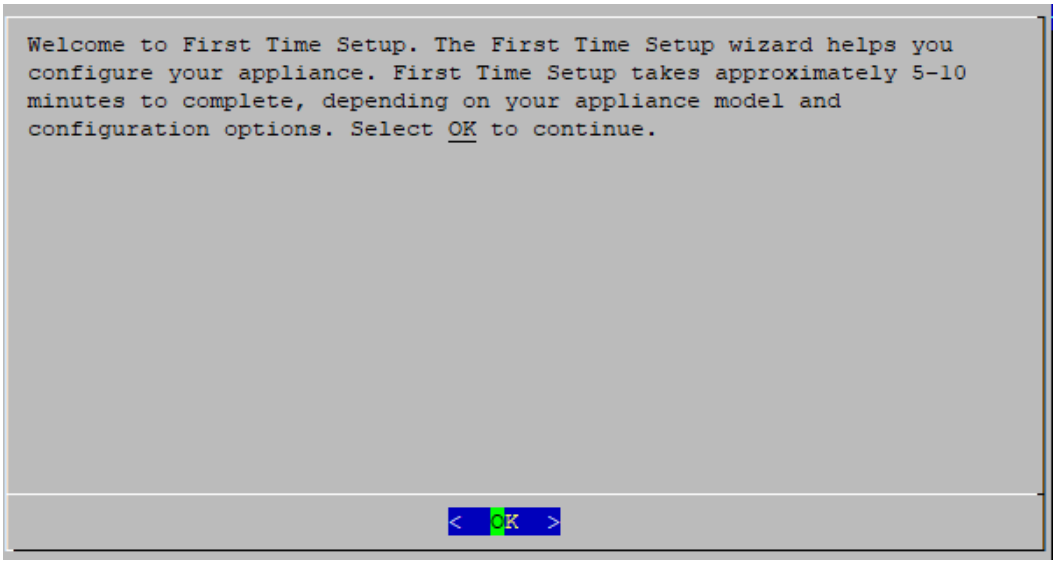
없이 플로우 컬렉터구성

플로우 컬렉터를 데이터 저장소 없이 사용하도록 설정하는 경우, 플로우 컬렉터은 텔레메트리를 플로우 컬렉터 또는 플로우 컬렉터 데이터베이스에 로컬로 저장합니다(5000 Series에만 해당).

1. 콘솔을 통해 플로우 컬렉터에 로그인합니다.
   - **로그인:** sysadmin
   - **기본 비밀번호**: lan1cope
   - 시스템을 구성할 때 기본 비밀번호를 변경합니다.
2. 시스템 구성(`SystemConfig`)이 열립니다.
3. 실패한 로그인 시도 정보를 검토합니다. **OK(확인)**를 선택하여 계속합니다.

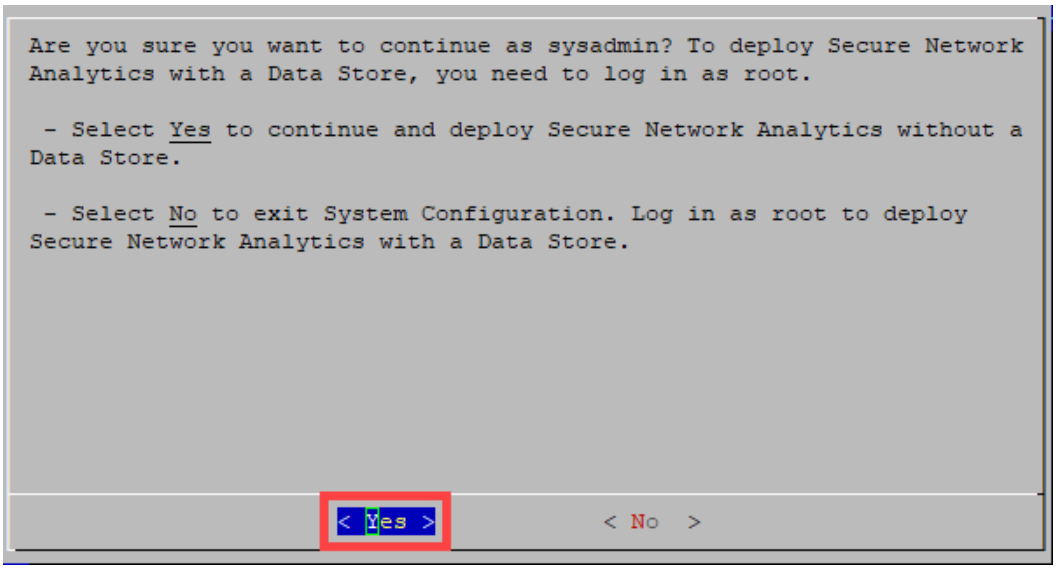


4. 최초 설정 소개를 검토합니다. **OK(확인)**를 선택하여 계속합니다.

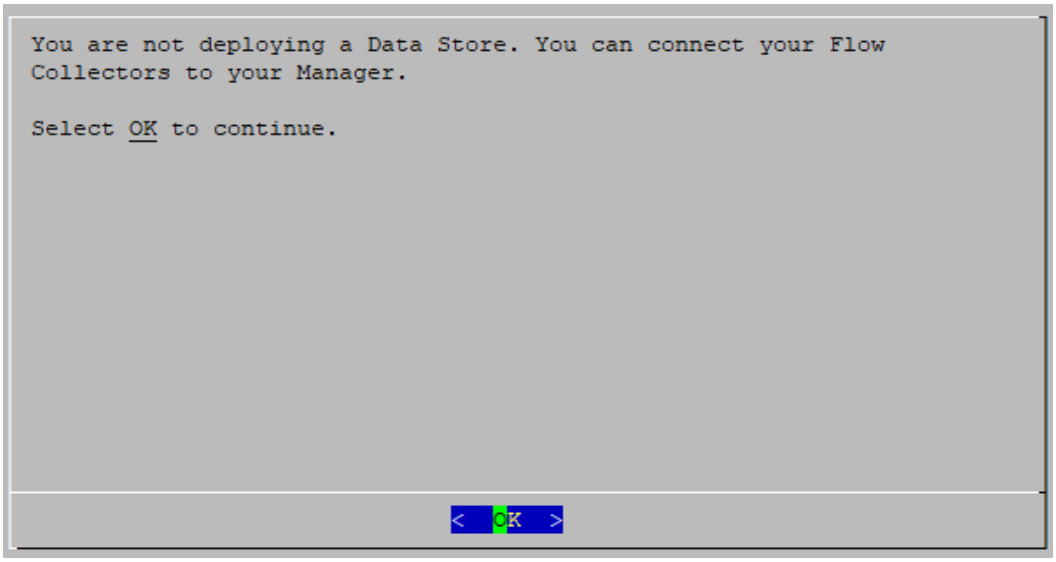


5. sysadmin 역할을 계속하시겠습니까? 별도의 데이터스토어 없이 구성을 계속 진행하려면 **Yes(예)**를 선택합니다.

> **Yes(예)**를 선택해야 합니다. 데이터스토어가 있는 Secure Network Analytics를 구축해야 하는 경우에는 이 섹션의 지침을 따르지 마십시오. 데이터 저장소에 대해 **데이터 저장소가 있는 플로우 컬렉터구성**의 지침을 따르십시오.
> 잘못된 선택을 한 경우 새 가상 어플라이언스를 구축하거나 어플라이언스를 RFD 합니다.

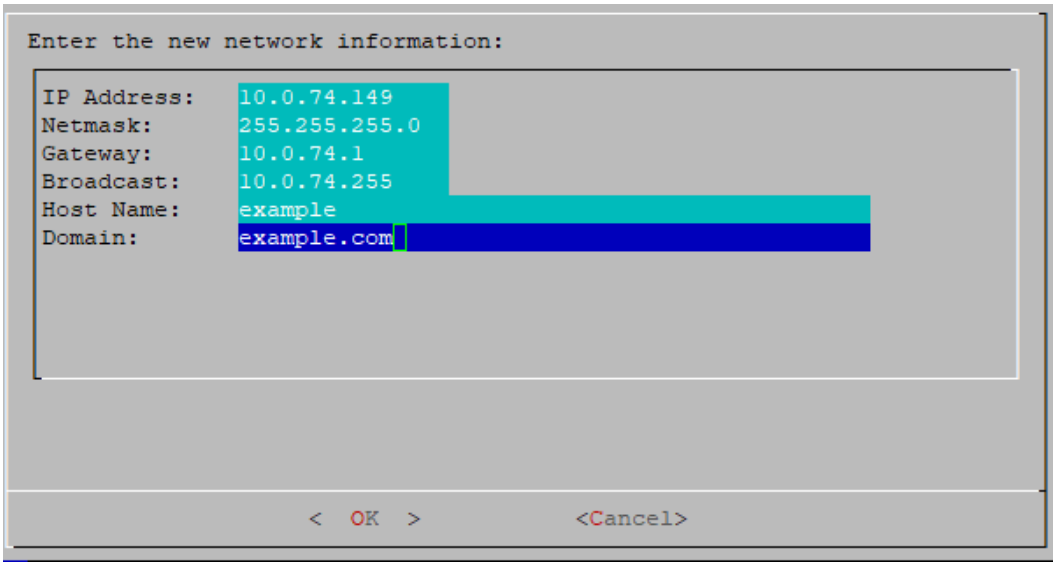


6. 데이터스토어 없이 Secure Network Analytics을 구축 중인지 확인합니다. **OK(확인)**를 선택하여 계속합니다.

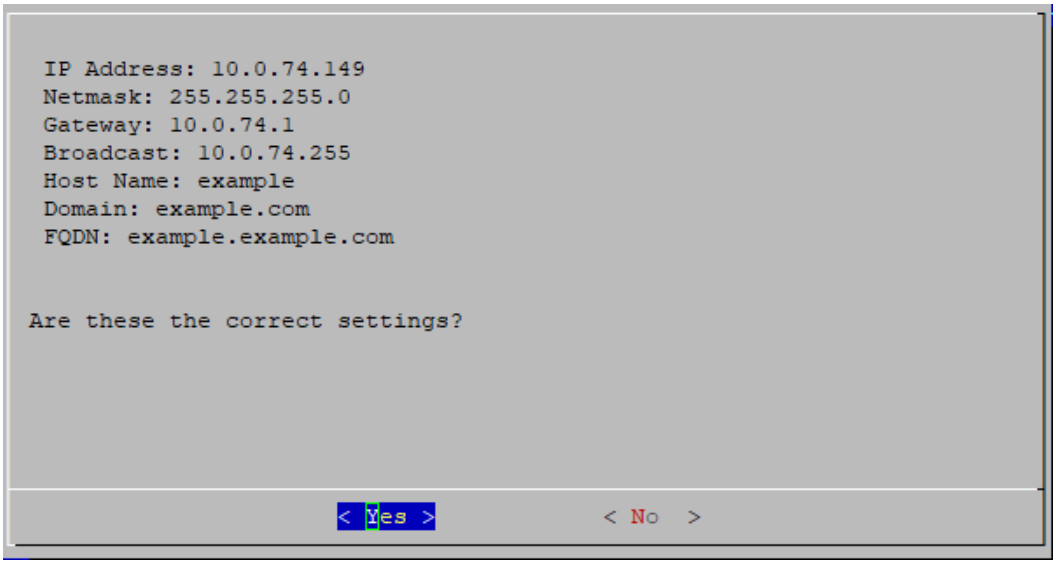


7. 관리 인터페이스 **IP 주소**, **넷마스크**, **게이트웨이**, **브로드캐스트**, **호스트 이름** 및 **도메인**을 입력합니다. **OK(확인)**를 선택하여 계속합니다.

> 각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.



8. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.

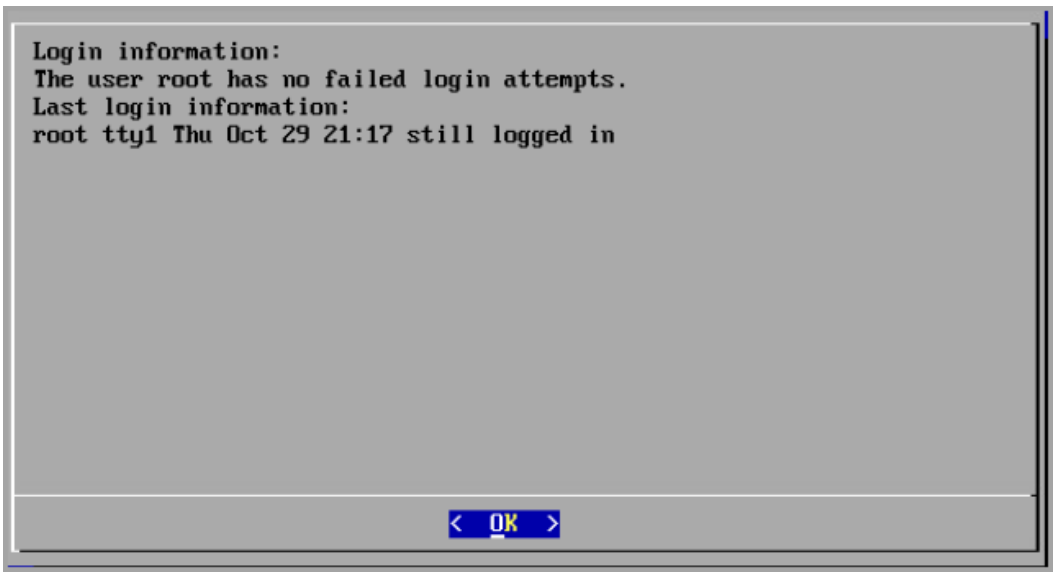


9. **OK(확인)**을 선택하여 선택을 확인합니다. 화면에 표시 되는 프롬프트에 따라 가상 환경을 종료하고 어플라이언스를 재시작합니다.
10. **Ctrl + Alt**를 눌러 콘솔을 종료합니다.
11. 시스템 다음 플로우 컬렉터에 대한 **데이터스토어**의 모든 단계를 반복합니다.

    - 최초 설정에서 데이터스토어없이 모든 플로우 컬렉터을 구성한 경우, 다음 섹션(**플로우 센서 또는 UDP Director**)로 이동하거나 **어플라이언스 구성 개요**로 돌아가 다른 어플라이언스를 구성합니다.
    - 최초 설정에서 모든 어플라이언스를 구성한 경우 **2. 매니지드 시스템 구성**

플로우 센서 또는 UDP Director 구성

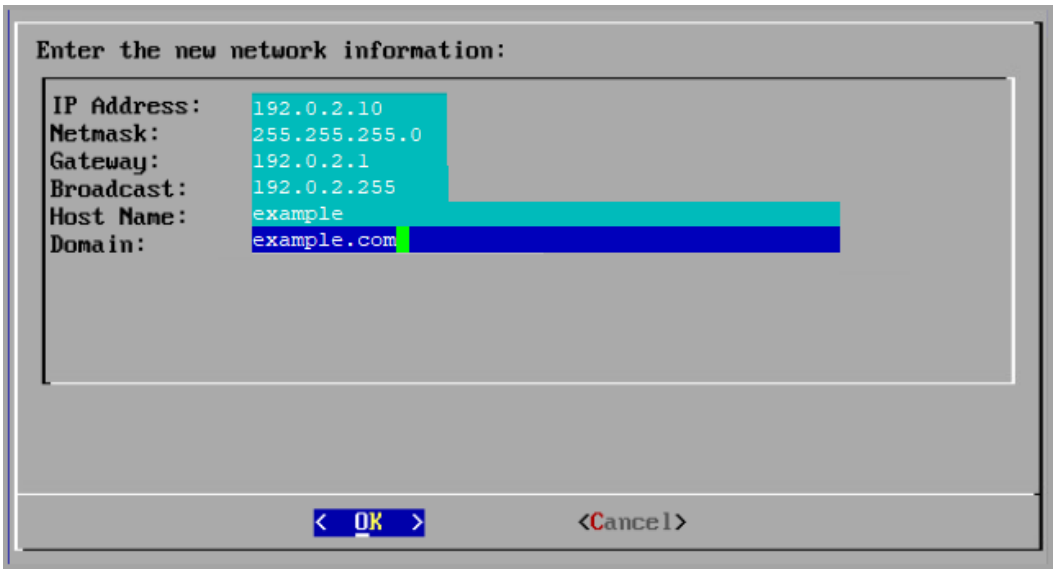
1. 콘솔을 통해 플로우 센서 또는 UDP Director다음에 로그인합니다.
   - **로그인:** sysadmin
   - **기본 비밀번호**: lan1cope
   - 시스템을 구성할 때 기본 비밀번호를 변경합니다.
2. 시스템 구성(`SystemConfig`)이 열립니다.
3. 실패한 로그인 시도 정보를 검토합니다. **OK(확인)**를 선택하여 계속합니다.



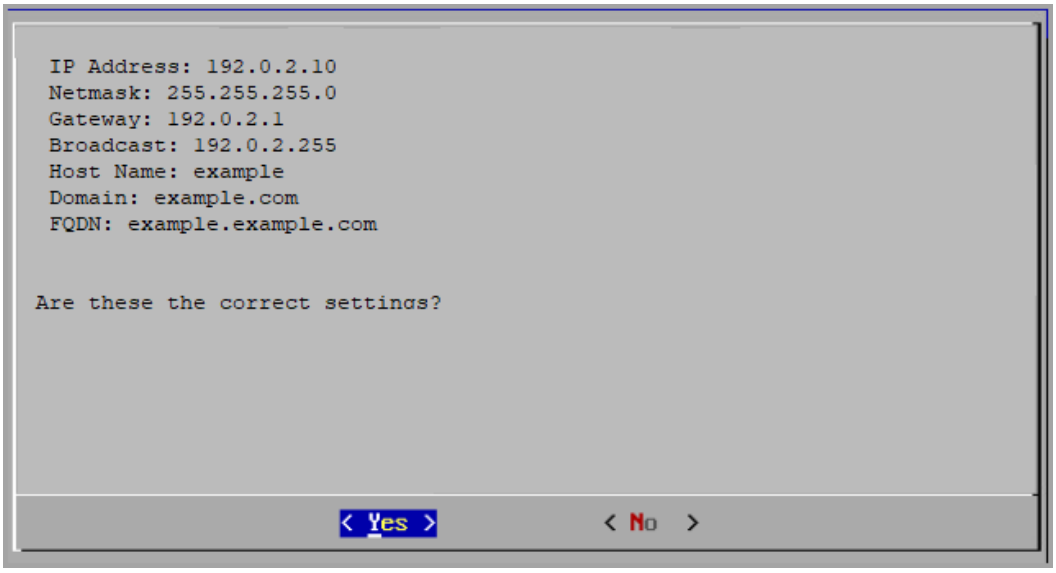
4. 최초 설정 소개를 검토합니다. **OK(확인)**를 선택하여 계속합니다.

5. 관리 인터페이스에 **IP 주소**, **넷마스크**, **게이트웨이**, **브로드캐스트**, **호스트 이름** 및 **도메인**을 입력하고, **OK(확인)**을 선택하여 계속합니다.

> 각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.



6. 설정을 확인합니다. **Yes(예)**를 선택하여 계속합니다.

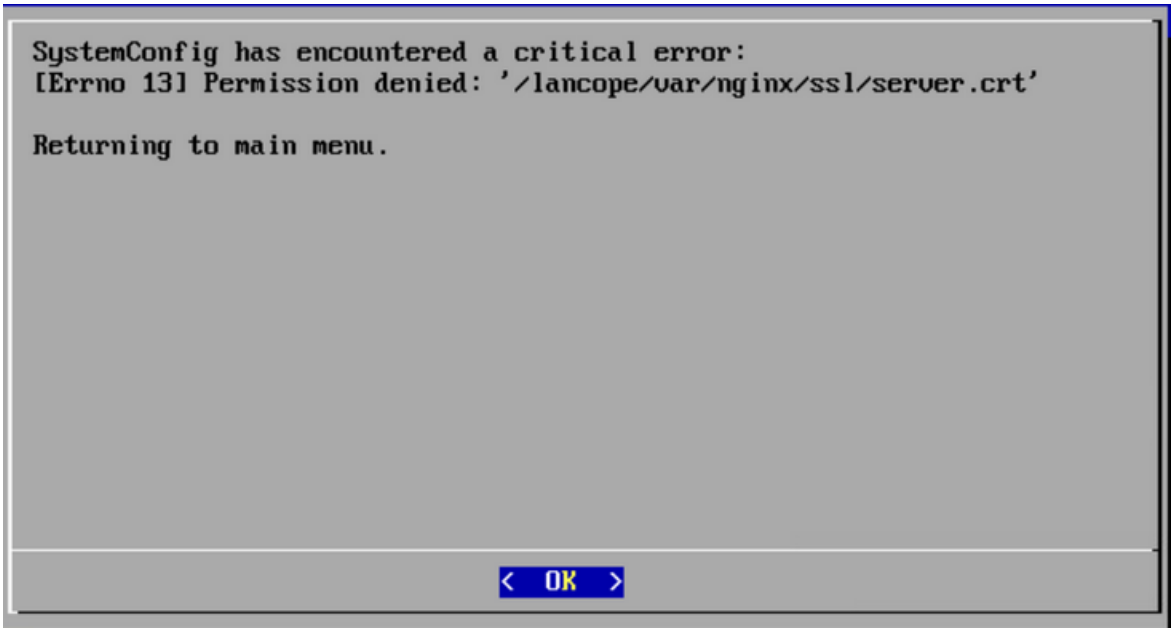


7. **OK(확인)**을 선택하여 선택을 확인합니다. 화면에 표시 되는 프롬프트에 따라 가상 환경을 종료하고 어플라이언스를 재시작합니다.
8. **Ctrl + Alt**를 눌러 콘솔을 종료합니다.
9. **플로우 센서 또는 UDP Director**의 모든 단계를 반복하여 시스템에서 다음 플로우 센서 또는 UDP Director를 구성합니다.

   최초 설정에서 모든 어플라이언스를 구성한 경우 **2. 매니지드 시스템 구성**

인증서 오류 문제 해결

VM 환경 사용량이 많은 경우 타이밍 오류가 발생할 수 있으며 일부 이벤트가 잘못된 순서로 발생할 수 있습니다. 인증서 오류(**.crt**)로 인해 권한이 거부되었다는 오류가 표시되면 다음을 수행합니다.



1. 어플라이언스 콘솔에 **sysadmin**으로 로그인합니다. 기본 비밀번호는 lan1cope입니다.
2. **Advanced(고급)** > **Root Shell(루트 셸)**을 선택합니다.
3. 다음 명령을 실행합니다.

   ```
   /lancope/admin/plugins/update/.98-FIX-SECRET-PERMS.sh
   ```

4. `SystemConfig`를 실행합니다.
5. 시스템 설정을 종료합니다.
6. **어플라이언스 구성 개요**로 돌아가 섹션의 모든 단계를 완료합니다. 어플라이언스에 액세스할 수 없는 경우 Cisco 지원팀에 문의하십시오.

어플라이언스에 액세스

어플라이언스를 재시작한 후에도 액세스할 수 없는 경우 다음을 수행합니다.

1. root로 로그인합니다.
2. 다음 명령을 실행하고 도커 컨테이너 및 서비스가 실행되고 있는지 확인합니다.
   - `docker ps`
   - `systemctl list-units --failed`
   - `systemd-analyze critical-chain`
3. 모든 도커 컨테이너와 서비스가 실행 중이면 로그인을 다시 시도합니다. 어플라이언스에 액세스할 수 없는 경우 Cisco 지원팀에 문의하십시오.

2. 매니지드 시스템 구성

어플라이언스에 처음 로그인할 때 어플라이언스 설정 도구를 사용하여 각 어플라이언스가 매니저에 의해 관리되도록 구성합니다.

준비

구성을 시작하기 전에 지침을 검토하여 어플라이언스 구성 순서, 모범 사례 및 추가 요구 사항을 파악합니다.

어플라이언스 설정 툴 요구 사항

- 방화벽 및 ACL(액세스 제어 목록)이 액세스를 허용하는지 확인합니다.
- 다음 항목에 대한 어플라이언스 및 IP 주소의 호스트 이름을 수집합니다.
    - 어플라이언스
    - 서브넷 마스크
    - 기본 브로드캐스트 게이트웨이
    - NTP 및 DNS 서버
    - 매니저 Central Management용 IP 주소

자세한 내용은 **어플라이언스 구성 요구 사항**을 참조하십시오.

매니지드 어플라이언스

어플라이언스 설정 도구의 일부로, 어플라이언스를 기본 매니저가 관리하도록 구성합니다.

매니저에서 어플라이언스를 관리하는 경우 Central Management를 사용하여 어플라이언스 구성을 편집하고, 소프트웨어를 업데이트하고, 재부팅하고, 종료하는 등의 작업을 수행할 수 있습니다.

매니저 페일오버

둘 이상의 매니저가 있는 경우 매니저 페일오버 쌍을 설정하여 하나가 다른 하나의 백업 콘솔로 사용되도록 할 수 있습니다.

- 어플라이언스 설정 도구를 사용해 개별 매니저를 구성합니다.
- 기본 및 보조 매니저를 계획합니다.
- 어플라이언스 설정 도구를 사용하여 두 매니저와 기타 모든 어플라이언스를 구성한 후 매니저 페일오버 관계를 정의합니다. 자세한 내용은 **3. 매니저 페일오버 관계**를 참조하십시오.

Secure Network Analytics 도메인

매니저를 구성할 때 Secure Network Analytics 어플라이언스에 대해 데이터 저장소 도메인 또는 비데이터 저장소 도메인을 생성합니다. Appliance Setup Tool(어플라이언스 설정 도구)에서

다른 어플라이언스를 구성할 때 생성한 도메인에 추가합니다. 자세한 내용은 **시스템 구성 계획**을 참조하십시오.

첫 번째 도메인으로 시스템 구성을 완료한 후 구성에 도메인을 추가할 수 있습니다(**도메인** 참조). 비 데이터스토어도메인으로 Secure Network Analytics를 구성하는 경우, 시스템 구성을 마친 후 구축에 데이터스토어를 추가할 수 있습니다. **비데이터 저장소 구축에 데이터 저장소 추가**의 지침을 따르십시오.

모범 사례

시스템을 성공적으로 구성하기 위해 이 가이드를 잘 따르십시오. 다음을 검토해야 합니다.

- **한 번에 하나씩:** 한 번에 하나의 어플라이언스를 구성합니다. 클러스터에서 다음 어플라이언스를 구성하기 전에 어플라이언스가 **Connected(연결됨)**(또는 **Data Store Not Initialized(데이터 저장소가 초기화되지 않음)** 상태인지 확인합니다.
- **순서:** 어플라이언스 설정 순서를 따르십시오.
- **여러 Central Manager:** 시스템에서 둘 이상의 Central Manager를 구성할 수 있습니다. 그러나 각 어플라이언스는 하나의 기본 매니저/Central Manager에서만 관리할 수 있습니다.
- **액세스:** Central Management에 액세스하려면 관리자 권한이 필요합니다.

어플라이언스 구성 순서

다음 순서로 어플라이언스를 구성하고 각 어플라이언스에 대한 세부 정보를 확인합니다.

주문	어플라이언스	세부 정보
1.	기본 매니저	기본 매니저는 Central Manager입니다. 시스템에서 다음 어플라이언스를 구성하기 전에 매니저가 **Connected(연결됨)** 상태인지 확인합니다. 매니저를 구성할 때 데이터 저장소가 있는 Secure Network Analytics 도메인(데이터 저장소 도메인) 또는 없는 데이터스토어(비데이터 저장소 도메인)을 생성합니다.
2.	모든 데이터 노드	데이터 저장소 구축에 필요합니다. 데이터 노드 어플라이언스 상태가 **데이터 저장소가 초기화되지 않음**인지 확인하고 클러스터에서 다음 어플라이언스를 구성합니다.
3.	플로우 컬렉터 5000 Series 데이터베이스	데이터베이스 어플라이언스의 상태가 **Connected(연결됨)**인지 확인하고 엔진 구성을 시작합니다. **데이터베이스 및 엔진 쌍:** 데이터베이스 및 엔진 쌍이 두 개 이상인 경우, 각 쌍을 한 번에 하나씩 설정합니다. 예를 들어, 쌍1(데이터베이스1 및 엔진1)을 구성한 다음 쌍 2(데이터베이스2 및 엔진2)를 구성합니다. 각 쌍에서 데이터베이스가 **Connected(연결됨)**로 표시되는지 확인하고 엔진 구성을 시작합니다. 또한 고유한 호스트 이름을 구성할 때 Central Management에서 식별할 수 있도록 각 데이터베이스 및 엔진 쌍의 이름을 지정합니다. 시스템 구성을 완료한 후 각 쌍의 신뢰 저장소에서 어플라이언스 ID 인증서를 검토할 수 있습니다. 자세한 내용은 **신뢰 저장소 인**

		증서 검토를 참조하십시오.
4.	플로우 컬렉터 5000 Series 엔진	플로우 컬렉터 5000 Series 데이터베이스가 **Connected(연결됨)** 상태인지 확인하고 엔진 구성을 시작합니다.
5.	기타 모든 플로우 컬렉터	**데이터 저장소가 있는 플로우 컬렉터**: 어플라이언스 상태가 **데이터 저장소가 초기화되지 않음**인지 확인하고 클러스터에서 다음 어플라이언스를 구성합니다. **데이터 저장소가 없는 플로우 컬렉터:** 어플라이언스 상태가 **Connected(연결됨)**인지 확인하고 클러스터에서 다음 어플라이언스를 설정합니다.
6.	UDP Director (FlowReplicators라고도 함)	UDP Director 어플라이언스 상태가 **Connected(연결됨)**인지 확인하고 클러스터에서 다음 어플라이언스를 설정합니다. UDP Director 대신 Cisco Telemetry Broker를 설치하는 경우, Secure Network Analytics 시스템 구성을 완료합니다. 그런 다음 Cisco Telemetry Broker 가상 어플라이언스 구축 및 구성 가이드의 지침을 따르십시오.
7.	플로우 센서s	플로우 센서 어플라이언스 상태가 **Connected(연결됨)**인지 확인하고 플로우 센서 구성을 시작합니다.
8.	보조 매니저 (사용되는 경우)	기본 매니저 어플라이언스 상태가 **Connected(연결됨)**으로 표시되는지 확인하고 보조 매니저 구성을 시작합니다. 보조 매니저는 자신을 Central Manager로 선택합니다. 어플라이언스 설정 도구를 사용하여 모든 어플라이언스를 설정한 후 페일오버를 설정합니다. 자세한 내용은 **3. 매니저 페일오버 관계**를 참조하십시오.

시스템에는 여기에 표시된 모든 어플라이언스가 없을 수 있습니다.

1. 어플라이언스 설정 도구에 로그인

어플라이언스 설정 도구를 사용하여 각 어플라이언스를 구성하려면 다음 지침을 따르십시오.

1. 브라우저의 주소 필드에 **https://** 를 입력한 후 어플라이언스의 IP 주소를 입력합니다.

    - **기본 매니저:** 기본 매니저를 먼저 구성합니다.
    - **Connected(연결됨):** 각 어플라이언스가 Connected(연결됨) 또는 Data Store Not Initialized(데이터 저장소가 초기화되지 않음) 상태인지 확인하고 클러스터에서 다음 어플라이언스를 구성합니다.
    - **순서:** 어플라이언스를 순서대로 구성하여 올바르게 통신하도록 합니다.

> 어플라이언스에 액세스할 수 없는 경우 1의 을 참조하십시오. 지침은 최초 설정을 사용하여 환경 구성을 참조하십시오.

2. 로그인하려면 다음 자격 증명을 입력합니다.

    - **사용자 이름:** admin
    - **비밀번호:** lan411cope

> 최초 설치가 아닌 경우 **문제 해결**(가이드의 끝 부분)로 이동하여 호스트 이름, 네트워크 도메인 이름 또는 IP 주소와 같은 어플라이언스 네트워크 설정을 변경합니다.

2. 어플라이언스 구성

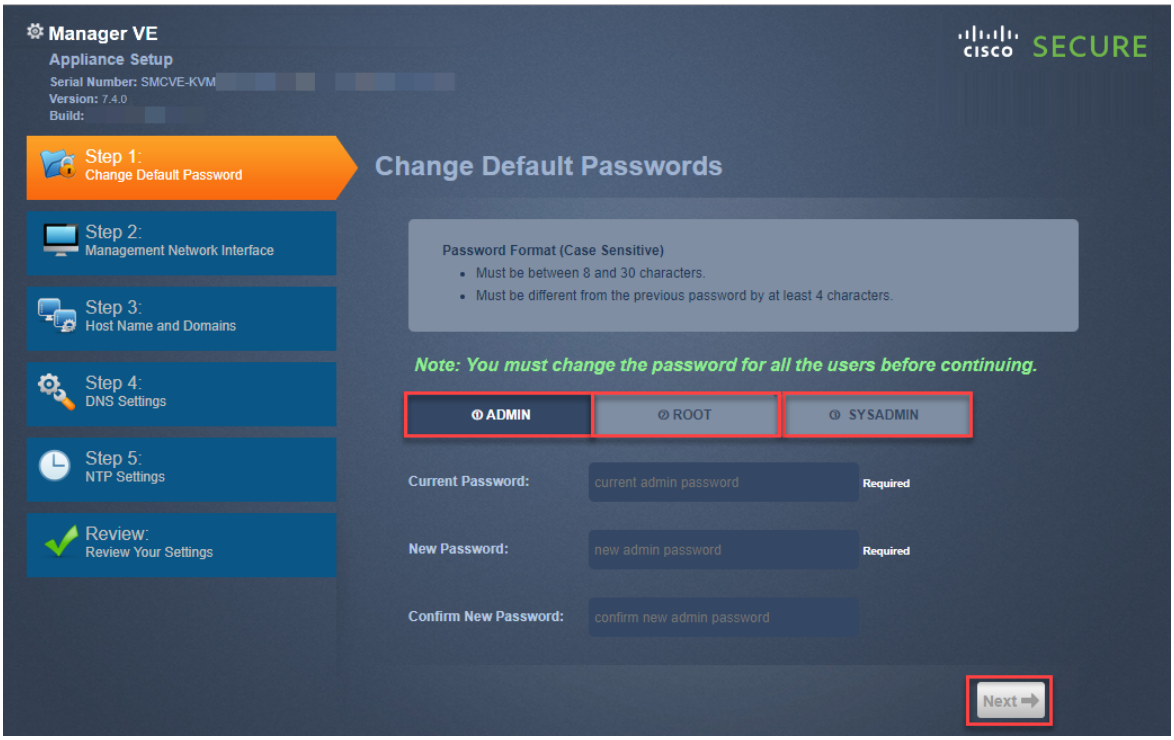
처음으로 어플라이언스에 로그인하면 어플라이언스 설정 툴이 각 설정 단계를 안내합니다.

1. **기본 비밀번호 변경:** admin, root, sysadmin에 대한 새 비밀번호를 입력합니다. **다음**을 클릭하여 각 사용자로 스크롤합니다.

   다음 기준을 사용합니다.

   - **길이:** 8~256 문자
   - **변경:** 새 비밀번호는 기본 비밀번호와 다르며 최소 4자 이상이어야 합니다.

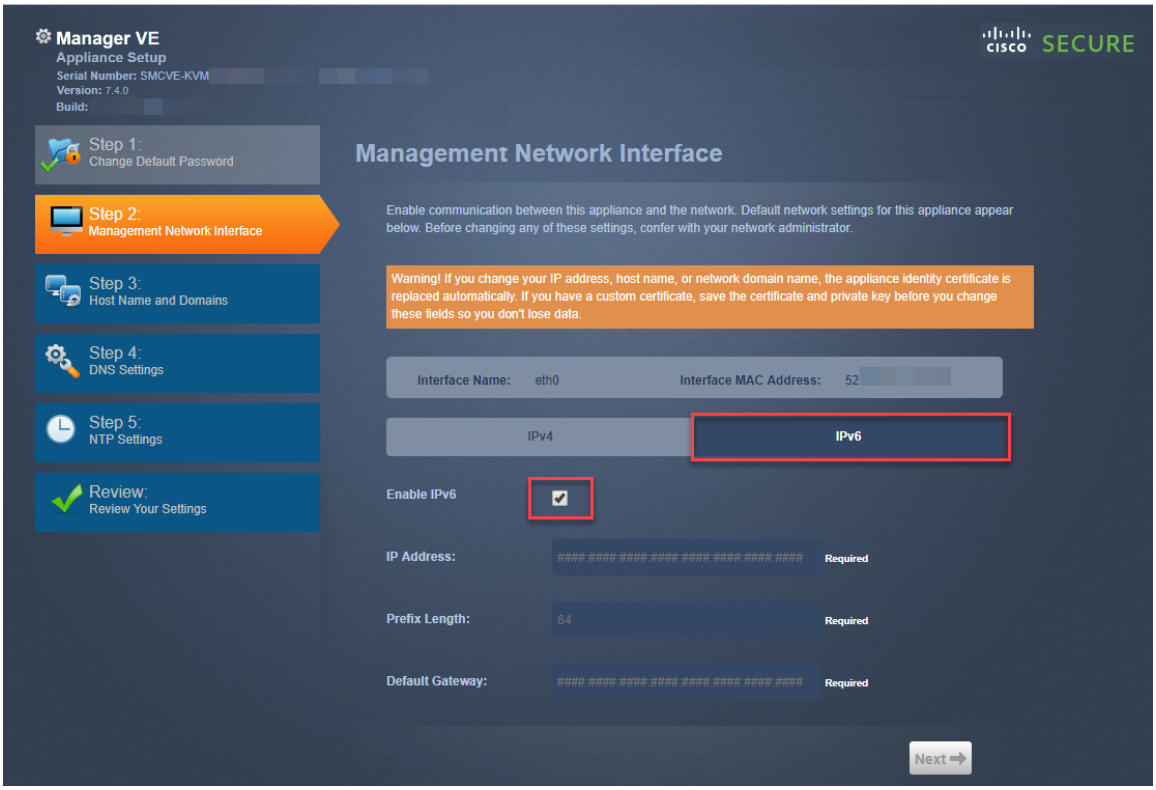
사용자	기본 비밀번호
관리자	lan411cope
root	lan1cope
sysadmin	lan1cope



> 하드웨어 설치 중 기본 비밀번호를 이미 변경한 경우 sysadmin 및 root 메뉴를 사용할 수 없습니다.

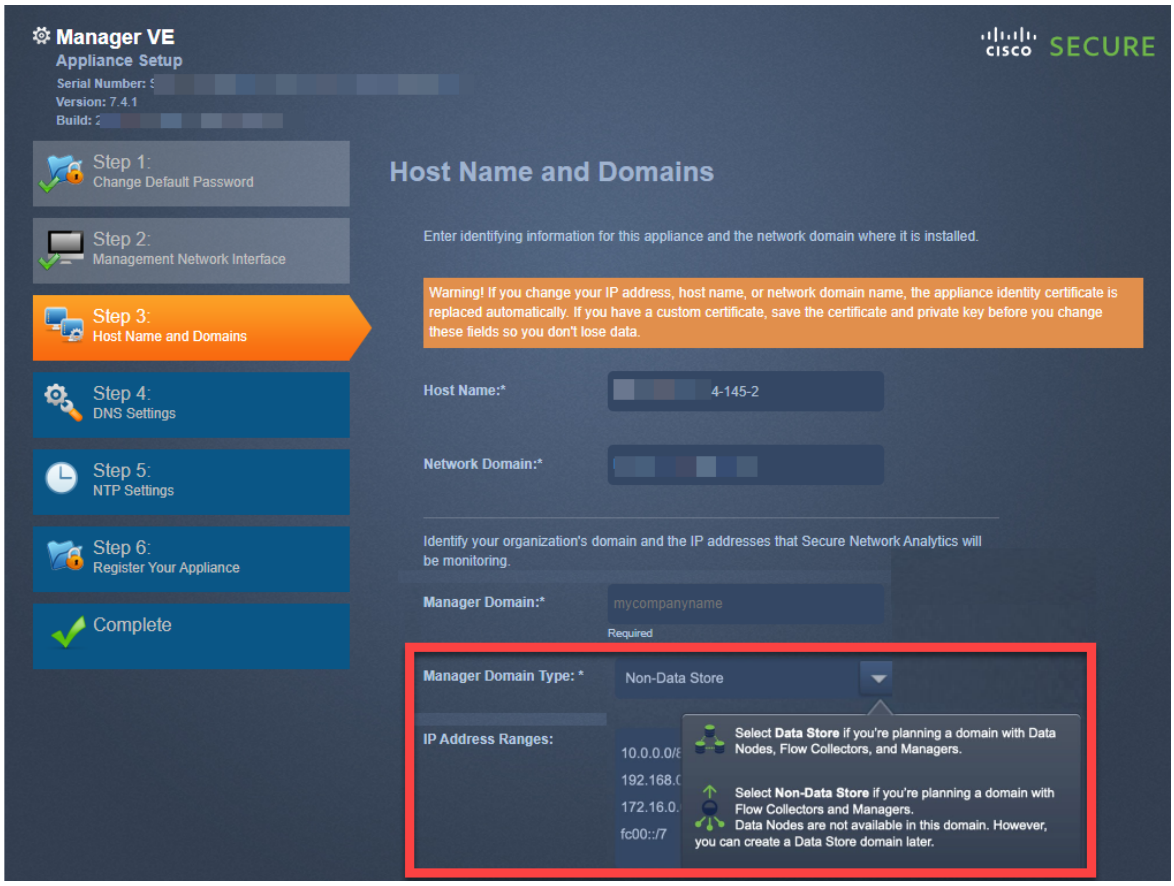
2. **관리 네트워크 인터페이스:** IP 주소 및 네트워크 인터페이스 필드를 검토합니다. 기본 설정이 올바른지 확인합니다. **다음**을 클릭합니다.

- **변경:** 이 정보를 변경하려면 네트워크 관리자와 협의하고 **문제 해결**을 참조합니다.
- **IPv6(선택 사항):** IPv6을 활성화하려면 **IPv6**을 클릭합니다. **IPv6 활성화** 체크 박스에 확인하고 필드를 채웁니다.



3. **호스트 이름 및 도메인**: 다음 정보를 입력합니다. **다음**을 클릭합니다.

필드 이름	참고
호스트 이름	각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 어플라이언스에 동일한 호스트 이름을 할당하면 어플라이언스가 성공적으로 설치되지 않습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다. **플로우 컬렉터5000 Series 데이터베이스 및 엔진 쌍:** 각 데이터베이스 및 엔진 쌍의 이름을 고유한 호스트 이름으로 지정하여 Central Management에서 쌍을 식별할 수 있게 합니다. 예를 들어 데이터베이스1과 엔진1, 데이터베이스2와 엔진2가 있습니다.
네트워크 도메인	각 어플라이언스에는 정규화된 도메인 이름이 필요합니다.
매니저 도메인 (매니저만 해당)	Secure Network Analytics 구축의 도메인 이름을 입력합니다.
매니저 도메인 유형 (매니저만 해당)	**데이터 저장소 도메인**: 최초 설정에서 데이터스토어으로 어플라이언스를 구성한 경우 데이터 저장소 도메인을 선택합니다. **비 데이터스토어 도메인:** 최초 설정에서 데이터스토어 없이 어플라이언스를 구성한 경우 비 데이터스토어 도메인을 선택합니다. 이 가이드의 시스템 구성을 완료한 후에 구축에 도메인을 추가할 수 있습니다. **도메인**을 참조하십시오.
IP 주소 범위 (매니저만 해당)	Secure Network Analytics 네트워크의 IP 주소 범위를 선택합니다.



4. **DNS 설정**: 기본값이 올바른지 확인하거나 도메인 서버 IP 주소를 입력합니다. **다음**을 클릭합니다.

   DNS 서버 추가 또는 삭제(선택 사항):

   - **추가:** + 아이콘을 클릭합니다.
   - **삭제:** DNS 서버를 선택하려면 이 체크 박스를 클릭합니다. - 아이콘을 클릭합니다.

5. **NTP 설정:** 기본값이 올바른지 확인하거나 **메뉴** 아이콘을 클릭하여 NTP(Network Time Protocol) 서버를 선택합니다. **다음**을 클릭합니다.

- **여러 NTP 서버:** 이중화 및 정확성을 위해 여러 NTP 서버를 설정하는 것이 좋습니다.
- **공개 소스:** pool.ntp.org는 우수한 NTP 공개 소스입니다.

NTP 서버 추가 또는 삭제(선택 사항):

- **추가:** + 아이콘을 클릭합니다.
- **삭제:** NTP 서버를 선택하려면 이 체크 박스를 클릭합니다. - 아이콘을 클릭합니다.

6. 기본 매니저는 Central Manager입니다. 다음과 같이 어플라이언스를 Central Management에 추가합니다.

   - **매니저:** 어플라이언스가 매니저인 경우, **3. 등록합니다. 매니저**를 등록합니다.
   - **기타 모든 어플라이언스:** 어플라이언스가 매니저이 아닌 경우 **4. Central Management에 어플라이언스 추가**

3. 등록합니다. 매니저

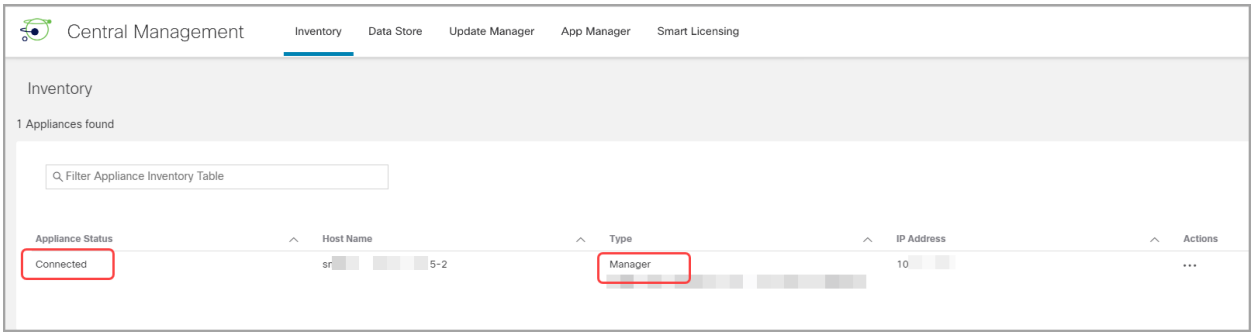
1. **설정 검토**: 어플라이언스 정보가 정확한지 확인합니다.
2. **적용** 또는 **재시작하고 계속**을 클릭합니다.

    - 어플라이언스가 다시 시작되는 동안 화면에 표시되는 프롬프트를 따르십시오.
    - 새 시스템 설정이 적용될 때까지 몇 분간 기다립니다. 페이지를 새로 고쳐야 할 수 있습니다.

3. 매니저에 로그인합니다.
4. 어플라이언스 설정 툴이 다시 열립니다. **Continue(계속)**를 클릭합니다.
5. 어플라이언스 등록 탭에서 IP 주소를 검토하고 **Save(저장)**를 클릭합니다.

    - 매니저 IP 주소는 자동으로 탐지되며 변경할 수 없습니다.
    - 이 단계에서는 매니저에 Central Management를 설치합니다.

6. 어플라이언스 설정이 완료되면 **Go to Dashboard(대시보드로 이동)**를 클릭합니다.
7. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
8. 인벤토리를 검토합니다. 매니저 어플라이언스 상태가 **Connected(연결됨)**으로 표시되는지 확인합니다.



> 기본 매니저 어플라이언스 상태가 연결됨으로 표시되는지 확인하고 구성 순서 및 세부 정보를 사용하여 클러스터의 다음 어플라이언스 구성을 시작합니다.

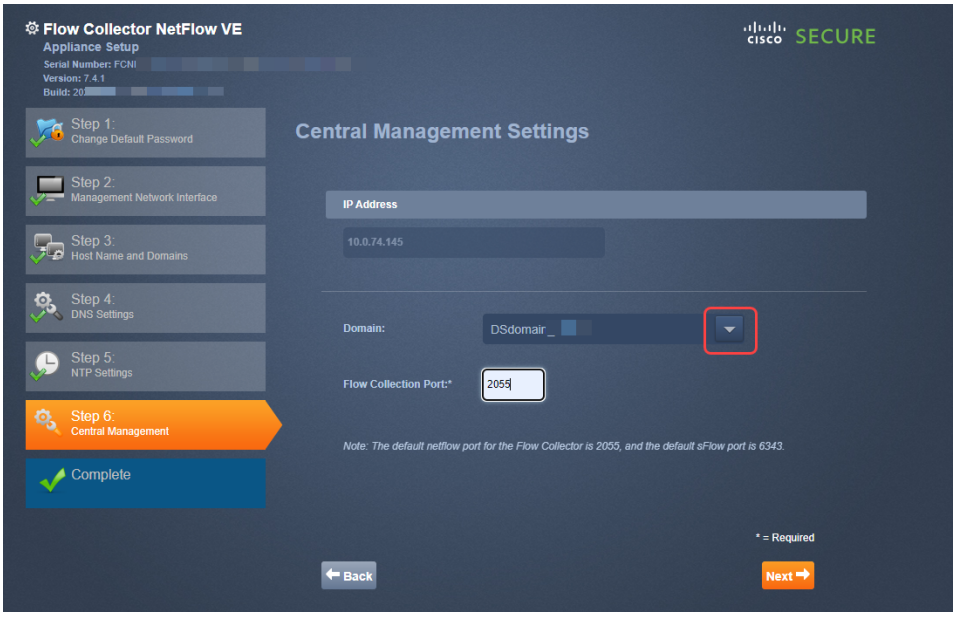
9. 시스템에서 다음 어플라이언스를 구성하려면 **1. 어플라이언스 설정 도구에 로그인**에 로그인하여 클러스터에서 다음 어플라이언스를 구성으로 이동합니다.

4. Central Management에 어플라이언스 추가

어플라이언스 설정 도구가 Central Management를 사용하는 어플라이언스 설정을 계속 안내합니다. 일부 단계는 어플라이언스에 따라 달라질 수 있습니다. 화면의 프롬프트를 따르십시오.

1. Central Management 탭에서 기본 매니저의 IP 주소를 입력합니다.
2. **Save(저장)**를 클릭합니다.
3. 기본 매니저 어플라이언스 ID 인증서를 신뢰하려면 화면에 표시되는 프롬프트를 따르십시오. **Yes(예)**를 클릭하여 인증서를 신뢰하고 어플라이언스가 매니저와 통신할 수 있도록 허용합니다.
4. 기본 매니저의 로그인 자격 증명을 입력합니다.
5. **Domain(도메인)**: Secure Network Analytics 도메인을 선택합니다. 매니저를 등록할 때 데이터 저장소 도메인 또는 비데이터 저장소 도메인으로 구성한 도메인입니다.
   - **플로우 컬렉터:** 플로우 컬렌션 포트 번호를 입력합니다. Netflow 기본값: 2055
   - **플로우 센서:** 플로우 컬렉터를 선택합니다.

Secure Network Analytics 도메인 선택



6. **Central Management로 이동**을 클릭합니다. **5. 어플라이언스 상태 확인**

5. 어플라이언스 상태 확인

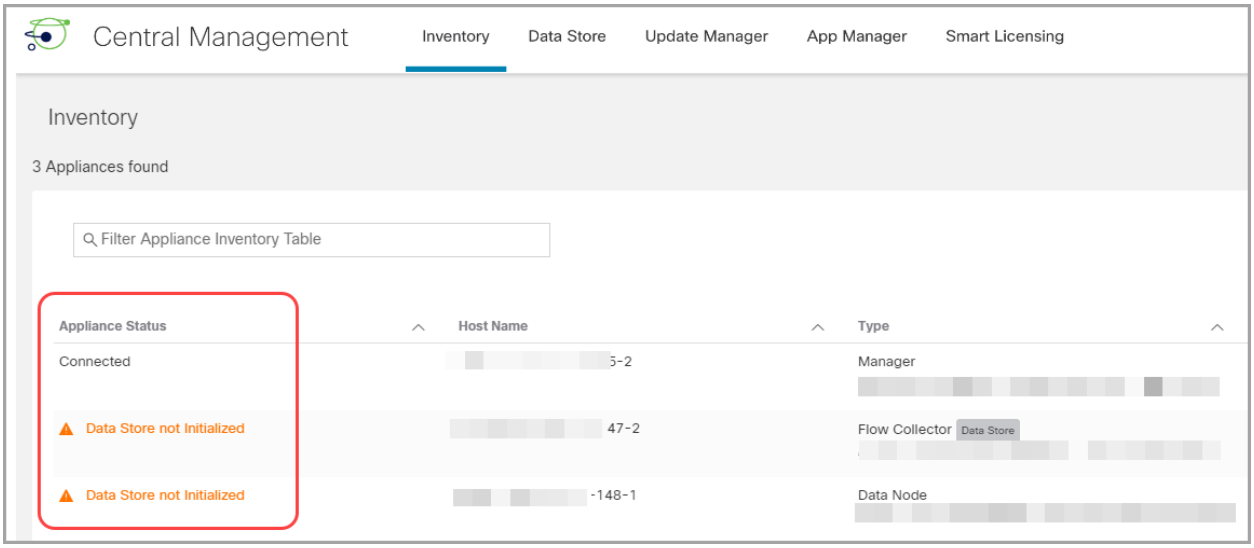
어플라이언스 설정 툴에서 어플라이언스를 설정하고 나면 Central Management에서 어플라이언스 상태를 확인합니다.

1. 어플라이언스 설정 도구에서 Central Management 인벤토리를 열거나 다음과 같이 열 수 있습니다.

   - 기본 매니저에 로그인합니다.
   - **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.

2. 인벤토리 탭의 어플라이언스를 검토합니다.

   - 어플라이언스가 인벤토리에 표시되는지 확인합니다.
   - **어플라이언스 상태:** 기본 매니저 및 각 어플라이언스가 **Connected(연결됨)**으로 표시되는지 확인하고 클러스터에서 다음 어플라이언스 구성을 시작합니다.
   - **Data Store Not Initialized(데이터 저장소가 초기화되지 않음)**: 데이터 저장소 도메인의 플로우 컬렉터 및 데이터 노드에 대해 어플라이언스 상태가 **데이터스토어Not Initialized(초기화되지 않음)**인지 확인합니다. 이후 절차에서 초기화를 완료하면 Connected(연결됨)로 표시됩니다.
   - **유형:** 플로우 컬렉터에 데이터스토어 태그가 있는 경우 데이터스토어 데이터베이스에 플로우를 전송하도록 구성됩니다.



> 기본 매니저 및 각 어플라이언스가 연결됨 또는 데이터 저장소가 초기화되지 않음으로 표시되는지 확인하고 구성 순서 및 세부 정보를 사용하여 클러스터의 다음 어플라이언스 구성을 시작합니다.

3. 시스템에서 다음 어플라이언스를 구성하려면 **1. 어플라이언스 설정 도구에 로그인**에 로그인하고 **5. 어플라이언스 상태 확인**

3. 매니저 페일오버 관계

정의

페일오버 구성이 두 개의 매니저 간 페일오버 을 설정하여 그 중 하나가 다른 하나의 백업 콘솔로 사용되도록 할 수 있습니다. Secure Network Analytics를 데이터 저장소에 구축한 경우, 데이터 저장소를 초기화하기 전에 페일오버를 구성해야 합니다.

보조 매니저가 없는 경우 **5. v7.4.2 패치 설치**

성공적인 페일오버 구성 및 작업을 위해서는 요구 사항을 검토하고 Secure Network Analytics 페일오버 구성 가이드의 지침을 따르십시오.

> 기본 매니저가 오프라인 상태가 되면 매니저가 역할을 자동으로 교체하지 않습니다. Secure Network Analytics페일오버 구성 가이드에 나와 있는 순서대로 매니저 역할을 변경해야 합니다.

데이터스토어

데이터 저장소와 함께 Secure Network Analytics를 구축한 경우, 페일오버를 구성한 다음 데이터 저장소를 초기화합니다. 데이터스토어를 초기화 후 페일오버를 구성하는 경우, Secure Network Analytics페일오버 구성 가이드의 지침에 따라 데이터스토어와의 보안 통신을 위한 보조 매니저를 구성합니다.

페일오버 구성

매니저를 페일오버 쌍으로 구성하려면 Secure Network Analytics페일오버 구성 가이드의 지침을 따르십시오.

가이드에는 다음을 포함하여 성공적인 구성에 중요한 세부 정보가 포함되어 있습니다.

- **인증서:** 어플라이언스 간의 통신을 위해 어플라이언스 간의 신뢰를 설정하려면 필요한 어플라이언스 신뢰 저장소에 올바른 인증서를 저장해야 합니다.
- **파일 백업:** 어플라이언스를 백업한 다음 페일오버 구성을 시작합니다.
- **구성 순서:** 페일오버를 위해 보조 매니저를 구성한 다음 기본 매니저를 구성합니다.
- **역할 변경:** 기본 매니저이 오프라인이 되면 가이드에 나와 있는 순서대로 매니저 역할을 변경해야 합니다. 이 순서가 중요하며 역할은 자동으로 교체되지 않습니다.
- **문제 해결:** 결책은 Secure Network Analytics페일오버 구성 가이드를 참조하십시오.

> 성공적인 구성 및 작업을 위해서는 Secure Network Analytics페일오버 구성 가이드의 지침을 따르십시오.

기본 및 보조 역할

구성 중에 기본 매니저 및 보조 매니저를 할당합니다. 구성을 저장하면 다음과 같은 일이 발생합니다.

- **기본 매니저**: 기본 매니저는 도메인 구성, 사용자 설정 및 정책을 보조 매니저에 푸시합니다. 기본 매니저을 사용해 어플라이언스를 관리하고, 어플라이언스 구성을 변경하고, 비밀번호를 변경하고, 알람을 정의하고, 정책을 적용하는 등의 작업을 수행합니다.
- **보조 매니저**: 보조 매니저는 해당 구성을 삭제하므로 기본 매니저 구성 및 설정과 동기화할 수 있습니다. 또한 보조 매니저가 모든 사용자에 대해 읽기 전용으로 변경됩니다. 그러면 보조 매니저의 섹션에 액세스할 수 없으며 보조 매니저에서 파일을 검색할 수 없습니다.

4. 사이트 이중화 구성

> 데이터스토어가 구성되어 있지 않거나 이중 사이트를 생성하지 않으려는 경우 **6. 초기화 데이터스토어**

사이트 이중화를 사용하면 유사한 어플라이언스로 별도 구축된 두 Cisco Secure Network Analytics 사이트의 클러스터에서 이중화에 가까운 방식을 설정할 수 있습니다. 사이트 이중화를 사용하면 기본 사이트에서 도메인 및 애널리틱스 설정을 유지하면서 이를 이중화 사이트와 수동으로 동기화할 수 있습니다. 또한 데이터 센터의 전원이 차단되는 경우 고가용성 보호 기능을 제공합니다. 사이트 이중화를 사용하면 이중화된 클러스터에 로그인하여 거의 동일한 데이터를 확인할 수 있습니다.

> 이 기능은 관리자 및 설정 관리자 역할만 사용할 수 있습니다.

사이트 이중화 설정 동기화에는 다음이 포함됩니다.

데이터스토어 도메인별 설정 및 알림 설정(활성화된 경우). 도메인 구성에는 다음이 포함됩니다.

- 호스트 그룹 관리
- 정책 관리
- 애플리케이션
- 엑스포터 SNMP 프로필(비밀번호 제외)
- 알람 심각도
- 서비스
- 도메인 AS 번호

애널리틱스 구성에는 다음 항목이 포함됩니다.

- 우선순위
- 국가 감시 목록
- 알림 만료

이중화 사이트 요구 사항

이중화 사이트 구성을 시작하기 전에 다음 요구 사항을 검토하십시오.

- 동일한 이름을 사용하여 기본 및 이중 사이트 모두에 이중 데이터스토어 도메인을 생성합니다. 두 사이트의 데이터스토어 도메인 수가 동일해야 하며 두 사이트의 데이터스토어 도메인 이름이 동일해야 합니다. 도메인에 대한 자세한 내용은 **도메인**을 참조하십시오.

> 사이트 이중화를 위해 데이터스토어 도메인만 동기화됩니다. 비데이터스토어도메인은 동기화되지 않습니다.

- 두 사이트의 Secure Network Analytics 소프트웨어 버전이 동일해야 합니다.
- 기본 매니저 신뢰 저장소에 이중화 매니저 인증서를 추가합니다. 자세한 내용은 신뢰 스토어에 인증서 추가를 참조하십시오.
- 기본 매니저 인증서를 이중화 매니저 신뢰 저장소에 추가합니다. 자세한 내용은 신뢰 스토어에 인증서 추가를 참조하십시오.

요구 사항을 완료하면 이중화 사이트 구성 절차를 진행할 수 있습니다.

신뢰 저장소에 인증서 추가

필수 어플라이언스 ID 인증서 및 체인을 신뢰 저장소에 저장하려면 다음 지침을 사용합니다.

신뢰 저장소 요구 사항

이 지침에서는 다음 요구 사항을 안내합니다.

- 기본 매니저 신뢰 저장소에 이중화 매니저 인증서 추가.
- 이중화 매니저 신뢰 저장소에 기본 매니저 인증서 추가.

인증서 체인

어플라이언스 ID 인증서에 인증서 체인이 있는 경우 해당 인증서 체인(루트 및 중가)을 신뢰 저장소에 추가하십시오.

신뢰 저장소에 인증서 업로드

각 파일을 개별적으로 업로드합니다.

1. 어플라이언스 ID 인증서 다운로드

다음 지침에 따라 어플라이언스 ID 인증서를 다운로드하고 저장합니다. 단계는 사용중인 브라우저에 따라 달라집니다.

인증서가 이미 저장되어 있는 경우 이 절차를 건너뛸 수 있습니다. **2. 매니저신뢰 저장소**

> 브라우저에서 잠금/보안 아이콘을 클릭할 수도 있습니다. 화면에 표시되는 프롬프트에 따라 인증서를 다운로드합니다. 단계는 사용중인 브라우저에 따라 달라집니다.

1. 브라우저 주소 표시 줄에서 IP 주소 뒤의 경로를 **/secrets/v1/server-identity**로 바꿉니다.

   예: https://<IPaddress>/secrets/v1/server-identity

2. 화면에 표시되는 프롬프트에 따라 인증서를 저장합니다.

   열기: 파일을 보려면 텍스트 파일 형식을 선택합니다.

   문제 해결: 인증서를 다운로드하라는 프롬프트가 표시되지 않으면 다운로드가 자동으로 되었을 수도 있는 만큼 다운로드 폴더를 확인하고 아니면 다른 브라우저를 사용해보십시

오.

3. 각 매니저에서 1단계와 2단계를 반복합니다.

2. 매니저신뢰 저장소에 인증서 추가

다음 지침에 따라 이중 매니저 어플라이언스 ID 인증서 및 체인(해당하는 경우)을 기본 매니저 신뢰 저장소에 저장합니다.

1. 매니저에 로그인합니다.
2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
3. 어플라이언스 상태가 Connected(연결됨)으로 표시되는지 확인합니다.
4. 매니저에 대한 **Actions(작업)** 메뉴를 클릭합니다.
5. **어플라이언스 설정 편집**을 선택합니다.
6. **Central Management 인벤토리 > 일반** 탭에서 **신뢰 저장소** 섹션을 찾습니다.
7. **새로 추가**를 클릭합니다.

> 각 어플라이언스 ID 인증서와 체인(루트 및 중간) 인증서를 개별적으로 업로드해야 합니다.

8. **식별 이름** 필드에 인증서의 이름을 입력합니다.
9. **Choose File(파일 선택)**을 클릭합니다. 인증서를 선택합니다.
10. **인증서 추가**를 클릭합니다. 신뢰 저장소 목록에 해당 인증서가 표시되는지 확인합니다.
11. 신뢰 저장소에 다른 필수 인증서를 추가하려면 6 ~ 9단계를 반복합니다.

    - 이중화 매니저에 로그인 한 경우 기본 매니저 인증서를 추가합니다.
    - 이중화 매니저에 로그인 한 경우 기본 매니저 인증서를 추가합니다.

12. **설정 적용**을 클릭합니다. 화면의 프롬프트를 따르십시오.
13. **Connected(연결됨):** Central Management 인벤토리 페이지에서 어플라이언스 상태가 Connected(연결됨)로 돌아오는지 확인합니다.
14. 다른 매니저에서 1~13단계를 반복합니다.

사이트 이중화 구성 열기

다음 지침에 따라 사이트 이중화 설정을 엽니다.

1. 매니저에 관리자 또는 구성 관리자로 로그인합니다.
2. 기본 메뉴에서 **Configure(구성) - GLOBAL Manager(전역 관리자)**를 선택합니다.
3. **사이트 이중화 구성** 탭을 클릭합니다.

이중화 사이트 구성

이중화 사이트를 구성하려면 다음 단계를 따르십시오.

1. **구성 활성화** 확인란을 선택합니다.
2. **이중화 사이트의 매니저 이름** 필드에 이중화 사이트의 매니저에 대한 FQDN(Fully Qualified Domain Name) 또는 IP 주소를 입력합니다. 참고로 매니저 이름은 매니저 ID 인증서의 공통 이름 또는 제목 대체 이름과 일치해야 합니다.
3. **Save(저장)** 버튼을 클릭하여 변경 사항을 저장합니다.
4. **Synchronize(동기화)** 버튼을 클릭하여 기본 사이트를 원격 사이트와 동기화합니다. 이렇게 하면 두 사이트 간에 도메인 구성 및 애널리틱스 구성이 동기화됩니다.
5. 화면에 표시되는 프롬프트에 따라 변경 사항을 동기화할 것임을 확인합니다. **Synchronize(동기화)**를 클릭하여 계속합니다.

   동기화가 진행 중임을 나타내는 "in progress(진행 중)" 줄임표 아이콘이 표시됩니다. 작업이 완료되면 성공 또는 실패 배너가 표시됩니다.

   > 동기화를 수행하면 프로세스에서 이중 사이트 플로우 컬렉터 엔진 구성을 덮어씁니다. 시간당 두 번 이상 동기화하지 않는 것이 좋습니다.

이중화 사이트 비활성화

이중화 사이트를 비활성화하려면 다음 단계를 수행합니다.

1. 이중화 사이트를 비활성화하려면 Enable Configuration(구성 활성화) 확인란을 선택 취소합니다.
2. **Save(저장)** 버튼을 클릭하여 변경 사항을 저장합니다. 이렇게 하면 이중화 사이트 및 Synchronize(동기화) 버튼이 비활성화됩니다.
3. (선택 사항) 비활성화된 이중 사이트의 사이트 인증서를 제거하면 Secure Network Analytics 시스템에 보호 레이어를 추가할 수 있습니다. 이중화 사이트 구성 절차 중에 추가한 사이트 인증서를 제거하려는 경우 다음 단계를 수행하여 인증서를 제거할 수 있습니다.
    1. 매니저에 로그인합니다.
    2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
    3. 어플라이언스 상태가 Connected(연결됨)으로 표시되는지 확인합니다.
    4. 매니저에 대한 **Actions(작업)** 메뉴를 클릭합니다.
    5. **어플라이언스 설정 편집**을 선택합니다.
    6. **Central Management 인벤토리 > 일반** 탭에서 **신뢰 저장소** 섹션을 찾습니다.
    7. **Actions(작업)** 열 아래에서 제거할 각 인증서에 대해 **Delete(삭제)**를 클릭합니다.

문제 해결

사이트 이중화 구성에 문제가 발생할 경우 다음을 확인합니다.

- 인증서가 올바른 신뢰 저장소에 있는지 확인합니다. 자세한 내용은 신뢰 스토어에 인증서 추가를 참조하십시오.
- Secure Network Analytics 소프트웨어 버전은 두 사이트에서 동일해야 합니다.
- 두 사이트에 있는 데이터스토어 도메인의 번호 및 이름이 일치해야 합니다.

로그 파일에서 오류를 검토하려면 /lancope/var/smc/log/smc-configuration.log로 이동합니다.

5. v7.4.2 패치 설치

어플라이언스에 최신 v7.4.2 패치를 설치합니다.

1. https://software.cisco.com에서 Cisco Software Central의 Cisco 스마트 어카운트에서 최신 **v7.4.2 패치**를 다운로드합니다.
2. 패치 readme 파일의 지침에 따라 각 패치를 설치합니다.
3. 어플라이언스를 최신 패치로 업데이트한 후 이 가이드의 다음 절차로 이동합니다.

   - **데이터 저장소 도메인:** **6. 초기화 데이터스토어**
   - **비데이터 저장소 도메인:** **7. 데스크톱 클라이언트 설치**

6. 초기화 데이터스토어

시스템 구성을 사용하여 데이터스토어를 초기화합니다. 이 절차의 일부로 SSH를 일시적으로 활성화합니다.

> 이 절차를 시작하기 전에 모든 어플라이언스를 Central Management 인벤토리에 추가합니다. 플로우 컬렉터는 데이터 저장소를 초기화하는 데 필요하지 않지만, 초기화 프로세스를 시작하기 전에 Central Management 인벤토리에 하나 이상의 데이터 노드와 매니저가 있어야 합니다.

1. 매니저 어플라이언스 콘솔(SystemConfig)에 root로 로그인합니다.
2. 기본 메뉴에서 **Data Store(데이터 저장소)**를 선택합니다.
3. **SSH**를 선택합니다. 화면에 표시되는 프롬프트에 따라 SSH를 활성화합니다.
4. 메뉴에서 Initialization(초기화)을 선택합니다.데이터스토어
5. 화면의 지시에 따라 데이터스토어를 초기화합니다.

   데이터스토어 메뉴를 종료하면 이전 SSH 설정이 복원됩니다.

6. 다음 절차로 이동합니다. **8. 통신 확인**

7. 데스크톱 클라이언트 설치

> v7.4.0부터는 SMC의 이름이 매니저로 변경되었습니다. 이 섹션에서는 SMC를 매니저이라고 합니다.

> Secure Network Analytics 시스템에 데이터스토어 플로우 컬렉터만 구축된 경우 데스크탑 클라이언트를 사용하지 않습니다. 하이브리드데이터스토어/비데이터스토어 시스템의 경우, 데스크탑 클라이언트은 비데이터스토어 도메인에서만 작동합니다.

다음 정보는 데스크톱 클라이언트 설치 및 사용 시 적용됩니다.

- 다른 버전의 데스크톱 클라이언트를 로컬로 설치할 수 있습니다.
- 데스크톱 클라이언트에는 Stealthwatch Management Console 및 SMC(매니저)와 같은 Stealthwatch 용어가 포함되어 있습니다.
- 여러 버전의 데스크톱 클라이언트에 액세스하려는 경우 각 매니저에 대해 다른 실행 파일이 필요합니다.
- 기본 및 보조 매니저를 모두 사용하는 경우 다른 매니저에 로그인하기 전에 하나의 매니저에서 로그아웃해야 합니다.
- 서로 다른 버전의 데스크톱 클라이언트를 동시에 열 수 있습니다.
- Secure Network Analytics의 이후 버전으로 업데이트하는 경우 데스크톱 클라이언트의 새 버전을 설치해야 합니다.
- 데이터스토어를 구축하는 경우 웹 애플리케이션을 사용하여 Secure Network Analytics 설치를 모니터링하고 구성합니다. 데스크톱 클라이언트는 데이터스토어과 호환되지 않습니다.

데스크톱 클라이언트 설치 지침은 Windows와 macOS에 따라 다릅니다.

- **Windows를 사용하여 데스크톱 클라이언트 설치**
- **macOS를 사용하여 데스크톱 클라이언트 설치**

또한 Windows 또는 macOS를 사용하는지에 따라 메모리 크기를 다르게 변경합니다.

- **Windows 탐색기에서 메모리 크기 변경**
- **파인더에서 메모리 크기 변경**

Windows를 사용하여 데스크톱 클라이언트 설치

- 데스크톱 클라이언트를 설치할 수 있는 충분한 권한이 있어야 합니다.
- 데스크톱 클라이언트에는 64비트 운영 체제가 필요합니다. 32비트 운영 체제 또는 Linux에서 실행할 수 없습니다.

Windows를 사용해 데스크톱 클라이언트를 설치하려면 다음 지침을 따르십시오.

1. 매니저에 로그인합니다.
2. (**다운로드**) 아이콘를 클릭합니다.
3. .exe 파일을 클릭하여 설치 프로세스를 시작합니다.
4. 마법사의 단계에 따라 데스크톱 클라이언트를 설치합니다.
5. 바탕 화면에서 데스크톱 클라이언트 아이콘을 클릭합니다.
6. **SMC 서버 이름** 필드에서 매니저 서버 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
7. 매니저 사용자 이름과 비밀번호를 입력합니다.
8. 화면에 표시되는 프롬프트에 따라 데스크톱 클라이언트를 열고 어플라이언스 ID 인증서를 신뢰합니다.

Windows 탐색기에서 메모리 크기 변경

데스크톱 클라이언트 인터페이스를 실행하기 위해 클라이언트 컴퓨터에 할당할 RAM(Random Access Memory)의 양을 변경할 수 있습니다.

열려 있는 많은 문서 또는 대량의 데이터 집합(예: 100k 레코드 이상을 사용하는 플로우 쿼리)으로 작업하는 경우 메모리 할당을 늘려 보십시오.

1. Windows Explorer에서 홈 디렉토리로 이동합니다.
2. AppData (앱데이터) > Roaming(로밍) > Stealthwatch 폴더를 엽니다.

   폴더가 숨겨져 있는 경우 "Stealthwatch"를 검색해야 할 수 있습니다.
3. Stealthwatch 디렉토리에서 원하는 Stealthwatch 버전이 포함된 폴더를 엽니다.
4. 편집을 시작하려면 적절한 편집 애플리케이션을 사용하여 **application.vmoptions** 파일을 엽니다. (데스크톱 클라이언트를 처음으로 연 후에 이 파일이 생성됩니다.)

   최소 메모리 크기(Xms): 512MB 이상을 할당하는 것이 좋습니다. 이 숫자는 파일의 세 번째 열에 표시됩니다.

   하나의 연속 라인에 콘텐츠를 표시하는 편집기의 경우 아래 이미지에서 강조 표시된 숫자를 참조해 최소 메모리 크기를 나타내는 숫자를 확인합니다.

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

최대 메모리(Xmx): 최대 메모리 크기는 컴퓨터 RAM 크기의 절반까지 할당할 수 있습니다. 이 숫자는 파일의 네 번째 열에 표시됩니다.

하나의 연속 라인에 콘텐츠를 표시하는 편집기의 경우 아래 이미지에서 강조 표시된 숫자를 참조해 최대 메모리 크기를 나타내는 숫자를 확인합니다.

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

전체 숫자를 사용합니다. 예를 들면 Xmx0.5m이 아닌 Xmx512m를 입력합니다.

- 데스크톱 클라이언트가 자주 "중단"되면 메모리 크기를 늘립니다.
- Java와 관련된 오류 메시지가 표시되면 메모리 할당을 줄여 보십시오.

macOS를 사용하여 데스크톱 클라이언트 설치

- 데스크톱 클라이언트를 설치할 수 있는 충분한 권한이 있어야 합니다.
- 데스크톱 클라이언트에는 64비트 운영 체제가 필요합니다. 32비트 운영 체제 또는 Linux에서 실행할 수 없습니다.

macOS를 사용해 데스크톱 클라이언트를 설치하려면 다음 지침을 따르십시오.

1. 매니저에 로그인합니다.
2. (**다운로드**) 아이콘를 클릭합니다.
3. .dmg 파일을 클릭하여 설치 프로세스를 시작합니다.

   아래에 표시된 것처럼 아이콘과 폴더가 모니터에 표시됩니다.

4. 데스크톱 클라이언트 아이콘()을 애플리케이션 폴더로 드래그합니다.

   실행 패드에 아이콘이 추가됩니다.

5. 바탕 화면에서 데스크톱 클라이언트 아이콘을 클릭합니다.
6. **SMC 서버 이름** 필드에서 매니저 서버 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
7. 매니저 사용자 이름과 비밀번호를 입력합니다.
8. 화면에 표시되는 프롬프트에 따라 데스크톱 클라이언트를 열고 어플라이언스 ID 인증서를 신뢰합니다.

파인더에서 메모리 크기 변경

데스크톱 클라이언트 인터페이스를 실행하기 위해 클라이언트 컴퓨터에 할당할 RAM(Random Access Memory)의 양을 변경할 수 있습니다.

열려 있는 많은 문서 또는 대량의 데이터 집합(예: 100k 레코드 이상을 사용하는 플로우 쿼리)으로 작업하는 경우 메모리 할당을 늘려 보십시오.

1. Finder에서 홈 디렉토리로 이동합니다.
2. Stealthwatch 폴더를 엽니다.
3. Stealthwatch 디렉토리에서 원하는 Stealthwatch 버전이 포함된 폴더를 엽니다.

4. 편집을 시작하려면 적절한 편집 애플리케이션을 사용하여 application.vmoptions 파일을 엽니다. (데스크톱 클라이언트를 처음으로 연 후에 이 파일이 생성됩니다.)

   최소 메모리 크기(Xms): 512MB 이상을 할당하는 것이 좋습니다. 이 숫자는 파일의 세 번째 열에 표시됩니다.

   하나의 연속 라인에 콘텐츠를 표시하는 편집기의 경우 아래 이미지에서 강조 표시된 숫자를 참조해 최소 메모리 크기를 나타내는 숫자를 확인합니다.

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   최대 메모리 크기(Xmx): 최대 메모리 크기에 대한 컴퓨터 RAM 크기의 절반을 할당할 수 있습니다. 이 숫자는 파일의 네 번째 열에 표시됩니다.

   하나의 연속 라인에 콘텐츠를 표시하는 편집기의 경우 아래 이미지에서 강조 표시된 숫자를 참조해 최대 메모리 크기를 나타내는 숫자를 확인합니다.

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   전체 숫자를 사용합니다. 예를 들면 Xmx0.5m이 아닌 Xmx512m를 입력합니다.

- 데스크톱 클라이언트가 자주 "중단"되면 메모리 크기를 늘립니다.
- Java와 관련된 오류 메시지가 표시되면 메모리 할당을 줄여 보십시오.

8. 통신 확인

1. 플로우 수집 트렌드 검토

1. 기본 매니저에 로그인합니다.

   페일오버 구성: 기본 매니저 및 보조 매니저다음에 로그인합니다.

2. 플로우 수집 트렌드 검토

2. 데이터 저장소 데이터베이스 상태 확인

> Secure Network Analytics를 데이터 저장소와 함께 구축하지 않은 경우에는 **3. 보고서 실행 보고서 작성기**.

1. 기본 매니저 대시보드에서 **Configure(구성) > GLOBAL Central Management(전역 Central Management)**를 선택합니다.
2. **데이터스토어** 탭을 클릭합니다.
3. 데이터스토어 데이터베이스 상태가 Up(작동)으로 표시되는지 확인합니다.

   데이터베이스 상태가 Down(중단)인 경우 데이터베이스의 Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다. **Start(시작)**를 선택합니다.

4. 모든 데이터 노드의 상태가 Up(작동)으로 표시되는지 확인합니다.

   데이터 노드 상태가 Down(중단)인 경우 데이터 노드에 대한 Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다. **Start(시작)**를 선택합니다.

데이터스토어 탭에 대한 자세한 내용은 **데이터 저장소 데이터베이스**를 참조하십시오.

3. 보고서 실행 보고서 작성기

1. 보안 정도 대시보드로 돌아갑니다.
2. **Report(보고서)** 메뉴를 선택합니다.
3. **Report Builder(보고서 작성기)**를 선택합니다.
4. **Create New Report(새 보고서 생성)**를 클릭합니다.
5. **플로우 컬렉터별 플로우 수집 트렌드** 템플릿을 클릭합니다.
6. 필요에 따라 파라미터를 선택합니다. **Run(실행)**을 클릭합니다.
7. 보고서를 검토하여 플로우 컬렉터가 플로우를 수신하고 있는지 확인합니다.
8. 플로우 컬렉터 데이터베이스(5000 Series만 해당) 또는 데이터 저장소가 있는 경우, 보고서 작성기 대시보드로 돌아와서 4~7단계를 반복하여 **플로우 데이터베이스 수집 트렌드 보고서**를 실행합니다. 데이터베이스 또는 데이터 저장소가 플로우를 수신하는지 확인합니다.

Report Builder(보고서 작성기)에 대한 자세한 내용은 도움말의 해당 정보를 참조하십시오.

9. 어플라이언스 구성 종료

어플라이언스에 대한 필수 구성을 완료해야 합니다.

어플라이언스	필수 설정	선택 설정
데이터 노드	없음	데이터 압축 플로우 인터페이스 통계
플로우 컬렉터s	없음	NetFlow를 sFlow로 변경
UDP Directors	없음	고가용성 (하드웨어에서만 사용 가능)
플로우 센서s	애플리케이션 ID와 페이로드	애플리케이션 식별

플로우 설정 변경 플로우 컬렉터

1. 플로우 컬렉터에 로그인합니다.
2. **Support(지원)** > **Advanced Settings(고급 설정)**을 클릭합니다.
3. **engine_startup_mode** 필드에서 다음 값 중 하나를 입력합니다.

   - 모델 파일의 기본값 - 0
   - NetFlow -1
   - sFlow-2

> engine_startup_mode 필드가 고급 설정 목록에 나타나지 않을 경우, Add New Option (새 옵션 추가) 및 Option Value(옵션 값 추가) 필드를 사용하여 페이지 아래쪽에 추가할 수 있습니다.

4. **Apply(적용)**을 클릭하고 **OK(확인)**을 클릭합니다.
5. 매니저에 로그인합니다.
6. **Configure(구성)** > **SYSTEM 플로우 컬렉터을 선택합니다**.
7. Monitor Port(모니터 포트) 필드에 다음 숫자 값을 입력합니다(NetFlow 및 sFlow용 업계 표준 기본 포트 번호입니다. 엑스포터가 비표준 포트를 사용하도록 구성된 경우, 해당 포트 번호를 대신 사용).

   - 2055 - NetFlow
   - 6343 - sFlow

8. **Save(저장)**을 클릭하여 변경 사항을 저장합니다.

   모드 전환(NetFlow에서 sFlow 또는 sFlow에서 NetFlow로)이 완료되면 이전 모드의 플로우를 기반으로 하는 다음 항목이 지워집니다.

   - 캐시: 호스트 캐시, 플로우 캐시, 보안 이벤트 캐시
   - 저장된 베이스라인 파일

대시보드에서 플로우 트렌드 그래프를 확인하여 플로우가 새 모드에서 처리되고 있는지 확인하여 모드 전환을 확인할 수 있습니다.

고가용성을 위한 UDP Director의 구성(하드웨어만 해당)

UDP Director를 고가용성 쌍으로 구성하려면 다음 지침을 사용합니다.

> 고가용성은 UDP Director 하드웨어 어플라이언스에서만 사용이 가능합니다. 가상 어플라이언스에는 고가용성이 제공되지 않습니다.

- **전달 규칙:** 고가용성을 설정할 계획이라면 하나 이상의 전달 규칙을 설정합니다. **전달 규칙 구성**을 참조하십시오.
- **고가용성:** UDP Director가 두 개 이상인 경우 고가용성 쌍을 설정할 수 있습니다. 고가용성을 설정하려는 경우 하나 이상의 전달 규칙을 설정합니다(**고가용성 구성** 참조).

전달 규칙 구성

SSL은 UDP Director에서 매니저로 메시지를 전송하는 데 사용됩니다.

1. 매니저에 로그인합니다.
2. **Configure(구성) > GLOBAL(전역)UDP Director**을 선택합니다.
3. 어플라이언스에 대한 **작업** 메뉴를 클릭합니다. **전달 규칙 설정**을 선택합니다.
4. **새 규칙 추가**를 클릭합니다.
5. **설명:** 규칙을 식별하기 위한 간략한 설명을 입력합니다.
6. **소스 IP 주소:포트:** UDP Director에 데이터를 전송하는 디바이스의 IP 주소를 입력하고 데이터가 전달될 포트 번호를 입력합니다.

   - **형식:** [IP 주소]:[포트 번호] 구문을 사용합니다.
   - **범위:** CIDR(Classless Inter-Domain Routing) 표시법을 사용하여 IP 주소 범위를 입력할 수 있습니다.
   - **모두:** "모두"를 입력하여 이 포트에서 모든 소스 IP 주소의 데이터를 수락할 수 있습니다.
   - **조합:** 소스 IP 주소:포트 조합을 규칙 내에 새 문자열로 추가할 수 있습니다.

   예:

   - 10.11.16.38:5322
   - 192.168.0.0/16:9000
   - All:2055

7. **대상 IP 주소:** UDP Director에서 데이터를 수신하는 디바이스의 IP 주소를 입력합니다.
8. **대상 포트 번호:** 수신하는 디바이스의 포트 번호를 입력합니다.
9. **Save(저장)**를 클릭합니다.
10. **선택 사항:** 변경 사항을 동기화하려면 동기화를 클릭합니다.
11. 필요에 따라 이 과정을 반복하여 전달 규칙을 추가합니다.
12. 고가용성 쌍을 설정하려면 **고가용성 구성**으로 이동합니다.

> 고가용성은 UDP Director 하드웨어 어플라이언스에서만 사용이 가능합니다. 가상 어플라이언스에는 고가용성이 제공되지 않습니다.

고가용성 구성

UDP Director가 두 개 이상인 경우 어플라이언스 관리자 인터페이스를 사용하여 고가용성을 구성합니다.

> 고가용성은 UDP Director 하드웨어 어플라이언스에서만 사용이 가능합니다. 가상 어플라이언스에는 고가용성이 제공되지 않습니다.

UDP Director HA(고가용성)를 통해 사용자는 이중화된 UDP Director에 대한 설정을 구성할 수 있습니다. 두 노드 모두 완전히 이중화되지만 한 번에 하나의 노드만 온라인 상태가 됩니다.

> UDP Director에 고가용성이 구성되어 있고 Secure Network Analytics를 버전 7.4.0 이상으로 업데이트하는 경우, 아래 지침에 따라 업데이트 후 고가용성을 다시 구성합니다.
> Secure Network Analytics 업데이트에 대한 자세한 내용은 업데이트 가이드를 참조하십시오.

기본 노드 및 보조 노드

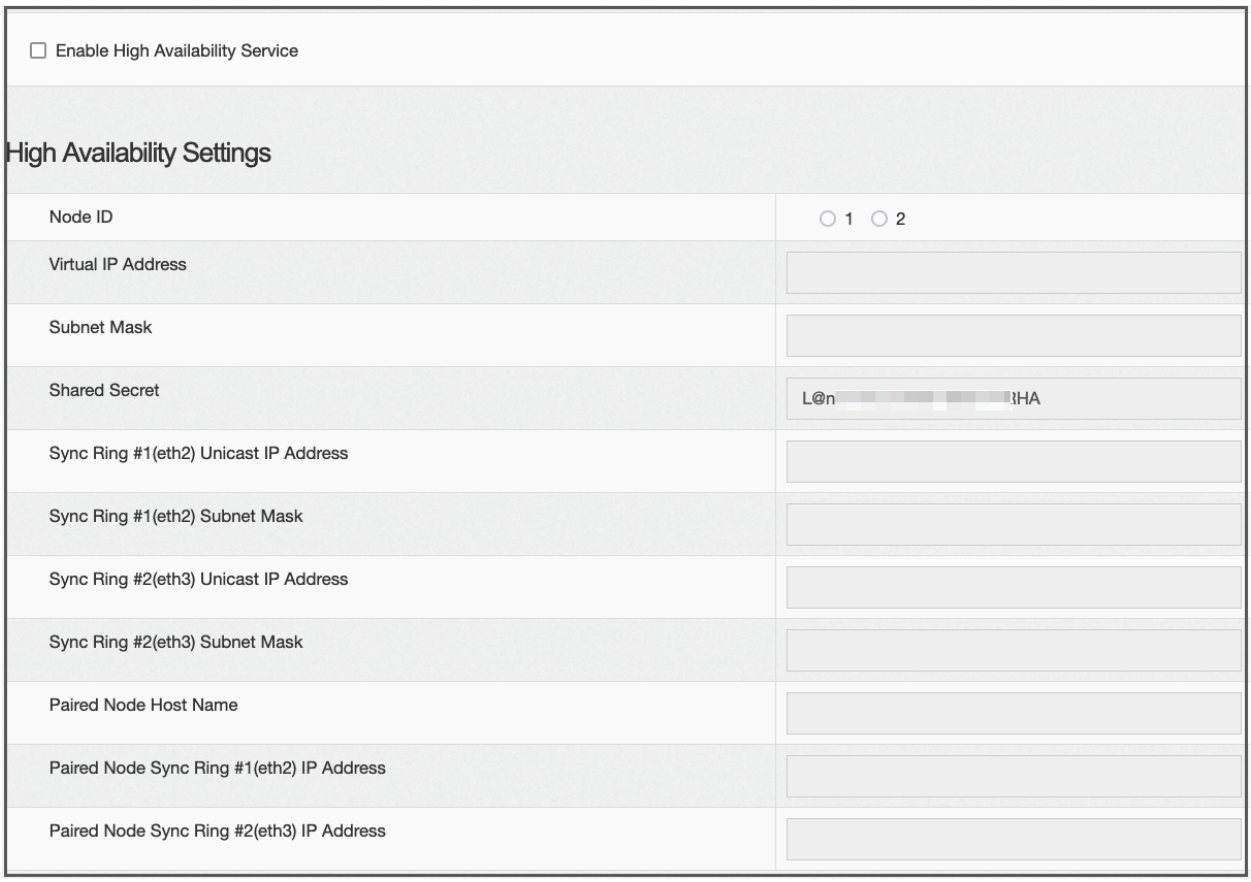
이 쌍에서 온라인 노드는 기본 노드이며 오프라인 노드는 보조 노드입니다. 이 쌍의 기본 노드에 오류가 발생하면 보조 노드가 이를 대체하여 기본 노드가 됩니다.

요구 사항

- **전달 규칙:** 고가용성 시스템에서 UDP Director에 대해 하나 이상의 전달 규칙을 구성합니다.
- **규칙 설정 파일 저장:** UDP Director에 이미 설정된 규칙이 있는 경우 UDP Director 규칙을 내보내기(규칙 설정 파일 저장)합니다. 그런 다음 이 파일을 두 번째 UDP Director로 가져와 각 일치 항목에 대한 규칙을 확인합니다.
- **순서:**먼저 기본 UDP Director를 구성한 다음 보조에서 구성 단계를 반복해야 합니다.
- **신규 또는 기존:** 두 UDP Director를 모두 새로 만든 경우, 이 가이드의 절차를 각각 따르십시오. 그러나, 보조 UDP Director가 Secure Network Analytics 시스템에서 어플라이언스로 이미 구성된 경우, 보조에 로그인하여 이 가이드에 설명된 대로 고가용성 구성 요소를 구성해야 합니다.

1. 기본 UDP Director고가용성 구성

1. 기본 UDP Director에 로그인합니다.
2. **설정** > **고가용성**을 클릭합니다.
3. 고가용성 설정을 위해 **고가용성 활성화** 체크 박스를 선택합니다.



4. **노드 ID**를 선택합니다. 기본 UDP Director인 경우 1을 선택합니다. 보조 UDP Director인 경우 2를 선택합니다.
5. **Virtual IP Address(가상 IP 주소)** 필드에 eth0 인터페이스와 동일한 서브넷에 있는 미사용 IP 주소를 입력합니다. **Subnet Mask(서브넷 마스크)** 값을 eth0 인터페이스에 사용되는 서브넷 마스크 값으로 설정합니다.

> 가상 IP 주소는 두 노드에서 동일해야 합니다.

6. **Shared Secret(공유 암호)** 필드에 두 UDP Director에 대한 문자열을 입력합니다. (보안 전송을 위해 암호화됩니다.)
7. **Sync Ring #1 (eth2) Unicast IP Address(동기화 링 #1(eth2) 유니캐스트 IP 주소)** 필드에 IP 주소와 서브넷 마스크를 입력합니다. (유니캐스트 IP 주소는 단일 네트워크 대상을 식별합니다.)
8. **Sync Ring #2 (eth3) Unicast IP Address(동기화 링 #2(eth3) 유니캐스트 IP 주소)** 필드에 IP 주소와 서브넷 마스크를 입력합니다.

   각 IP 주소(eth0, eth02, eth03)는 고유한 개별 유니캐스트 서브넷에 있어야 합니다.

9. **Paired Node Host Name(페어링된 노드 호스트 이름)** 필드에 보조 UDP Director의 호스트 이름을 입력합니다.
10. **Paired Node Sync Ring #1(eth2) IP Address(페어링된 노드 동기화 링 #1(eth2) IP 주소** 필드에 보조 UDP Director의 Eth2 IP 주소를 입력합니다.
11. **Paired Node Sync Ring #1(eth3) IP Address(페어링된 노드 동기화 링 #1(eth3) IP 주소** 필드에 보조 UDP Director의 Eth3 IP 주소를 입력합니다.
12. 설정을 검토한 후 **Apply(적용)**을 클릭하여 구성을 설정합니다.
13. 클러스터의 두 번째 UDP Director를 구성하려면 다음 섹션을 계속 진행합니다.

2. 고가용성
을 위한 보조 UDP Director구성

> 위의 4단계에서 노드 ID 2를 선택한 경우 기본 UDP Director에 대해 아래 단계를 완료합니다.

보조 UDP Director를 구성하려면 다음 단계를 완료합니다.

1. 보조 UDP Director에 로그인합니다.
2. **설정** > **고가용성**을 클릭합니다.
3. **페어링된 노드 호스트 이름** 필드에 보조 UDP Director의 호스트 이름을 입력합니다.
4. 이 화면의 모든 파라미터(첫 번째 어플라이언스에서 변경한 모든 고급 파라미터 포함)를 다음을 제외한 모든 필드에 대해 첫 번째 어플라이언스와 똑같이 구성합니다.
   - **Sync Ring 1(eth2) 유니캐스트 IP 주소**: 기본 UDP Director의 이 필드에 구성한 것과는 다른 IP 주소를 입력합니다. 단, 이는 Sync Ring 1 유니캐스트 주소와 동일한 서브넷에 있어야 합니다.
   - **Sync Ring 2(eth3) 유니캐스트 IP 주소**: 기본 UDP Director의 이 필드에 구성한 것과는 다른 IP 주소를 입력합니다. 단, 이는 Sync Ring 2 유니캐스트 주소와 동일한 서브넷에 있어야 합니다.
   - **페어링된 노드 호스트 이름**: 이 필드에 기본 UDP Director의 호스트 이름을 입력합니다.
   - **페어링된 노드 Sync Ring #1(eth2) IP 주소**: 이 필드에 기본 UDP Director의 Eth2 IP 주소를 입력합니다.
   - **페어링된 노드 Sync Ring #1(eth3) IP 주소**: 이 필드에 기본 UDP Director의 Eth3 IP 주소를 입력합니다.
5. 변경 사항을 저장하고 이 어플라이언스에서 클러스터링 서비스를 시작하려면 **적용**을 클릭합니다.
6. 기본 어플라이언스를 지정하려면 **승격** 버튼을 클릭합니다.

플로우 센서

1을 구성. 애플리케이션 ID와 페이로드 구성

플로우 센서 구성에는 애플리케이션 ID와 페이로드를 구성하는 추가 단계가 필요합니다.

1. 플로우 센서어플라이언스 관리 인터페이스에 로그인합니다.
2. **설정** > **고급 설정**을 클릭합니다.

고급 설정 페이지가 열립니다.

3. 적절한 네트워크 설정을 선택합니다.

항목	설명
패킷 페이로드 내보내기	플로우 센서에서 컬렉터로 전송하는 데이터에 첫 26바이트의 바이너리 페이로드 데이터를 포함할지를 지정할 수 있습니다.
애플리케이션 ID 내보내기	플로우 센서에서 컬렉터로 데이터를 전송하기 전에 애플리케이션을 식별할지를 지정할 수 있습니다. 또한, 이 설정은 다음 설정을 적용하기 위해 활성화되어야 합니다. IPv6 포함 - 플로우 센서에서 IPv4 및 IPv6 패킷을 분석할지를 지정할 수 있습니다. 이 설정을 비활성화하면 플로우 센서에서는 IPv4 패킷만 분석합니다. HTTPS 헤더 데이터 내보내기 - 플로우 센서에서 컬렉터로 전송하는 데이터에 HTTPS 플로우의 헤더 데이터를 포함할지를 지정할 수 있습니다. 이 데이터는 SSL 일반 이름 및 SSL 조직 이름을 포함합니다. 이 설정에서는 플로우 유형을 IPFIX로 설정해야 합니다. 최대값은 256바이트입니다. HTTP 헤더 데이터 내보내기 - 플로우 센서에서 컬렉터로 전송하는 데이터에 HTTP 플로우의 헤더 데이터를 포함할지를 지정할 수 있습니다. 이 설정을 선택하면 보조 필드를 통해 플로우 센서에서 플로우 데이터의 일부로 포함하는 HTTP 경로(바이트 단위)의 최대 길이를 지정할 수 있습니다. 이 설정에서는 플로우 유형을 IPFIX로 설정해야 합니다.
VXLAN 역캡슐화 활성화	플로우 센서가 VXLAN(Virtual Extensible Local Area Network) 역캡슐화 기능을 사용할지 여부를 지정할 수 있습니다. VXLAN 역캡슐화를 사용하지 않으면 플로우 센서는 단순히 가상 터널 엔드포인트(VTEP) 간 플로우로서 VXLAN 캡슐화된 트래픽을 탐지합니다. 캡슐화는 터널링된 트래픽을 분석하고 네트워크 트래픽 패턴에 대한 통찰력을 얻을 수 있어 훨씬 더 풍부한 콘텐츠를 제공할 수 있습니다.

항목	설명
	플로우 센서는 원래 표준 VXLAN 포트(4789)로 전송된 VXLAN 트래픽만 역캡슐화합니다.
GENEVE 역캡슐화 활성화	모니터링 포트에서 수신한 트래픽에 대해 플로우 센서이 GENEVE(일반 네트워크 가상화 캡슐화) 역캡슐화를 사용할지 여부를 지정할 수 있습니다.
ERSPAN 역캡슐화 활성화	플로우 센서이 ERSPAN(캡슐화된 원격 스위칭 포트 분석기) 역캡슐화 기능을 사용하여 패킷에서 ERSPAN 헤더를 감지한 다음 헤더를 역캡슐화하고 내부 패킷 내용을 처리할지 여부를 지정할 수 있습니다. 플로우 센서에서 ERSPAN 터널의 종료를 허용하려면 모니터링 인터페이스에 IP 주소를 할당해야 합니다. ERSPAN 역캡슐화는 FS 4210에서 지원되지 않습니다.
착신 전환 처리 활성화	플로우 센서가 착신 전환(XFF) 처리를 사용해 HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소를 식별할지 여부를 지정할 수 있습니다. ETA 및 착신 전환 처리는 함께 구성할 수 없습니다.
ETA 처리 활성화	플로우 센서가 IDP 및 SPLT 필드를 생성해 매니저에 전송하는 데 ETA 처리를 사용할지 여부를 지정할 수 있습니다. ETA를 활성화하면 특히 v9 사용 시 NetFlow 대역폭 사용량이 증가합니다. Flow Export 형식에는 IPFIX를 사용하는 것이 좋습니다. ETA 및 착신 전환 처리는 함께 구성할 수 없습니다. Dell 또는 PowerEdge 플로우 센서 모델에서는 ETA를 활성화할 수 없습니다.
로드 밸런싱 활성화	플로우 센서 4000 Series에서 둘 이상의 플로우 컬렉터에 플로우 데이터를 배포할 수 있는지 여부를 지정할 수 있습니다. 플로우 센서의 플로우 데이터가 한 플로우 컬렉터의 용량을 초과하는 경우 이 옵션을 사용합니다.

항목	설명
모니터링 인터페이스 선택	다음을 지정할 수 있습니다. • 플로우 센서 4240 - 2 x 40G 또는 4 x 10G(SFP) 인터페이스 • 플로우 센서 4300 - 2 x 40G/100G 또는 4 x 10G(SFP) 인터페이스 이 설정이 제대로 작동하려면 여러 개의 플로우 컬렉터를 사용해야 하며 로드 밸런싱이 활성화되어 있어야 합니다. 자세한 내용은 및 플로우 센서로드 밸런서 통합 가이드를 참조하십시오. 이 옵션은 플로우 센서 4240 및 플로우 센서 4300에서만 사용할 수 있습니다. 기본 설정은 2 x 40G입니다.
캐시 모드	다음 설정 중 하나를 선택할 수 있습니다. 모든 모니터링 포트에 단일 공유 캐시 사용 - • 비대칭 라우팅이 있는 경우에 사용합니다. • 애플리케이션 및 레이턴시 계산을 위한 단일 상태 테이블입니다. • 적은 메모리를 사용합니다. • 전반적인 pps 처리 속도가 낮습니다. • 여러 인터페이스 전반에서 생성된 하나의 NetFlow 이벤트가 발생합니다. • 플로우 센서에 두 개의 포트만 있고 TAP에 의해 연결되는 경우에만 사용합니다. 각 모니터링 포트에 독립적 캐시 사용 - • 각 플로우 센서 인터페이스 전반에서 패킷 중복 제거를 허용합니다. • 많은 메모리를 사용합니다. • 전반적인 pps 처리 속도가 높습니다. • 각 인터페이스는 고유한 레이턴시 및 애플리케이션 데이터베이스를 유지 관리합니다. • 각 인터페이스에 대해 지정된 패킷을 보여주는 고유한 NetFlow 레코드가 생성됩니다.

4. **적용**을 클릭하여 설정을 저장합니다.

2. 애플리케이션 식별을 위한 플로우 센서 설정(선택 사항)

플로우 센서가 애플리케이션을 식별하도록 하려면 다음 설정을 구성합니다.

1. 플로우 센서 어플라이언스 관리 인터페이스에 로그인합니다.
2. **설정** > **고급 설정**을 클릭합니다.
3. **애플리케이션 ID 내보내기** 체크 박스를 선택합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.
4. 모니터링 NIC가 1개 이상인 경우 **캐시 모드** 섹션에서 다음 옵션 중 하나를 선택합니다.
   - **모든 모니터링 포트에 대해 단일 공유 캐시 사용:** 일반적으로 TAP 방법을 사용하여 플로우를 모니터링하는 시스템에 사용됩니다.
   - **각 모니터링 포트에 독립적 캐시 사용:** 일반적으로 우수한 성능을 경험하기 위해 사용되며 방법을 사용하여 플로우를 모니터링하는 시스템에 사용됩니다.

3. 어플라이언스 재시작

1. **작업** > **어플라이언스 재시작**을 선택합니다.
2. Central Management에서 어플라이언스 상태가 Connected(연결됨)인지 확인합니다.

10. 텔레메트리 구성

데이터 저장소와 함께 Secure Network Analytics를 구축한 경우 플로우 컬렉터는 여러 유형의 텔레메트리를 동시에 수집할 수 있습니다. 최초 설정 중에 플로우 컬렉터를 구성하거나 기존 플로우 컬렉터인 경우 플로우 컬렉터 고급 설정을 사용하여 텔레메트리 수집 설정을 업데이트할 수 있습니다.

> 텔레메트리 포트가 고유한지 확인합니다. 텔레메트리 포트를 중복으로 구성하면 플로우 데이터 손실을 방지하기 위해 포트가 내부 기본값으로 재설정됩니다. 예를 들어, NetFlow와 NVM을 동일한 텔레메트리 포트로 내보내는 경우, NVM 데이터를 내보내는 각 디바이스는 플로우 컬렉터에 내보내기를 생성하고 플로우 컬렉터 엔진의 내보내기 리소스를 소진하여 플로우 데이터가 손실됩니다.

Network Visibility Module

NVM(Network Visibility Module 을 선택하고 구성한 경우 플로우 컬렉터는 NVM 플로우를 수집하고 저장합니다. Cisco Secure Network 애널리틱스 엔드포인트 라이선스 및 NVM(Network Visibility Module) 구성 가이드의 지침에 따라 구성 요구 사항을 완료하십시오.

방화벽 로그

Firewall Logs(방화벽 로그)를 선택하고 구성한 경우 플로우 컬렉터는 Cisco Security Analytics and Logging(온프레미스)에 대한 방화벽 이벤트 로그를 수집하고 저장합니다. 보안 분석 및 로깅: 방화벽 이벤트 통합 가이드의 지침에 따라 구성 요구 사항을 완료합니다.

앱 요구 사항: 방화벽 로그를 선택하고 구성하는 경우 매니저에 Security Analytics and Logging (온프레미스) 앱을 설치합니다.

텔레메트리 설정 업데이트

NetFlow 또는 다른 텔레메트리를 수집하는 기존 플로우 컬렉터가 있는 경우 플로우 컬렉터 고급 설정을 사용하여 텔레메트리 수집 설정을 업데이트할 수 있습니다. 고급 설정에 액세스하려면 다음과 같이 합니다.

1. 플로우 컬렉터(이전의 어플라이언스 관리(Admin) 인터페이스)에 로그인합니다.
2. **Support(지원) > Advanced Settings(고급 설정)**을 선택합니다.

> 각 텔레메트리 유형에는 두 가지 설정이 있습니다. Advanced Settings(고급 설정)를 사용하여 텔레메트리를 구성하는 방법에 대한 자세한 내용을 보려면 도움말의 지침을 따르십시오. ? **(도움말) 아이콘 > Help(도움말)**를 선택합니다.

Cisco Telemetry Broker

UDP Director를 사용하여 NetFlow를 플로우 컬렉터에 전송하는 대신, 이제 Cisco Telemetry Broker를 사용하여 여러 입력에서 네트워크 텔레메트리를 수집하고 텔레메트리 형식을 변환하고 해당 텔레메트리를 하나 또는 여러 대상에 전달할 수 있습니다. Cisco Telemetry Broker를

설치하려면 Cisco Telemetry Broker 가상 어플라이언스 구축 및 구성 가이드의 지침을 따르십시오.

11. 라이선싱 Secure Network Analytics

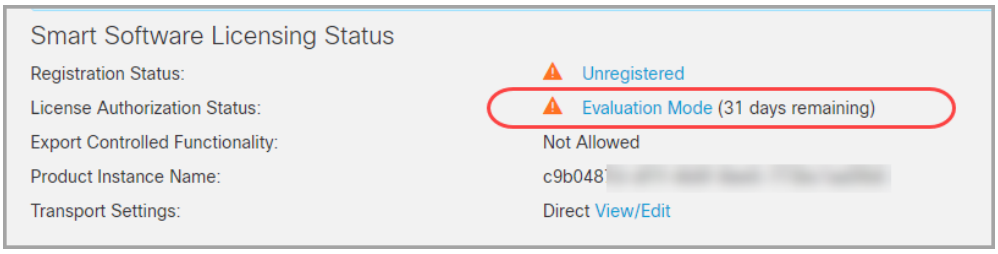
Cisco Smart 소프트웨어 라이선싱을 사용하여 Secure Network Analytics어플라이언스 및 기능에 라이선스를 부여합니다. 자세한 내용은 cisco.com에서 Smart 라이선싱을 참조하십시오.

- **온라인:** Smart 라이선싱 및 Secure Network Analytics를 온라인으로 사용하려면 Secure Network AnalyticsSmart 소프트웨어 라이선싱 가이드를 참조하십시오. 이 구성을 사용하려면 인터넷 액세스가 필요합니다.
- **오프라인:** 폐쇄형/에어갭 네트워크에 대한 라이선싱 옵션을 논의하려면 Cisco 지원팀에 문의하십시오.
- **Cisco Smart 어카운트:** Cisco Smart 어카운트를 설정하려면 https://software.cisco.com에서 등록하거나 관리자에게 문의하십시오.

평가 모드

Secure Network Analytics 평가 모드를 사용할 경우 선택한 기능을 90일간 사용할 수 있습니다. Secure Network Analytics의 최대 기본 기능을 사용하고 계정에 라이선스 및 기능을 추가하려면 제품 인스턴스를 Smart Software 라이선싱에 등록하십시오.

> 90일 평가 기간이 만료되기 전 제품 인스턴스를 등록했는지 확인하십시오. 평가 기간이 만료되면 플로우 수집이 중지됩니다. 플로우 수집을 다시 시작하려면 제품 인스턴스를 등록하십시오.



- **Admin 사용자:** 매니저에서 스마트 라이선싱 상태 및 사용량 세부 정보를 검토하려면 admin 사용자로 로그인합니다.
- **남은 일수:** 평가 모드의 남은 일수를 검토하려면 매니저에 admin 사용자로 로그인합니다. **Central Management(중앙 관리)** > **Smart Licensing(스마트 라이선싱)**으로 이동합니다. **라이선스 인증 상태**를 검토합니다.
- **제품 인스턴스:** 제품 인스턴스 이름은 매니저 및 매니지드 어플라이언스를 포함하는 Secure Network Analytics 제품 인스턴스의 식별자입니다.

12. 관리 Secure Network Analytics

어플라이언스 구성을 완료하면 도움말은 환경을 관리하고 행동을 조사하고 위협에 대응하는 방법 등에 대한 지침을 제공합니다.

> 지침을 검토하려면 아무 페이지에서 (**도움말**) 아이콘 > **도움말**을 클릭합니다.

호스트 그룹 구성

1. 매니저다음에 로그인합니다.
2. **구성** > **호스트 그룹 관리 탐지**를 선택합니다.

정책 생성 및 관리

1. 매니저다음에 로그인합니다.
2. **구성** > **정책 관리 탐지**를 선택합니다.

플로우 검색 구축

1. 매니저다음에 로그인합니다.
2. **Investigate(조사)** > **Flow Search(플로우 검색)**을 선택합니다.

보고서 작성기에서 보고서 실행

1. 매니저다음에 로그인합니다.
2. **Report(보고서)** > **Report Builder(보고서 작성기)**를 선택합니다.

사용자 권한 관리

1. 매니저다음에 로그인합니다.
2. **Configure(구성)** > **GLOBAL User Management(전역 사용자 관리)**를 선택합니다.

동작 조사(알람, 보안 이벤트 등)

알람, 이벤트, 호스트 등을 조사하는 방법에 대한 자세한 내용은 도움말의 정보를 참조하십시오.

1. 매니저다음에 로그인합니다.
2. (**도움말**) 아이콘를 클릭합니다.
3. **Help(도움말)**를 선택합니다.
4. 페이지 상단에서 **Help(도움말)** 메뉴를 선택합니다.
5. **조사 동작**을 선택합니다.

위협에 대응

정책 정보를 보려면 도움말의 정보를 검토합니다.

1. 매니저다음에 로그인합니다.
2. (**도움말**) 아이콘를 클릭합니다.
3. **Help(도움말)**를 선택합니다.
4. 페이지 상단에서 **Help(도움말)** 메뉴를 선택합니다.
5. **위협에 대응**을 선택합니다.

분석

Secure Network Analytics 동적 엔티티 모델링을 사용하여 네트워크의 상태를 추적합니다. Secure Network Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. 자세한 내용은 분석: 탐지, 알림 및 관찰 가이드를 참조하십시오.

어플라이언스를 설치하려면 Virtual Edition 어플라이언스 설치 가이드, x2xx Series 하드웨어 어플라이언스 설치 가이드 또는 x3xx Series 하드웨어 어플라이언스 설치 가이드의 지침을 따르십시오.

애플리케이션

Secure Network Analytics 앱은 의 Secure Network Analytics 기능을 향상 및 확장하는 독립적으로 릴리스할 수 있는 선택적 기능입니다.

Secure Network Analytics 앱의 릴리스 일정은 일반 Secure Network Analytics 업그레이드 프로세스와 별개입니다. 따라서 코어 Secure Network Analytics 릴리스에 연결하지 않고도 필요에 따라 Secure Network Analytics 앱을 업데이트할 수 있습니다. Secure Network Analytics의 새로운 릴리스에 대응하도록 설계된 앱을 즉시 설치하지 못할 수도 있습니다. 최신 버전의 앱은 몇 주 동안 기다려야 할 수 있습니다.

최신 Secure Network Analytics 앱 정보, 가용성 및 호환성에 대해서는 다음을 참조하십시오.

- Secure Network Analytics 앱 버전 호환성 매트릭스
- Secure Network Analytics 앱 릴리스 노트

인증/권한 부여

Secure Network Analytics를 사용한 각 인증 또는 권한 부여 설정에 대한 자세한 내용은 다음 지침을 참조하십시오.

이름	지침
LDAP	도움말의 지침을 따르십시오. 1. 매니저다음에 로그인합니다. 2. **Configure(구성) > GLOBAL User Management(전역 사용자 관리)**를 선택합니다. 3. **Authentication and Authorization(인증 및 권한 부여)** 탭을 클릭합니다. 4. (**도움말**) 아이콘 > **도움말**을 선택합니다.
SAML SSO(Security Assertion Markup Language Single Sign-On)	이 가이드의 **SAML SSO 구성** 섹션을 참조하십시오.
TACACS + 설정 가이드	TACACS+ 구성 가이드.

SAML SSO 구성

다음 지침에 따라 SAML SSO(보안 어설션 마크업 언어 Single Sign-On)을 구성합니다. SSO는 사용자가 하나의 자격 증명 세트를 사용해 여러 애플리케이션에 액세스할 수 있도록 하는 인증 프로세스입니다.

지원 상세정보

다음 설정이 지원되거나 지원되지 않습니다.

지원	지원되지 않음
Microsoft ADFS(Active Directory Federation Services) 2.0	Microsoft ADFS의 클라우드 서비스
Microsoft ADFS의 온프레미스 솔루션	IWA(윈도우 통합 인증)
추가 프록시	외부 서비스
	SAML 요청 서명

> 데스크톱 클라이언트는 데이터스토어 구축에서 지원되지 않습니다.

1. 설정 준비

SSO를 구성하려면 다음 정보가 필요합니다.

요건	세부 정보
ID 공급자 URL	URL은 정규화된 도메인 이름 또는 IPv4 주소를 사용해야 합니다.
ID 공급자 인증서	IDP URL이 HTTPS로 시작되면 CA 인증서를 다운로드합니다.

2. Trust Store에 인증서 업로드

IDP(Identity Service Provider) URL이 HTTPS로 시작되는 경우, **루트 CA 인증서**를 매니저 신뢰 저장소에 추가합니다.

> IDP URL이 HTTPS로 시작되지 않는 경우 이 단계를 건너뛰고 다음 섹션인 **3. 서비스 제공자 설정**

다음 지침을 사용하여 매니저 신뢰 저장소에 루트 CA 인증서를 추가합니다.

1. Central Management 인벤토리 페이지에서 매니저에 대한 **Actions(작업)** 메뉴를 클릭합니다.
2. **어플라이언스 설정 편집**을 선택합니다.
3. **어플라이언스 관리자** > **일반** 탭에서 Trust Store 섹션을 찾습니다.
4. **새로 추가**를 클릭합니다.
5. **식별 이름** 필드에 인증서의 이름을 입력합니다.
6. **Choose File(파일 선택)**을 클릭합니다. 새 인증서를 선택합니다.
7. **인증서 추가**를 클릭합니다. Trust Store 목록에 새 인증서가 표시되는지 확인합니다.
8. **설정 적용**을 클릭합니다. 화면의 프롬프트를 따르십시오.
9. **Connected(연결됨):** 인벤토리 페이지에서 매니저이 구성 변경을 완료하고 어플라이언스 상태가 **Connected(연결됨)**으로 돌아오는지 확인합니다.

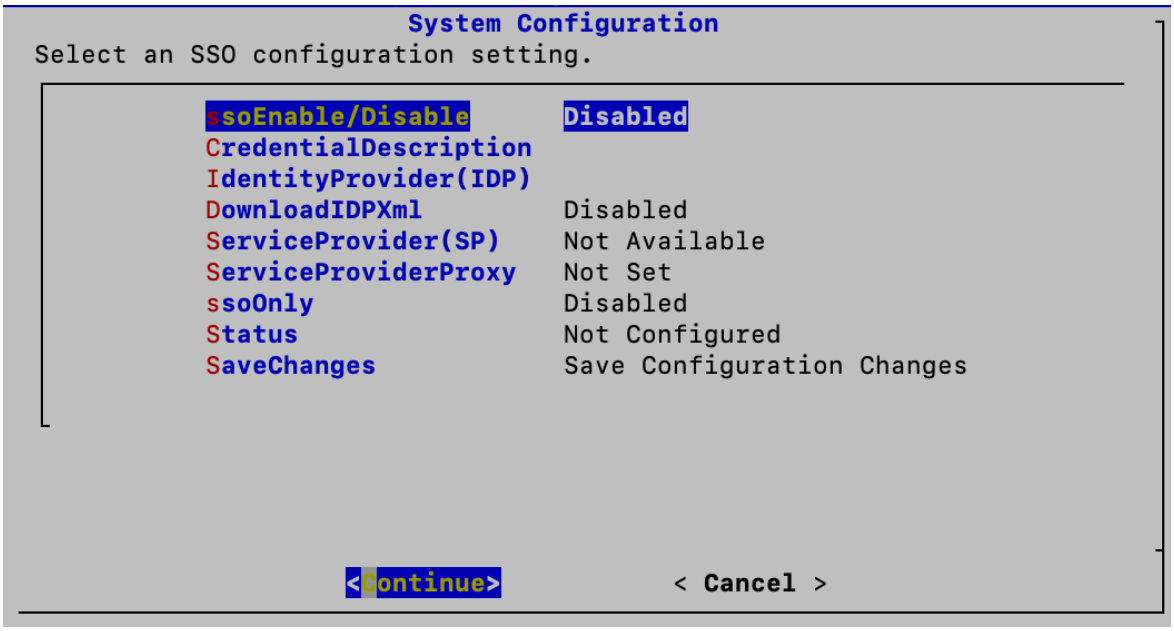
> 설정 변경 사항이 보류 중인 경우 어플라이언스가 강제로 재부팅되지 않도록 합니다.

10. 보조 매니저가 있는 경우 이 절차를 반복하여 보조 매니저 신뢰 저장소에 루트 CA 인증서를 추가합니다.
11. 매니저 신뢰 저장소에 루트 CA 인증서를 추가한 경우 다음 섹션으로 이동합니다.

> LDP에서 메타데이터를 업데이트하는 경우 SSO가 연결되지 않을 수 있습니다. 메타데이터를 업데이트해야 합니다. 이 작업을 수행하는 가장 쉬운 방법은 시스템 구성 도구에서 새 SSO 정보를 업데이트한 후 리부팅하는 것입니다.

3. 서비스 제공자 설정

1. 먼저 매니저 콘솔에 root로 로그인합니다.
2. `SystemConfig`를 입력합니다. Enter를 누릅니다.
3. **고급**을 선택합니다.
4. **SSO**를 선택합니다.
5. **SSO 활성화/비활성화**가 **비활성화** 상태로 표시되어 있는지 확인합니다.



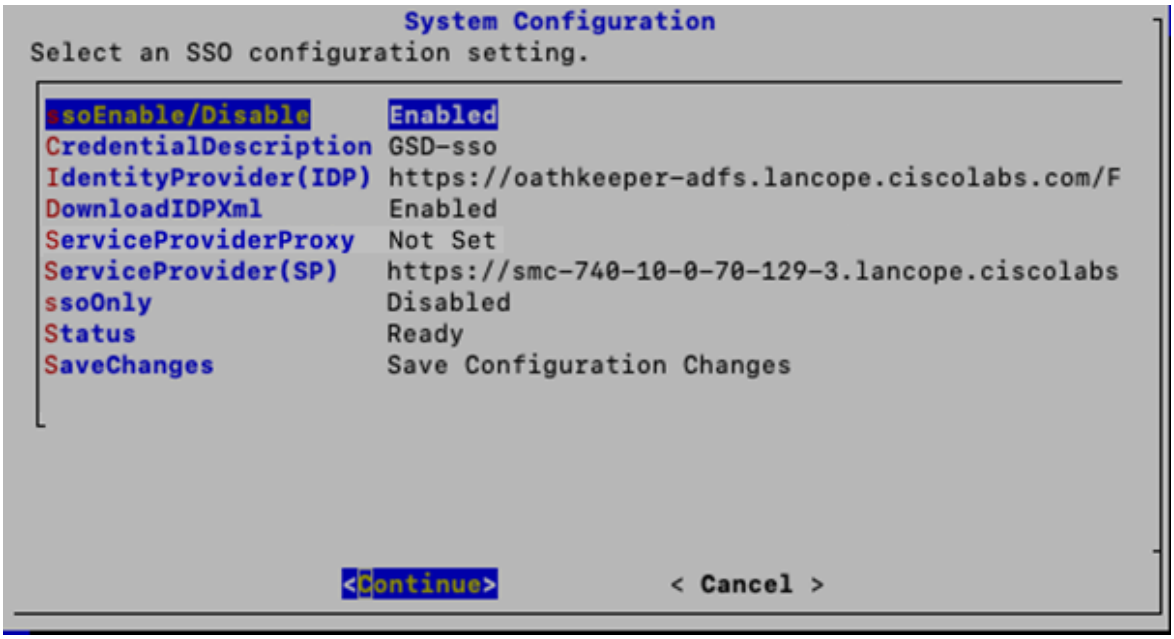
6. **IDP(IdentityProvider)**를 선택합니다. **Continue(계속)**를 클릭합니다.
7. IDP의 설정 파일을 다운로드할 수 있는 URL을 입력합니다.

   요구 사항: FQDN(정규화된 도메인 이름) 또는 IPv4 주소를 입력합니다.

8. **DownloadIDP**를 선택합니다. 화면에 표시되는 프롬프트에 따라 활성화합니다.
9. **SaveChanges**를 선택합니다. **Continue(계속)**를 클릭합니다.

   화면에 표시되는 프롬프트에 따라 IDP 설정 파일을 다운로드합니다.

10. **SSO**를 선택합니다.
11. **서비스 공급자(SP)**를 검토합니다. URL을 복사합니다. 이를 사용하여 IDP를 구성합니다.
12. **상태**를 검토합니다. **준비**로 표시되는지 확인합니다.



4. SSO 활성화

1. **sso활성화/비활성화**를 선택합니다.
2. 화면에 표시되는 프롬프트에 따라 SSO를 활성화합니다.
3. **CredentialDescription**을 선택합니다. **Continue(계속)**를 클릭합니다.
4. 사용자가 로그인해야 하는 SSO 서비스 자격 증명에 대한 설명을 입력합니다.
5. **OK(확인)**를 클릭합니다.
6. **DownloadIDP**를 선택합니다. 새 SSO 설정을 저장해야 할 때까지 DownloadIDP를 비활성화합니다.

   - **Continue(계속)**를 클릭합니다.
   - 화면에 표시되는 프롬프트에 따라 DownloadIDP를 비활성화합니다.

7. **SaveChanges**를 선택합니다. **Continue(계속)**를 클릭합니다.
8. 시스템 설정을 종료합니다.

5. 통신 사업자 프록시 구성(선택 사항)

1. **SSO 활성화/비활성화**가 **활성화** 상태로 표시되어 있는지 확인합니다.
2. **ServiceProviderProxy(서비스 제공자 프록시)**를 선택합니다.
3. 사용할 서비스 제공자 프록시의 FQDN(Fully Qualified Domain Name)을 입력합니다.
4. **OK(확인)**를 클릭합니다.
5. 프록시 구성 프로세스를 완료하려면 매니저를 재부팅하십시오.

6. ID 공급자 설정

1. 브라우저의 주소 필드에 서비스 제공자 URL을 입력합니다.
2. 서비스 공급자 메타데이터 파일 **sp.xml**을 다운로드합니다.
3. **sp.xml**로 ID 공급자를 설정합니다.
4. 발신 클레임 유형에 사용자 이메일 주소가 포함되어 있는지 확인합니다.

   - **예를 들어,** 속성 저장소가 Active Directory인 경우, 발신 클레임 유형을 LDAP 속성 유형 사용자 ID의 이메일 주소로 설정합니다.
   - **Microsoft ADFS(Active Directory Federation Services):** IDP 유형이 ADFS인 경우 다음 맞춤형 규칙을 확인합니다.

```
 c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue
(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

7. SSO 사용자 추가

SSO 사용자를 추가하려면 다음 지침을 따르십시오. 사용자는 IDP를 통해/로 인증됩니다.

1. 매니저(웹 앱)다음에 로그인합니다.
2. **Configure(구성) > GLOBAL User Management(전역 사용자 관리)**를 선택합니다.
3. **만들기** > **사용자**를 선택합니다.

   지침을 보려면 (**도움말**) 아이콘를 클릭합니다. **Help(도움말)**를 선택합니다. 사용자를 추가하는 방법에 대한 자세한 내용은 "사용자 구성"을 참조하십시오.

4. 필드를 입력하여 새 사용자를 생성합니다. 다음과 같이 사용자를 구성합니다.
   - **인증 서비스:** SSO를 선택합니다.
   - **사용자 이름:** IDP 계정용 이메일 주소의 첫 번째 부분을 입력합니다. ID가 로그인 시 SSO에 사용되는 것과 동일한지 확인합니다. 예를 들어 name@cisco.com의 경우 이 필드에는 "name"을 입력합니다.
5. **Save(저장)**를 클릭합니다.
6. SSO 사용자가 사용자 관리에 표시되는지 확인합니다.

8. SAML 로그인 테스트

1. 웹 UI 로그인 페이지에서 **SSO로 로그인**를 선택합니다.
2. 인증서 버튼을 클릭합니다.
3. 로그인 자격 증명을 입력합니다. 매니저가 Security Insight 대시보드로 열립니다.

문제 해결

시나리오	참고
계정 잠금	긴급 어카운트 액세스를 통해 시스템 설정에서만 SSO를 비활성화합니다.
IDP XML 다운로드 불가	IDP 인증서가 매니저 신뢰 저장소에 업로드되었는지 확인합니다.
IDP 설정 저장 불가	IDP 설정을 검토하고 입력한 데이터가 정확하며 공백이 포함되지 않았는지 확인합니다. 또한 IDP 이벤트 로그를 검토합니다.
추가 문제	브라우저의 SAML 트레이서를 다운로드합니다. SSO 로그인을 반복하여 IDP와 SP 간의 교류를 검토합니다.

도메인

도메인은 모니터링 및 관리하려는 호스트 및 기타 디바이스의 그룹입니다. 플로우 컬렉터은 도메인 내에 존재하며, 하나의 Secure Network Analytics 시스템 내에 여러 도메인을 보유할 수 있습니다. 도메인은 다른 도메인과 완전히 독립적이며 모든 도메인은 호스트 그룹 트리를 포함합니다. 호스트 그룹 트리에 있는 호스트 그룹에 대한 자세한 내용은 도움말의 호스트 그룹 관리 및 구성을 참조하십시오.

이 섹션에서는 다음 주제를 다룹니다.

- **데이터 저장소 도메인 및 비데이터 저장소 도메인**
- **도메인 추가 및 구성**
- **동기화 데이터스토어 및 비데이터스토어 도메인**
- **도메인 삭제**

데이터 저장소 도메인 및 비데이터 저장소 도메인

어플라이언스 설정 도구에서 매니저를 구성하고 시스템을 설정할 때는 데이터 저장소가 있는 Secure Network Analytics 도메인(데이터 저장소 도메인) 또는 데이터스토어가 없는 도메인(비데이터 저장소 도메인)을 생성합니다.

- **데이터 저장소 도메인:** 플로우 컬렉터는 스토리지용 데이터 저장소 데이터 노드로 텔레메트리를 보냅니다.
- **비데이터 저장소 도메인:** 플로우 컬렉터은 텔레메트리를 플로우 컬렉터 또는 플로우 컬렉터 데이터베이스에 로컬로 저장합니다(5000 Series만 해당).
- **하이브리드 구성:** 하이브리드 구성을 사용한 Secure Network Analytics에 데이터 저장소 도메인 및 비데이터 저장소 도메인을 구성할 수 있습니다. 플로우 컬렉터를 구성할 때 플로우 컬렉터가 데이터를 전송할 도메인을 선택할 수 있습니다.

> 비데이터 저장소 구축에 데이터스토어 도메인을 추가하는 경우, **비데이터 저장소 구축에 데이터 저장소 추가**의 지침을 검토하십시오.

도메인 추가 및 구성

다음 지침에 따라 도메인을 추가하고 도메인 설정을 정의합니다. 또한 비데이터스토어 구성을 새 데이터스토어 도메인으로 가져올 수 있습니다.

- **역할 권한:** 도메인을 구성하려면 관리자 또는 설정 관리자 역할이 필요합니다. 전력 분석가는 도메인을 볼 수만 있습니다.
- **데이터 저장소 도메인:** 비데이터 저장소 구축에 데이터스토어 도메인을 추가하는 경우 이 절차를 시작하기 전에 **비데이터 저장소 구축에 데이터 저장소 추가**의 지침을 검토하십시오.

1. 도메인 추가

1. 메뉴 모음에서 **[Current domain name(현재 도메인 이름)] 선택 → Add Domain(도메인 추가)**을 클릭합니다.

2. 다음 필드를 구성합니다.

   - **도메인 이름**: 도메인에 할당할 이름입니다. 이 이름은 호스트 그룹 트리에 표시됩니다.
   - **방법 선택**: 아래 표에 설명된 방법 중 하나를 선택하여 추가하려는 도메인에 사용할 호스트 그룹 구조를 지정합니다.

이 방법을 선택할 경우	수행할 작업
기본	Secure Network Analytics은 기본 호스트 그룹 구조가 있지만 플로우 컬렉터가 없는 도메인을 생성합니다.
파일에서 가져오기	Secure Network Analytics 도메인을 생성하고 사용자가 내보낸 특정 도메인 콘텐츠(호스트 그룹, 도메인 또는 둘 다)를 기준으로 적절한 구성을 사용합니다. 도메인 구성이 포함된 XML 파일을 내보내는 방법에 대한 자세한 내용은 내보내기 설정 섹션을 참조하십시오. • 도메인 설정을 포함하는 XML 파일은 이전 버전과 호환되지 않습니다. 이러한 파일은 동일한 시스템 버전 번호 내에서만 호환됩니다(예: 플로우 컬렉터 v7.0에서 매니저 v7.0으로). • 호스트 그룹 관리 페이지를 사용하여 전체 호스트 그룹 설정을 가져올 수도 있습니다. • 다른 도메인에서 호스트 그룹 트리의 네트워크 디바이스 브랜치에 있는 인터페이스 그룹을 가져와야 하는 경우, 이 옵션을 사용합니다. 먼저 그룹을 XML 파일로 로컬 드라이브에 내보내야 합니다. • XML 파일에 포함된 플로우 컬렉터 중 아무것도 가져오지 않습니다.

> 플로우 컬렉터를 기존 도메인에 추가하면 해당 도메인의 특정 구성(정책, 알람 심각도, 서비스, 엑스포터 SNMP 등)이 이 플로우 컬렉터에 적용됩니다.

3. **Add Domain(도메인 추가)**을 클릭하여 도메인 유형을 선택합니다. 데이터스토어 도메인은 데이터스토어를 사용하는 Secure Network Analytics 시스템용이고, 비데이터 저장소 도메인은 데이터스토어를 사용하지 않는 Secure Network Analytics 시스템용입니다. 자세한 내용은 **데이터 저장소 도메인 및 비데이터 저장소 도메인**을 참조하십시오.

   데이터스토어 도메인을 추가하는 경우 **데이터스토어 도메인으로 구성** 확인란을 선택합니다.

> 데이터스토어 도메인을 두 개 이상 생성한 경우 애널리틱스를 활성화하지 마십시오. 이렇게 하면 애널리틱스의 성능이 최적화되지 않습니다.

4. 구성을 저장하려면 **Add(추가)**를 클릭합니다.

기존의 비데이터스토어 도메인 구성을 가져와 데이터 저장소 도메인 생성(선택 사항)

현재 비데이터스토어 도메인에 있고 향후 데이터스토어로 확장을 위해 Secure Network Analytics 시스템에 데이터스토어 도메인을 추가하려는 경우, 비데이터스토어 구성을 새 데이터스토어 도메인으로 가져오면 됩니다.

기존 도메인을 가져올 때 알람, 호스트 그룹 등의 항목을 다시 구성할 필요가 없습니다. 기존 도메인에서 가져오는 것은 새 도메인을 만드는 것과 비슷하지만 기존 구성을 이용합니다.

도메인을 새로 생성한 경우 Secure Network Analytics 설정을 다시 구성해야 합니다.

아래 단계에 따라 새 데이터스토어 도메인을 추가하고 비데이터스토어 도메인의 모든 설정을 가져옵니다..

1. **도메인 추가** 드롭다운 메뉴를 사용하여 비데이터스토어 도메인을 선택합니다
2. 상단 메뉴에서 **Configure(구성) > SYSTEM Domain Properties(시스템 도메인 속성)**을 선택합니다.
3. **모든 구성 내보내기** 라디오 버튼이 선택되어 있는지 확인합니다. 내보내는 데이터 목록을 확인하려면 아래의 도메인 설정 구성 섹션을 참조하십시오.
4. XML 파일을 다운로드하려면 **내보내기** 버튼을 클릭합니다.
5. 페이지 왼쪽 상단, 메인 메뉴 왼쪽 끝에 있는 **[Current domain name(현재 도메인 이름)] > Add Domain(도메인 추가)**을 클릭합니다.
6. 도메인 이름 필드에 새 **도메인 이름**을 입력합니다.
7. 방법 선택 드롭다운 메뉴를 클릭하고 **파일에서 가져오기** 옵션을 선택합니다.
8. 4단계에서 다운로드한 XML 파일을 선택합니다.
9. **데이터스토어** 도메인으로 구성 확인란을 클릭하여 선택합니다.
10. **Add(추가)** 버튼을 클릭하여 새 도메인을 추가합니다.

2. 도메인 설정 구성

1. 추가하려는 도메인에 대해 다음 설정을 완료합니다.

설정	설명
도메인 이름	현재 속한 도메인의 이름입니다.
아카이브 시간	도메인의 각 플로우 컬렉터이 모든 카운트를 지우는 시간을 설정할 수 있습니다. 0~23 사이의 정수를 입력할 수 있으며 여기서 0은 현지 시간으로 자정입니다. 현지 표준 시간대는 아카이브 시간 필드 오른쪽에 표시됩니다. 정의된 시간이 되면 플로우 컬렉터는 모든 색인 수를 0으로 재설정합니다. 또한 플로우 컬렉터는 이전 24시간 동안 수집한 로그 파일 및 웹 파일을 저장한 다음, 데이터를 수집하는 새로운 하루를 시작합니다.

내부 AS(Autonomous System) 번호	내부 AS 번호 필드 내부를 클릭하고 AS 번호를 입력합니다. 쉼표로 여러 항목을 구분하거나 별도의 줄에 항목을 입력할 때마다 **Enter** 를 누릅니다. 플로우 컬렉터를 포함하는 도메인에만 내부 자동 시스템(AS) 번호를 할당할 수 있습니다. Secure Network Analytics에서 이 번호를 포함하는 트래픽이 발생하는 경우, Cisco는 해당 트래픽을 Autonomous System Traffic(자동 시스템 트래픽) 문서에서 "원본" 트래픽으로 분류합니다. 원본 트래픽은 네트워크를 통과하는 외부 네트워크에서 나오는 트래픽(트랜짓 트래픽)과 달리, 네트워크에서 나가거나 네트워크 내의 트래픽을 나타냅니다. 자동 시스템 트래픽 문서에 대한 내용은 데스크톱 클라이언트 도움말의 "자동 시스템 트래픽" 항목을 참조하십시오.

2. 내보내기 설정 구성

   도메인 속성 대화 상자의 내보내기 페이지에서 특정 도메인 콘텐츠를 내보낼 수 있습니다. 나중에 추가하는 추가 도메인의 템플릿으로 해당 콘텐츠를 사용할 수 있습니다.

   사용 가능한 설정에 대한 정보는 다음 표를 참조하십시오.

이 확인란을 선택하면...	**Secure Network Analytics 데이터 내보내기...**
모든 구성 내보내기*	아래 "도메인 구성 내보내기"에 모든 데이터가 나열되어 있습니다. 또한 플로우 컬렉터와 엑스포터 및 해당 인터페이스 목록도 내보내게 됩니다.
호스트 그룹 구성 내보내기	호스트 그룹 이름 및 IP 주소 범위를 포함한 전체 호스트 그룹 정의 구조이 출력에는 정책이 포함되지 않습니다.
도메인 구성 내보내기	• 도메인 속성 대화 상자의 아카이브 시간 설정입니다. • 모든 서비스 정의. 서비스에 대한 내용은 데스크톱 클라이언트 도움말의 "서비스" 항목을 참조하십시오. • 모든 알람 구성 설정 알람 구성에 대한 자세한 내용은 데스트톱 클라이언트 도움말의 "알람 심각도 정보" 항목을 참조하십시오. • 호스트 그룹 이름 및 IP 주소 범위를 포함한 전체 호스트 그룹 구조 자세한 내용은 Secure Network Analytics 도움말의 "호스트 그룹 관리 및 구성" 항목을 참조하십시오. • 모든 정책. 자세한 내용은 Secure Network Analytics 도움말의 핵심 정책 관리 항목을 참조하십시오. 완화 알람 작업은 기본값에서 수동으로 변경한 경우에만 내보내집니다 (*승계되지 않음으로 설정*).
* 이러한 명령의 결과 XML 파일을 사용하여 호스트 그룹 구성을 교체할 수 있습니다. 자세한 내용은 데스크톱 클라이언트 도움말에서 "호스트 그룹 구성을 교체하는 방법" 항목을 참조하십시오.	

3. **Export(내보내기)**를 클릭합니다.

   Secure Network Analytics 해당 설정을 다운로드 폴더에 다운로드되는 XML 파일에 저장합니다.

> 도메인 내보내기는 설정을 백업하는 것과 다릅니다. 어플라이언스 설정을 백업하려면 **어플라이언스 구성 백업 생성**을 참조하십시오.

동기화 데이터스토어 및 비데이터스토어 도메인

비데이터스토어플로우 컬렉터 도메인을 데이터스토어플로우 컬렉터 도메인으로 전환 중인 경우, 비데이터스토어 도메인과 데이터스토어도메인 간에 구성 및 튜닝을 동기화할 수 있습니다. 이 섹션에서는 비데이터스토어 도메인을 관련 데이터스토어 도메인과 동기화하는 프로세스에 대해 설명합니다

시작하기 전에

비데이터스토어 도메인과 동기화할 데이터스토어 도메인을 이미 생성했는지 확인합니다. **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**에 설명된 프로세스를 이미 따른 경우, 데이터스토어 도메인이 이미 생성되어 있어야 합니다. 도메인 추가에 대한 지침은 **도메인 추가 및 구성**을 참조하십시오.

> You need administrator access for this procedure.

Synchronized Properties

The following properties will be synchronized between domains:

- Data Store domain specific configuration as well as alert configuration (if enabled). Domain configuration includes:
  - Host Group Management
  - Alarm Severity
  - Policy Management
  - Services, Applications
  - Exporter SNMP profiles (not including passwords)
  - Domain AS Numbers.

Recommended Synchronization Frequency

While you can synchronize your domains as often as you like, we recommend that you limit your synchronizations to only after you perform a group of changes or once a day or week. This is because the synchronization process requires the use of resources that take away from daily processing.

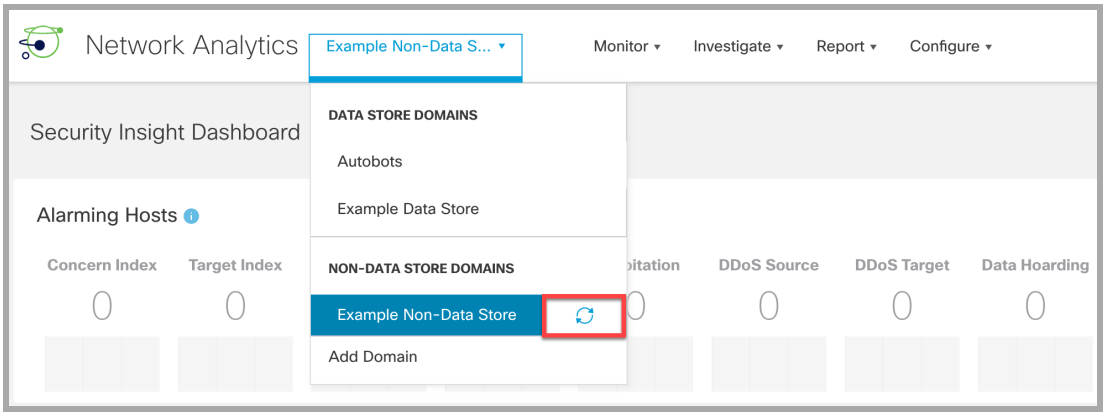
Synchronizing Domains Procedure

Follow these steps to synchronize your Non-데이터스토어 domain (Source) with your 데이터스토어 domain (Target).

1. From the menu bar, choose the Non-데이터스토어 domain that you want to synchronize with your 데이터스토어 domain.
2. From the main menu, choose **Configure > SYSTEM Domain Properties**.
3. Select the **Edit** button.
4. Choose the Data Store domain that you want to synchronize this domain with in the **Target Domain to Synchronize** drop-down menu.

> You can only synchronize your target 데이터스토어 domain with one source Non-데이터스토어 domain. If you attempt to synchronize your target Data Store domain with more then one source Non-데이터스토어 domain, you will receive an error.

5. Click the **Save** button to save your changes. A synchronize button appears next to the Non-데이터스토어 domain that you selected to synchronize with your 데이터스토어 domain.



도메인 동기화 대상 도메인 제거

아래 단계에 따라 대상 도메인을 제거합니다.

1. 메뉴 모음에서 데이터스토어 도메인과 동기화하려는 비데이터스토어 도메인을 선택합니다.
2. 기본 메뉴에서 **Configure(구성) > Domain Properties(도메인 속성)**를 선택합니다.
3. **Edit(편집)** 버튼을 선택합니다.
4. **Clear Target Domain(대상 도메인 삭제)** 버튼을 클릭합니다.
5. **Save(저장)** 버튼을 클릭하여 변경 사항을 저장합니다.

도메인 삭제

도메인을 삭제하기 전에 이러한 지침을 검토하여 요구 사항을 이해해야 합니다.

> 도메인을 삭제하면 해당 도메인에 대해 수집된 모든 데이터에 액세스할 수 없게 됩니다. 수집된 데이터에 더 이상 액세스할 필요가 없는 도메인만 삭제하십시오.

1. Central Management에서 플로우 컬렉터 제거

도메인에 플로우 컬렉터이 포함되어 있는 경우, 도메인을 삭제하기 전에 Central Management에서 이를 제거하십시오. 플로우 컬렉터를 다른 도메인에 추가할 수 있지만, 이 절차에는 공장 기본값(RFD)으로 재설정이 포함됩니다. 지침은 다음을 참조하십시오.

1. **Central Management에서 어플라이언스 제거**
2. **공장 기본값 재설정**
3. **Central Management에 어플라이언스 추가**

> Central Management에서 플로우 컬렉터를 제거하고 도메인을 삭제하면 관련 플로우 컬렉터 데이터가 손실됩니다.

2. 도메인 삭제

1. 에 먼저 액세스해야 하는 경우 드롭다운 메뉴에서 **[Current domain name(현재 도메인 이름)]**을 선택합니다.

2. 메인 메뉴에서 **Configure(구성) > SYSTEM Domain Properties(시스템 도메인 속성)**을 선택합니다.
3. **Delete Domain(도메인 삭제)**를 클릭합니다.

> 도메인을 삭제하면 해당 도메인에 대해 수집된 모든 데이터에 액세스할 수 없게 됩니다. 수집된 데이터에 더 이상 액세스할 필요가 없는 도메인만 삭제하십시오.

데스크탑 클라이언트 도메인 삭제

Secure Network Analytics에서 데이터 저장소 없이 데스크탑 클라이언트를 사용하는 경우, 데스크탑 클라이언트에서 도메인을 삭제할 수도 있습니다.

> 삭제하려는 도메인에 대해 수집된 모든 데이터에 액세스할 수 없게 되므로 삭제할 데스크톱 클라이언트 도메인을 결정할 때는 주의하십시오.
> **해결 방법**: 실수로 데스크톱 클라이언트에서 모든 도메인을 삭제하고 관리자 웹 애플리케이션에서 잠긴 경우 데스크톱 클라이언트에서 데이터 저장소가 아닌 새 도메인을 생성합니다. 이렇게 하면 매니저 웹 애플리케이션에 다시 액세스할 수 있습니다. 도메인 생성에 대한 자세한 내용은 데스크톱 클라이언트 도움말의 Add Domain(도메인 추가) 항목을 참조하십시오.

통합 및 추가 구성

다음과 같은 추가 통합 및 구성을 이용할 수 있습니다.

https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html. 통합이 여기에 표시된 목록보다 더 많을 수 있습니다.

- Stealthwatch로 NSEL 내보내기를 위한 Cisco ASA 구성
- 고객 성공 메트릭 설정 가이드
- 여러 NetFlow 엑스포터 활성화
- 엔드포인트 라이선스 및 NVM(Network Visibility Module) 구성 가이드
- 플로우 센서 및 로드 밸런서 통합 가이드
- 전역 위협 알림 구성 가이드
- ISE 및 ISE-PIC 설정 가이드
- Secure Network Analytics 및 SecureX 통합 가이드
- 매니지드 어플라이언스용 SSL/TLS 인증서
- TACACS + 설정 가이드
- Cisco Security Analytics and Logging(온프레미스)

비밀번호

다음과 같이 비밀번호를 변경할 수 있습니다.

- **비밀번호 재설정 활성화 또는 비활성화**
- **비밀번호를 기본 설정으로 재설정**
- **비밀번호 변경**
- **데이터 저장소 데이터베이스 비밀번호 변경**
- **플로우 컬렉터 데이터베이스 비밀번호 변경(비데이터 저장소 도메인)**

비밀번호 재설정 활성화 또는 비활성화

비밀번호 재설정 기능을 활성화하거나 비활성화하려면 다음 지침을 따르십시오. Enable(활성화)을 선택하면 GRUB 명령줄 인터페이스를 사용하여 비밀번호를 기본 설정으로 재설정할 수 있습니다.

> 비밀번호 재설정을 비활성화하고 비밀번호를 잃어버릴 경우 어플라이언스에 저장된 데이터에 대한 액세스 권한을 잃게 됩니다. 어플라이언스에 다시 액세스하려면 공장 기본값으로 재설정하고 다시 구성합니다.

1. 어플라이언스 콘솔에 root로 로그인합니다.
2. **SystemConfig**를 입력합니다. Enter를 누릅니다.
3. **Security(보안)**를 선택합니다.
4. **Password Reset(비밀번호 재설정)**를 선택합니다.
5. 화면에 표시되는 프롬프트에 따라 SSH를 활성화하거나 비활성화합니다.

비밀번호를 기본 설정으로 재설정

비밀번호를 기본 설정으로 재설정하는 방법에는 두 가지가 있습니다.

- **Admin 비밀번호:** 에서 **관리자 비밀번호 재설정 매니저**
- **Admin, Root, Sysadmin 비밀번호:** **Admin, Root, Sysadmin 비밀번호를 기본값으로 재설정**을 사용합니다.

> 어플라이언스 비밀번호를 기본값으로 재설정한 후에 변경해야 합니다. 이 단계는 보안에 중요합니다. 자세한 지침은 **비밀번호 변경**을 참조하십시오.

관리자 비밀번호 재설정 매니저

다음 지침에 따라 매니저에서 **admin** 비밀번호를 기본 설정으로 재설정합니다. 이후 보안을 극대화하기 위해 어플라이언스 비밀번호를 변경합니다.

- **요구 사항**: 이 지침을 완료하려면 어플라이언스 루트 비밀번호가 필요합니다.
- **다른 사용자:** 이 지침에 따라 admin 사용자가 기본 비밀번호로 재설정됩니다. 개별 사용자 비밀번호는 변경되지 않습니다.
- **기타 어플라이언스:** 이 지침은 다른 Secure Network Analytics 어플라이언스(플로우 컬렉터, 플로우 센서 또는 UDP Director)의 admin 비밀번호를 재설정하지 않습니다.

1. 어플라이언스 콘솔에 root로 로그인합니다.
2. `rm /lancope/var/smc/config/users/admin/user.xml`을 입력합니다. Enter를 누릅니다.
3. `docker restart smc`를 입력합니다. Enter를 누릅니다.
4. `docker restart nginx`를 입력합니다. Enter를 누릅니다.

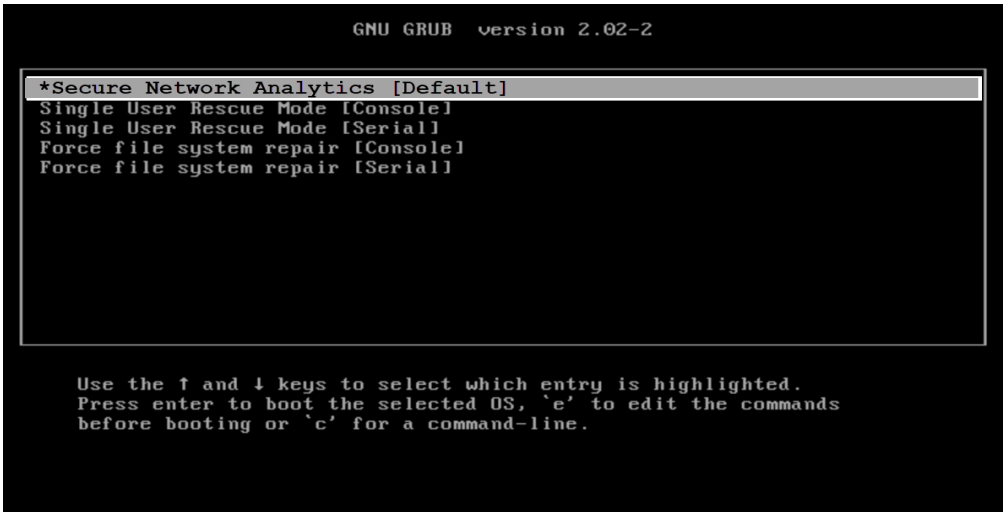
   이렇게 하면 admin 비밀번호가 기본값으로 재설정됩니다.

5. 어플라이언스 콘솔을 종료합니다.
6. admin 비밀번호를 기본값에서 변경하려면 **비밀번호 변경**으로 이동합니다. 이 단계는 보안에 중요합니다.

Admin, Root, Sysadmin 비밀번호를 기본값으로 재설정

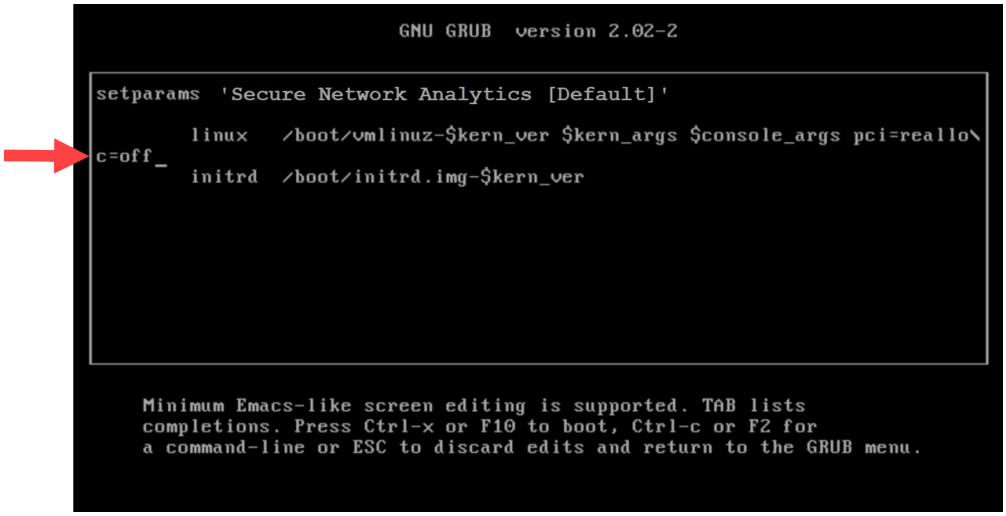
콘솔 액세스를 사용하여 어플라이언스 **admin**, **root** 및 **sysadmin** 비밀번호를 기본 설정으로 재설정합니다. 이후 보안을 극대화하기 위해 어플라이언스 비밀번호를 변경합니다.

1. 어플라이언스 콘솔(CIMC 또는 하이퍼바이저)다음에 로그인합니다.
2. 어플라이언스를 재부팅합니다.
3. 콘솔 화면에 GRUB 메뉴가 표시되면 "e"를 입력하여 편집 모드를 시작합니다.



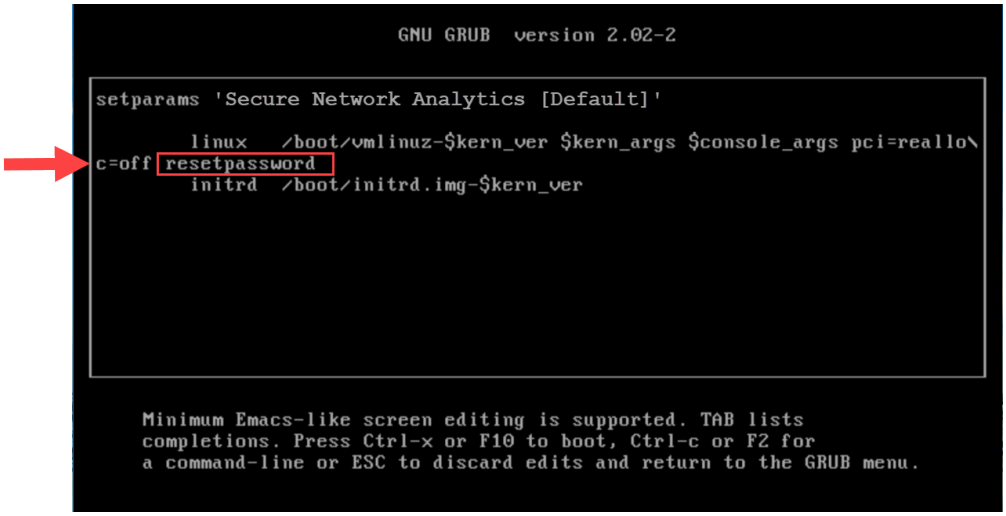
4. 커서를 두 번째 라인으로 이동합니다.

어플라이언스 버전에 따라 명령줄이 약간 다르게 보일 수 있습니다.



5. 명령줄을 다음 예와 같이 설정하려면 `resetpassword`를 입력하고 `c=off`를 입력합니다.

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
 c=off resetpassword
```



6. CTRL-X를 입력하여 부팅을 재개합니다.

   이렇게 하면 admin, root 및 sysadmin 비밀번호가 기본값으로 재설정됩니다.

7. 기본값에서 비밀번호를 변경하려면 **비밀번호 변경**으로 이동합니다. 이 단계는 보안에 중요합니다.

비밀번호 변경

다음 지침에 따라 비밀번호를 기본 비밀번호 또는 이전 비밀번호에서 변경합니다. 다음 기준을 사용하는지 확인합니다.

- **길이:** 8~256 문자
- **변경**: 새 비밀번호는 이전 비밀번호와 최소 4자 이상 달라야 합니다.

사용자	기본 비밀번호
관리자	lan411cope
root	lan1cope
sysadmin	lan1cope

Sysadmin 비밀번호 변경

1. 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
2. **Security(보안)**를 선택합니다.
3. **비밀번호**를 선택합니다.
4. 화면에 표시되는 프롬프트에 따라 sysadmin 비밀번호를 변경합니다.
5. 시스템 설정을 종료합니다.

Root 비밀번호 변경

1. 어플라이언스 콘솔에 root로 로그인합니다.
2. **SystemConfig**를 입력합니다. Enter를 누릅니다.
3. **Security(보안)**를 선택합니다.
4. **비밀번호**를 선택합니다.
5. 화면에 표시되는 메시지에 따라 루트 비밀번호를 변경합니다.
6. 시스템 설정을 종료합니다.

Admin 비밀번호 변경 매니저

1. 매니저에 admin으로 로그인합니다.

    - **URL:** https://<IPAddress>
    - **로그인:** admin
    - **기본 비밀번호**: lan411cope

2. **Configure(구성) > GLOBAL User Management(전역 사용자 관리)**를 선택합니다.
3. 목록에서 **admin** 사용자를 찾습니다.
4. **작업** 메뉴를 클릭합니다. **비밀번호 변경**을 선택합니다.
5. 화면에 표시되는 메시지에 따라 관리자 비밀번호를 변경합니다. 다음 기준을 사용합니다.

    - **길이:** 8~256 문자
    - **변경:** 새 비밀번호는 기본 비밀번호와 다르며 최소 4자 이상이어야 합니다.

다른 모든 어플라이언스에서 Admin 비밀번호 변경

다음 지침에 따라 데이터 노드, 플로우 컬렉터, 플로우 센서 또는 UDP Director에서 admin 사용자 비밀번호를 변경합니다.

1. 어플라이언스 관리 인터페이스에 admin으로 로그인

    - **URL:** https://<IPAddress>
    - **로그인:** admin
    - **기본 비밀번호**: lan411cope

2. **Manage Users(사용자 관리)** > **Change Password(비밀번호 변경)**을 선택합니다.
3. 현재 비밀번호와 새 비밀번호를 입력합니다.
4. **적용**을 클릭합니다. 화면에 표시되는 메시지에 따라 비밀번호를 변경합니다.
5. 다른 어플라이언스에서 admin 비밀번호를 변경하려면 1~4단계를 반복합니다.

데이터 저장소 데이터베이스 비밀번호 변경

데이터스토어 시스템 구성을 사용하여 데이터베이스 비밀번호(dbadmin 및 readonlyuser)를 변경합니다. 이 절차의 일부로 SSH를 일시적으로 활성화해야 합니다.

1. 매니저 어플라이언스 콘솔(SystemConfig)에 root로 로그인합니다.
2. 기본 메뉴에서 **Data Store(데이터 저장소)**를 선택합니다.
3. **SSH**를 선택합니다. 화면에 표시되는 프롬프트에 따라 SSH를 활성화합니다.
4. 데이터스토어메뉴에서 **Password(비밀번호)**를 선택합니다.
5. 화면에 표시되는 메시지에 따라 비밀번호를 변경합니다.

    데이터스토어 메뉴를 종료하면 이전 SSH 설정이 복원됩니다.

플로우 컬렉터 데이터베이스 비밀번호 변경(비데이터 저장소 도메인)

Central Management 페이지의 데이터베이스 탭을 사용하여 비데이터 저장소 도메인에 있는 모든 플로우 컬렉터 데이터베이스의 플로우 컬렉터 데이터베이스 비밀번호를 업데이트합니

다.

> 기본 비밀번호를 변경해야 합니다. 새 플로우 컬렉터가 Central Management에 추가되면 데이터베이스 비밀번호가 현재 비밀번호와 일치하도록 자동으로 업데이트됩니다.

1. Central Management를 엽니다.
2. 데이터베이스 탭을 클릭합니다.
3. 임의의 비밀번호를 생성하려면 **Generate Password(비밀번호 생성)** 버튼을 클릭합니다. 그렇지 않은 경우 비밀번호 및 비밀번호 확인 필드에 비밀번호를 입력합니다.
4. 선택한 비밀번호를 보려면 **비밀번호 표시** 체크 박스를 선택합니다.
5. **Apply Settings(설정 적용)** 버튼을 클릭하여 변경 사항을 저장합니다.

> 데이터베이스 비밀번호를 변경하면 비데이터 저장소 플로우 컬렉터 및 전환 플로우 컬렉터만 새 비밀번호를 수신합니다.

SSL/TLS 어플라이언스 ID 및 추가 SSL/TLS 클라이언트 ID

SSL/TLS 어플라이언스 ID 및 추가 SSL/TLS 클라이언트 ID를 사용하여 선택한 어플라이언스에 대한 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 인증서를 관리합니다. 모든 인증서 관련 변경 사항은 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

> 인증서는 시스템 보안에 중요합니다. 인증서를 부적절하게 수정하면 Secure Network Analytics 어플라이언스 통신이 중단되며 데이터 손실이 발생할 수 있습니다. 모든 인증서 관련 변경 사항은 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

어플라이언스 ID

각 Secure Network Analytics version 7.x 어플라이언스는 고유한 자체 서명 어플라이언스 ID 인증서를 사용해 설치됩니다. 어플라이언스 ID 인증서를 교체하려면 매니지드 어플라이언스를 위한 SSL/TLS 인증서 가이드의 지침을 따르십시오.

어플라이언스는 SSL 인증서를 사용하여 다른 어플라이언스에 대한 ID를 확인합니다. 예를 들어 매니저가 플로우 쿼리를 생성하고 플로우 컬렉터와 통신할 때, 매니저는 서버 ID 인증서를 제시하여 인증됩니다. 플로우 컬렉터는 제공된 서버 ID 인증서가 신뢰할 수 있는 인증서인지 확인합니다.

클라이언트 ID

클라이언트 ID는 외부 서비스 간 통신에 사용됩니다. 세부 정보는 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

인증서 검토

다음 지침에 따라 선택한 어플라이언스에 대한 어플라이언스 ID 인증서를 검토합니다.

1. Central Management를 엽니다.
2. 어플라이언스에 대한 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **어플라이언스 설정 편집**을 선택합니다.
4. **어플라이언스** 탭을 선택합니다.
5. **어플라이언스 ID 인증서를 검토하려면,** SSL/TLS Appliance Identity(SSL/TLS 어플라이언스 ID) 섹션으로 이동합니다.

   클라이언트 ID 인증서를 검토하려면, Additional SSL/TLS Client Identities(추가 SSL/TLS 클라이언트 ID) 섹션으로 이동합니다.

> 인증서는 시스템 보안에 중요합니다. 인증서를 부적절하게 수정하면 Secure Network Analytics 어플라이언스 통신이 중단되며 데이터 손실이 발생할 수 있습니다. 모든 인증서 관련 변경 사항은 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

사용자 지정 인증서를 사용하여 Central Management에 어플라이언스 추가

자세한 내용은 **Central Management에 어플라이언스 추가**를 참조하십시오. 어플라이언스에 맞춤 인증서가 있는 경우 Central Management에 어플라이언스를 추가하기 전에 ID 인증서 및 인증서 체인(루트 및 중간)을 매니저 Trust Store에 저장해야 합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.

> 어플라이언스에 맞춤 인증서가 있는 경우 Central Management에 어플라이언스를 추가하기 전에 ID 인증서 및 인증서 체인(루트 및 중간)을 매니저 Trust Store에 저장해야 합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.

호스트 이름, 네트워크 도메인 이름 또는 IP 주소 변경

어플라이언스를 설치하고 구성한 후에 어플라이언스 호스트 이름, 네트워크 도메인 이름 또는 IP 주소를 변경하려면, 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

이 절차의 일환으로 Central Management에서 일시적으로 어플라이언스를 제거하면 어플라이언스 ID 인증서가 자동으로 교체됩니다.

> 어플라이언스 ID 인증서는 이 절차 중 자동 대체됩니다.
>
> **어플라이언스에서 사용자 지정 인증서를 사용하는 경우,** Cisco 지원팀에 문의하여 이러한 설정을 변경하십시오. 여기에 나와 있는 지침은 사용하지 마십시오. 사용자 지정 인증서 및 개인 키의 복사본이 있는지 확인합니다.

신뢰 스토어 인증서 검토

어플라이언스 신뢰 저장소에 인증서를 추가하면 해당 ID(다른 Secure Network Analytics 어플라이언스 또는 외부 서비스)와의 통신이 허용됩니다.

- **지침:** 모든 신뢰 저장소 변경은 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.
- **개별 파일 업로드:** 파일에 둘 이상의 인증서가 포함된 경우, 각 인증서를 신뢰 저장소에 개별적으로 업로드합니다.

> 어플라이언스 신뢰 저장소에 인증서를 추가하면 어플라이언스는 해당 ID를 신뢰하고 해당 ID와의 통신을 허용합니다. 모든 신뢰 저장소 변경은 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

다음 지침에 따라 선택한 어플라이언스 신뢰 저장소에 저장된 인증서를 검토합니다.

1. Central Management를 엽니다.
2. 어플라이언스에 대한 **작업** 메뉴를 클릭합니다.
3. **어플라이언스 설정 편집**을 선택합니다.
4. **일반** 탭을 선택합니다.
5. **신뢰 저장소** 목록을 검토합니다.

위협 피드

Cisco Secure Network Analytics 위협 피드(이전 명칭: Stealthwatch 위험 인텔리전스 피드)는 네트워크에 대한 위협에 대하여 전역 위협 피드의 데이터를 제공합니다. 피드는 자주 업데이트되며 악의적인 활동에 사용되는 것으로 확인된 IP 주소, 포트 번호, 프로토콜, 호스트 이름 및 URL을 포함합니다. 피드에 포함되는 호스트 그룹은 커맨드 앤 컨트롤 서버, bogons 및 Tors입니다.

라이선싱

Cisco Smart Account에 위협 피드 라이선스를 추가합니다. 지침은 Secure Network Analytics 스마트 소프트웨어 라이선싱 가이드를 참조하십시오.

활성화 중

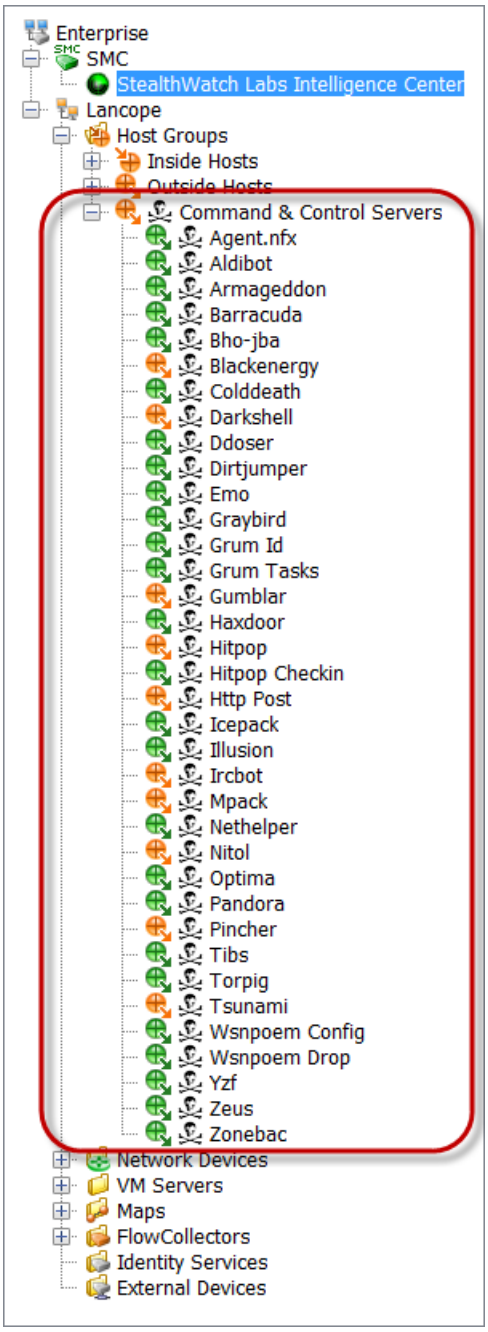
Central Management에서 피드를 활성화하려면 도움말의 지침을 따르십시오. 지침의 일부로 DNS 서버 및 방화벽을 구성하게 됩니다. 또한 페일오버 구성이 있는 경우, 기본 매니저와 보조 매니저에서 위협 피드를 활성화해야 합니다.

1. 기본 매니저에 로그인합니다.
2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
3. **(도움말) 아이콘**를 클릭합니다. **Help(도움말)**를 선택합니다.
4. **Appliance Configuration(어플라이언스 구성) > 위협 피드**를 선택합니다.

알람 및 보안 이벤트 검토

위협 피드가 활성화된 경우 Stealthwatch 랩 인텔리전스 센터 아이콘이 알람 상태와 함께 데스크톱 클라이언트 엔터프라이즈 트리에 표시되고 위협이 해당 호스트 그룹 브랜치에 표시됩니다. 자세한 내용은 데스크톱 클라이언트 사용자 가이드 또는 도움말을 참조하십시오.

> **도움말:** 도움말을 확인하려면 Stealthwatch **랩 인텔리전스 센터** 브랜치를 마우스 오른쪽 버튼으로 클릭한 다음 **Configuration(구성) > SLIC Threat Feed Configuration(SLIC 위협 피드 구성)**을 선택합니다. **도움말**을 클릭합니다.



Central Management(어플라이언스 관리)

Central Management를 사용하여 기본 매니저에서 어플라이언스를 관리합니다. 여기에는 Central Management에 대한 개요를 포함하며 각 섹션에 대한 세부 정보는 도움말에서 확인하십시오.

- **Central Management 정보:** Central Management가 어플라이언스를 관리하는 경우 상태를 검토하고 어플라이언스 설정 편집, 소프트웨어 업데이트, 재푸팅, 종료 등을 관리할 수 있습니다.
- **도움말:** 도움말을 열려면 ? (**도움말**) 아이콘를 클릭합니다. **Help(도움말)**를 선택합니다.

이 섹션에서는 다음 내용을 다룹니다.

- **Central Management 및 어플라이언스 관리 인터페이스**
- **Central Management 열기**
- **어플라이언스 관리자 열기**
- **어플라이언스 구성 편집**
- **어플라이언스 통계 보기**
- **Central Management에서 어플라이언스 제거**
- **Central Management에 어플라이언스 추가**
- **어플라이언스 구성 백업 생성**
- **SSH 활성화/비활성화**

Central Management 및 어플라이언스 관리 인터페이스

Central Management를 통해 어플라이언스를 관리하면 Central Management 및 어플라이언스 관리 인터페이스(어플라이언스 관리자)에서 다음과 같은 어플라이언스 기능에 액세스할 수 있습니다.

중앙 관리	어플라이언스 관리자 인터페이스
어플라이언스 컨피그레이션 수정	시스템 통계 보기
라이선스 상태 검토(개요)	
설정 파일 백업	데이터베이스 파일 백업
감사 로그 보기	진단 팩 생성

재부팅	네트워크 호스트 및 IP 조회
종료	패킷 캡처
소프트웨어 업데이트	DNS 캐시 지우기
	어플라이언스별 설정

> 데이터스토어 호환성을 위해 플로우 컬렉터를 구성할 경우 어플라이언스 관리 인터페이스(어플라이언스 관리)에서 특정 기능을 숨깁니다. Central Management를 사용하여 플로우 컬렉터 및 기타 관련 작업을 설정합니다.

Central Management 열기

1. 기본 매니저에 로그인합니다.
2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.

어플라이언스 관리자 열기

Central Management 또는 어플라이언스 직접 로그인을 통해 어플라이언스 관리 인터페이스에 액세스할 수 있습니다.

Central Management를 통해 어플라이언스 관리자 열기

1. Central Management 인벤토리 페이지에서 어플라이언스에 대한 **Actions(작업)** 메뉴를 클릭합니다.
2. **어플라이언스 통계 보기**를 선택합니다.
3. 어플라이언스 관리 인터페이스에 로그인합니다.

직접 로그인을 통해 어플라이언스 관리자 열기

1. 브라우저 주소 표시줄에 다음과 같이 어플라이언스 IP 주소를 입력합니다.

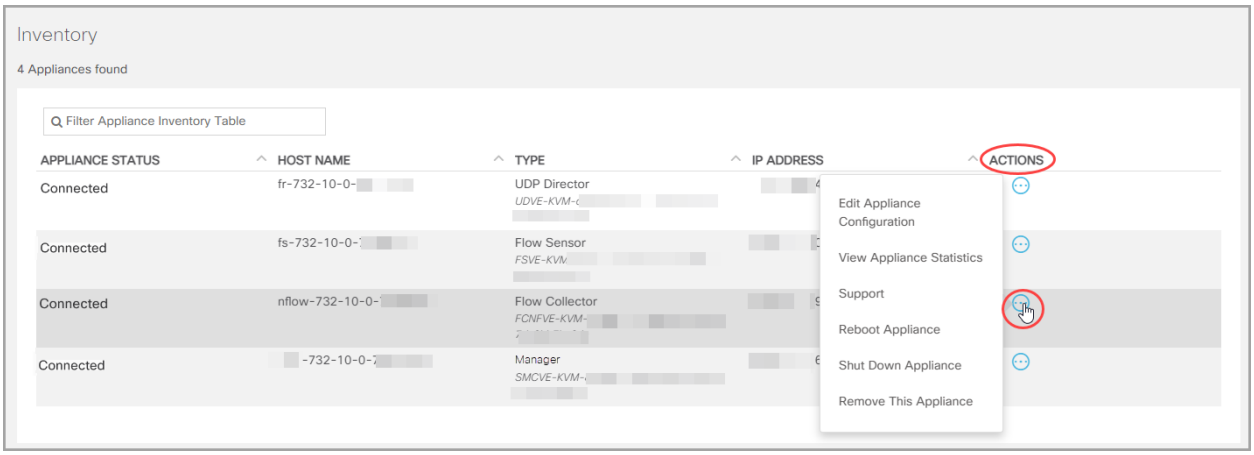
   https://<IPAddress>

   - **매니저:** IP 주소 뒤에 **/매니저smc/index.html**를 추가합니다.
   - **예:** https://1.1.1.1/매니저/index.html

2. Enter를 누릅니다.

어플라이언스 구성 편집

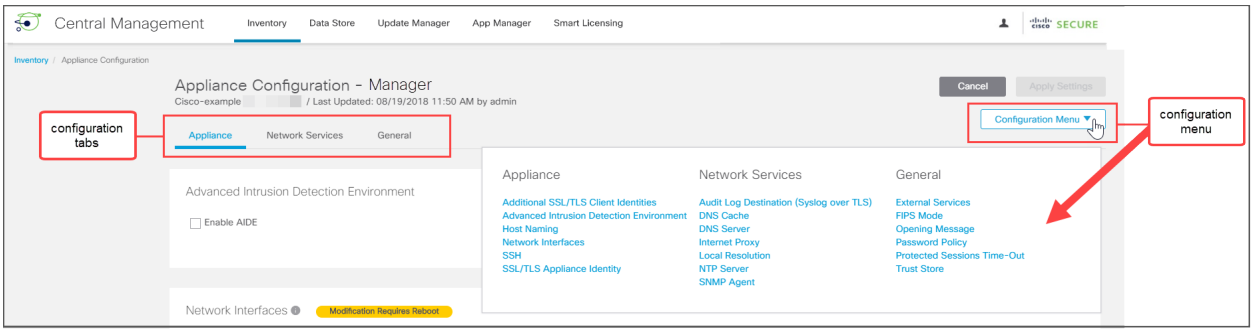
1. Central Management 인벤토리 페이지에서 어플라이언스에 대한 **Actions(작업)** 메뉴를 클릭합니다.
2. **어플라이언스 설정 편집**을 선택합니다.



3. **설정** 메뉴를 클릭합니다. 목록에서 항목을 선택합니다.

   또는

   각 탭을 클릭하여 각 설정 범주를 검토합니다.



4. 필요에 따라 각 설정 섹션을 변경합니다. 각 설정 탭에서 둘 이상의 설정 범주를 편집할 수 있습니다.

> 지침을 보려면 **사용자** 아이콘을 클릭합니다.

5. **설정 적용**을 클릭합니다. 화면에 표시되는 프롬프트를 따라 설정 변경 사항을 저장합니다.

   일부 변경 사항은 시스템을 재부팅해야 합니다. 기다리고 싶은 경우 변경 사항을 되돌리고 구성 설정을 편집하고 나중에 다시 부팅할 수 있습니다.

> 어플라이언스가 자동으로 재부팅됩니다. 설정 변경 사항이 보류 중인 경우 어플라이언스가 강제로 재부팅되지 않도록 합니다. 어플라이언스 상태가 Connected(연결됨)인지 확인하려면 Central Management > 인벤토리를 검토하십시오.

6. **Connected(연결됨):** 인벤토리 페이지에서 어플라이언스가 구성 변경을 완료하고 어플라이언스 상태가 **Connected(연결됨)**으로 돌아오는지 확인합니다.

어플라이언스 통계 보기

가리키기: 각 어플라이언스 상태에 대한 자세한 내용을 보려면 포인터를 상태 위에 놓습니다.

시스템 통계, 서비스, 디스크 사용량 및 도커 서비스를 확인하려면 어플라이언스 관리 인터페이스에 로그인합니다.

1. Central Management 인벤토리 페이지에서 어플라이언스에 대한 **Actions(작업)** 메뉴를 클릭합니다.
2. **어플라이언스 통계 보기**를 선택합니다.
3. 어플라이언스 관리 인터페이스에 로그인합니다.

Central Management에서 어플라이언스 제거

다음 지침을 사용하여 Central Management에서 어플라이언스를 제거합니다.

1. Central Management 인벤토리 페이지에서 어플라이언스에 대한 **Actions(작업)** 메뉴를 클릭합니다.
2. **이 어플라이언스 제거**를 선택합니다.

   - **데이터 저장소 어플라이언스:** 추가 요구 사항을 확인하려면 **Central Manager에서 데이터스토어 어플라이언스 제거**로 이동하십시오.
   - **플로우 컬렉터:** Central Management에서 플로우 컬렉터를 제거하면 도메인에서도 제거됩니다. 다른 도메인에 추가하려는 경우 공장 기본값(RFD)을 재설정해야 합니다. 자세한 내용은 **Central Management에 어플라이언스 추가** 및 **Central Management에서 어플라이언스 제거**를 참조하십시오.
   - **Config 채널 다운:** 설정 채널이 다운되어 어플라이언스를 제거하는 경우 추가 지침을 확인하기 위해 문제 해결의 Config 채널 다운 절차로 이동합니다.
   - **문제 해결:** 어플라이언스 관리 인터페이스에 로그인하고 어플라이언스가 Central Management에서 제거되지 않은 경우 문제 해결의 구성 채널 중단 절차로 이동하여 시스템 설정을 사용하여 어플라이언스를 제거합니다.
   - **Central Management:** 다른 Central Management에 어플라이언스를 추가하려면 어플라이언스 설정 툴을 사용합니다.

> 어플라이언스에 맞춤 인증서가 있는 경우 Central Management에 어플라이언스를 추가하기 전에 ID 인증서 및 인증서 체인(루트 및 중간)을 매니저 Trust Store에 저장해야 합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.

Central Manager에서 데이터스토어 어플라이언스 제거

Central Manager(매니저, 플로우 컬렉터, 데이터 노드)에서 데이터스토어어플라이언스를 제거하는 경우, 데이터스토어 자체에서 제거되지는 않습니다. 수작업으로 정리해야 합니다.

- **관리자 및 플로우 컬렉터:** 매니저 및 플로우 컬렉터의 경우, **/lancope/var/services/data-store/config-datastore-inventory-snapshot** 디렉토리에서 제거할 수 있습니다.
- **데이터 노드:** 데이터 노드를 삭제하는 프로세스는 더 복잡하므로 Cisco 지원팀에 지원을 요청하십시오.

Central Management에 어플라이언스 추가

어플라이언스 설정 도구를 사용하여 Central Management에 어플라이언스를 추가합니다. 다음을 검토하는 것이 중요합니다.

- **맞춤 인증서:** 어플라이언스에 맞춤 인증서가 있는 경우 Central Management에 어플라이언스를 추가하기 전에 ID 인증서 및 인증서 체인(루트 및 중간)을 자체 Trust Store 및 매니저 Trust Store에 저장해야 합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.
- **매니저관리 자격 증명:** Central Management에 어플라이언스를 추가하려면 매니저, 사용자 ID 및 비밀번호가 필요합니다.
- **RFD:** 어플라이언스에서 공장 기본값을 재설정하는 경우, (RFD를 수행할 때 네트워크 설정을 유지하는 경우에도) Central Management에 추가하기 전에 어플라이언스 IP 주소, 호스트 이름 및 도메인을 구성합니다.

  sysadmin으로 어플라이언스 콘솔에 로그인하고 화면에 표시되는 프롬프트에 따라 IP 주소, 호스트 이름, 도메인을 구성합니다. 지침은 Secure Network Analytics 하드웨어 또는 Virtual Edition 설치 가이드를 참조하십시오.

- **신규 설치:** 신규 설치인 경우에는 설치를 완료하고 IP 주소, 호스트 이름 및 도메인을 구성한 후 Central Management에 추가합니다. 자세한 내용은 **1. 최초 설정을 사용하여 환경 구성**

> 어플라이언스에 맞춤 인증서가 있는 경우 Central Management에 어플라이언스를 추가하기 전에 ID 인증서 및 인증서 체인(루트 및 중간)을 매니저 Trust Store에 저장해야 합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서를 참조하십시오.

1. 어플라이언스에 로그인합니다.

   브라우저 주소 표시줄에 다음과 같이 어플라이언스 IP 주소를 입력합니다: **https://<IPAddress>**

2. URL 끝을 /lc-ast로 교체합니다.

https://<IPAddress>/lc-ast

3. Enter를 누릅니다.
4. **다음**을 클릭하여 Central Management 탭으로 스크롤합니다.
5. **IP 주소:** 매니저/Central Manager IP 주소를 입력합니다.
6. **Save(저장)**를 클릭합니다.
7. 화면의 지시에 따라 매니저 관리 자격 증명을 입력하고 구성을 완료합니다. 어플라이언스의 유형에 따라 추가 정보를 입력해야 할 수 있습니다.
8. 어플라이언스 설정 툴에 대한 자세한 내용은 **2. 매니지드 시스템 구성**

어플라이언스 구성 백업 생성

Central Management를 사용하여 어플라이언스 설정을 백업합니다.

> 어플라이언스를 백업하기 전에 도움말의 지침을 따르십시오. 데이터 저장소를 백업하려면 **데이터스토어 백업 생성**을 참조하십시오. 플로우 컬렉터 데이터베이스를 백업하려면 **데이터베이스 백업 생성(비데이터스토어 도메인)**을 참조하십시오.

1. Central Management를 엽니다.
2. 어플라이언스에 대한 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **Support(지원)**를 선택합니다.
4. **Configuration Files(구성 파일)** 탭을 선택합니다.
5. ? (**도움말**) 아이콘를 선택합니다. 도움말의 지침을 따르십시오.

   어플라이언스 구성 백업을 복원하려면 도움말의 지침을 따르십시오.

SSH 활성화/비활성화

이 섹션을 사용하여 SSH(Secure Shell)를 사용하여 어플라이언스에 액세스하는 기능을 제어합니다.

기본값: 비활성화

> SSH를 활성화하면 시스템의 보안 침해 위험이 증가합니다. SSH를 필요한 경우에만 활성화하는 것이 중요합니다. SSH 사용을 완료하면 SSH를 비활성화합니다.

SSH 열기

다음 지침에 따라 선택한 어플라이언스에 대한 SSH를 엽니다.

1. Central Management를 엽니다.
2. 어플라이언스에 대한 **작업** 메뉴를 클릭합니다.
3. **어플라이언스 설정 편집**을 선택합니다.
4. **어플라이언스** 탭을 선택합니다.

SSH 활성화

1. SSH 섹션을 찾습니다.
2. 어플라이언스에서 SSH 액세스를 허용하려면 **SSH 활성화** 확인란을 선택합니다.
3. 어플라이언스에 대한 루트 액세스를 허용하려면 **Enable Root SSH Access(루트 SSH 액세스 활성화)** 확인란을 선택합니다.

4. **설정 적용**을 클릭합니다.
5. 화면의 프롬프트를 따르십시오.

SSH 비활성화

1. 어플라이언스에서 SSH 액세스를 제거하려면 **SSH 활성화** 확인란을 클릭하여 선택을 취소합니다.
2. 어플라이언스에서 루트 액세스를 제거하려면 **Enable Root SSH Access(루트 SSH 액세스 활성화)** 확인란을 클릭하여 선택을 취소합니다.
3. **설정 적용**을 클릭합니다.
4. 화면의 프롬프트를 따르십시오.

데이터베이스 백업 생성(비데이터스토어 도메인)

다음 지침에 따라 관리자 및 플로우 컬렉터 데이터베이스를 백업합니다. 데이터 저장소를 백업하려면 **데이터스토어 백업 생성**을 참조하십시오.

> 백업이 없는 상태에서 업데이트 과정 중에 문제가 발생하는 경우 파일을 복구할 수 없습니다. 다음 지침을 따르고 데이터베이스 백업을 위한 모든 절차를 완료합니다. 또한 이 절차는 비데이터스토어 플로우 컬렉터에만 적용됩니다. 도움이 필요하면 Cisco 지원팀에 문의하십시오.

이 프로제스에서 다음 절차를 완료해야 합니다.

1. **플로우 컬렉터 데이터베이스 트리밍**
2. **데이터베이스 스냅샷 삭제**
3. **원격 파일 시스템 백업**
4. **데이터베이스 스냅샷 삭제**

1. 플로우 컬렉터 데이터베이스 트리밍

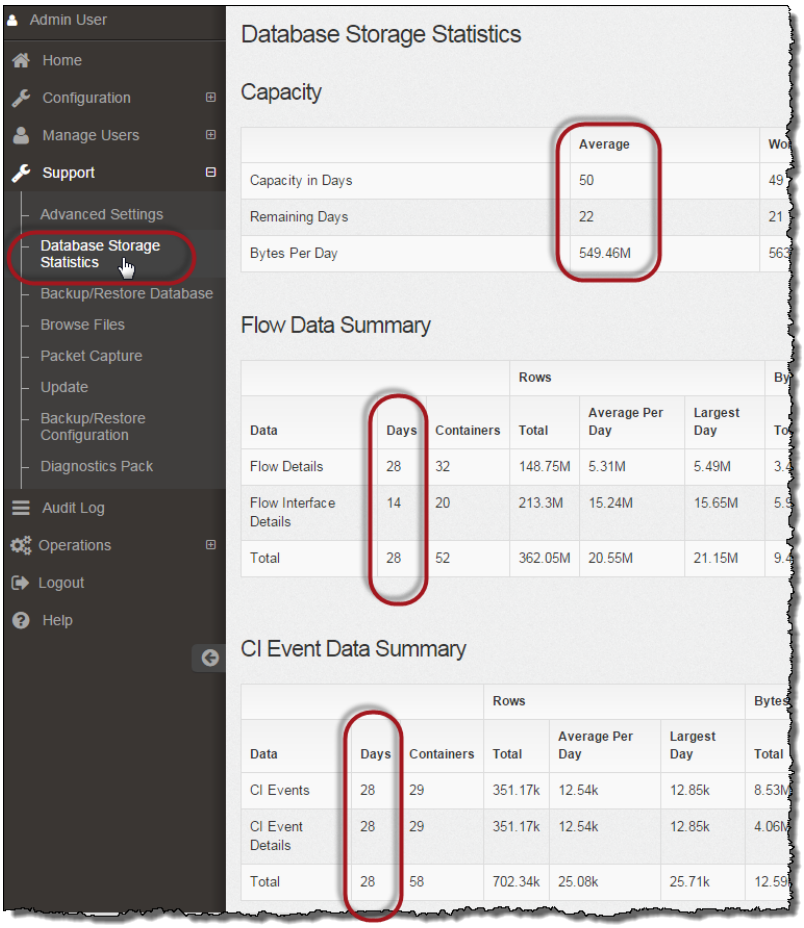
플로우 컬렉터 데이터베이스 백업을 완료하는 데 며칠이 걸릴 수 있으며 데이터베이스가 큰 경우 네트워크 속도가 느려집니다. 데이터베이스를 백업하기 전에 플로우 컬렉터 데이터베이스를 트리밍하는 것이 좋습니다. 이렇게 하면 플로우 저장에 사용할 수 있는 디스크 공간이 확보되며 데이터베이스를 백업하는 데 걸리는 시간이 단축됩니다.

플로우 컬렉터는 디스크 공간 및 일일 수집되는 데이터의 양을 기준으로 최대 일수를 저장합니다. 최대(/lancope/var 파티션의 75%)에 도달하면 데이터베이스는 새 데이터를 허용하기 위해 가장 오래된 데이터를 먼저 삭제하기 시작합니다.

1. 데이터베이스 스토리지 통계 리뷰

다음 지침에 따라 데이터베이스 스토리지를 확인합니다.

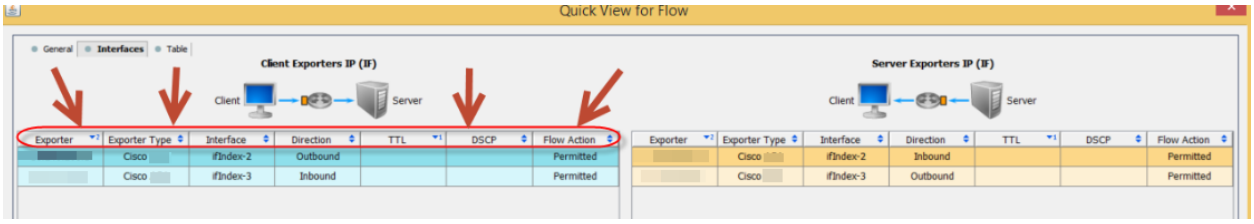
1. 플로우 센서 어플라이언스 관리 인터페이스에 로그인합니다.
2. **Support(지원)** > **Database Storage Statistics(데이터베이스 스토리지 통계)**를 클릭합니다.
3. Capacity(용량), Flow Data Summary(플로우 데이터 요약) 및 CI Event Data Summary (CI 이벤트 데이터 요약)(또는 Security Event Data Summary(보안 이벤트 데이터 요약))에 저장된 일수를 검토합니다.



2. 인터페이스 세부 정보 트리밍

플로우 인터페이스 데이터는 엑스포터의 인터페이스와 관련된 데이터입니다. Secure Network Analytics은 플로우 인터페이스 데이터 및 플로우 데이터를 저장합니다.

플로우 인터페이스 기본 설정은 시스템에서 플로우 데이터를 푸시하도록 하여 가능한 모든 인터페이스 통계를 유지할 수 있도록 합니다. 이 기능은 데스크탑 클라이언트를 데이터스토어 시스템에 적용되지 않는 기본 도구로 사용합니다. 트리밍 절차가 비 데이터스토어시스템에만 적용됨을 나타내기 위해 노드가 필요할 수 있습니다.



이 데이터를 백업하는 데 시간이 걸립니다. 모두 필요하지 않은 경우 스토리지 제한을 단축합니다(예: 7일). 이 제한보다 오래된 데이터는 손실됩니다.

다음 지침에 따라 설정한 제한보다 오래된 인터페이스 통계 데이터를 데이터베이스에서 삭제하여 플로우 저장에 사용할 수 있는 디스크 공간을 확보할 수 있습니다.

1. 관리자 사용자로 데스크탑 클라이언트에 로그인합니다.
2. 엔터프라이즈 트리에서 플로우 컬렉터를 찾습니다. 더하기(**+**) 기호를 클릭하여 컨테이너를 확장합니다.
3. 플로우 컬렉터를 마우스 오른쪽 버튼으로 클릭합니다. **Configuration(구성)** > **Properties (속성)**을 선택합니다.
4. Flow Collector Properties(플로우 컬렉터 속성) 대화 상자에서 **Advanced(고급)**를 클릭합니다.
5. **Store flow interface data(플로우 인터페이스 데이터 저장)**를 선택합니다.
6. 스토리지 제한을 줄이십시오. 예를 들어 제한을 **Up to 7 days(7일까지)**로 설정하는 경우, 7일보다 오래된 것은 손실됩니다.
7. **OK(확인)**를 클릭합니다.
8. 5분 정도 기다려서 다음 단계로 진행합니다.

3. 플로우 세부 정보 및 CI 이벤트 데이터 트리밍

플로우 컬렉터 데이터베이스에서 플로우 세부 정보 및 CI 이벤트/세부 정보의 크기를 줄이려면 Cisco 지원팀에 문의하십시오. 이 단계는 선택 사항이며 트리밍 프로세스를 완료하는 데 몇 분 정도밖에 걸리지 않지만 이 프로세스에서는 지침이 필요합니다.

NetFlow를 트리밍하는 경우 플로우 컬렉터 데이터베이스에서 Flow Details(플로우 세부 정보) 및 CI Event/Details(플로우 세부 정보)를 유지할 기간(일)을 지정합니다. 이 설정에서는 두 가지가 발생합니다.

- 데이터베이스는 입력한 일수로 트리밍됩니다.
- 데이터베이스는 가장 오래된 날짜를 기준으로 이전 데이터 롤아웃을 시작하지만 가능한 한 많은 양을 저장하지 않습니다.

2. 데이터베이스 스냅샷 삭제

백업 파일을 생성하기 전에 다음 지침을 사용하여 매니저 및 플로우 컬렉터 데이터베이스에 저장된 스냅샷을 삭제하십시오.

> 매니저 및 플로우 컬렉터 데이터베이스 스냅샷을 삭제해야 합니다. 이 단계는 성공적인 백업에 중요합니다.

1. 매니저 및 플로우 컬렉터 어플라이언스 데이터베이스 콘솔에 **admin**로 로그인합니다.
2. **스냅샷 확인:** 다음을 입력:

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from
database_snapshots;"
```

3. **스냅샷 삭제(있는 경우):** 다음을 입력:

```
/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. **스냅샷 폴더가 제거될 때까지 기다립니다.** 다음을 확인합니다.

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   결과가 비어 있지 않으면 계속 기다립니다. 데이터베이스의 크기에 따라 몇 분 정도 기다려야 폴더가 제거될 수 있습니다.

5. 1 ~ 4단계를 반복하여 저장된 모든 매니저 및 플로우 컬렉터 데이터베이스 스냅샷을 삭제합니다.

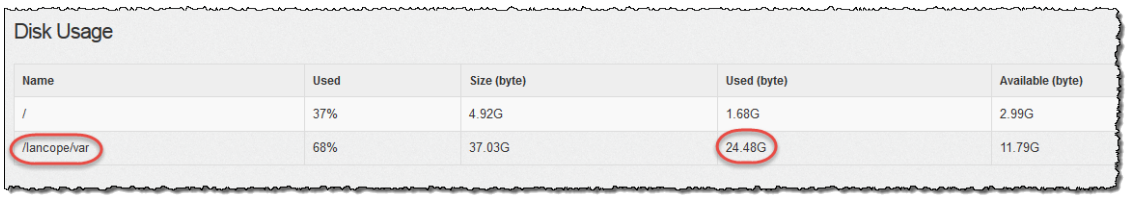
3. 원격 파일 시스템 백업

원격 파일 시스템에 데이터베이스를 백업하려면 다음 단계를 완료하십시오.

- **공간**: 원격 파일 시스템에 데이터베이스 백업을 저장할 공간이 충분한지 확인합니다.
- **시간**: 데이터베이스를 한 번 백업한 후에는 마지막 백업 이후 변경된 내용만 백업되므로 후속 백업이 더 빨라집니다. 이 프로세스는 분당 약 0.5GB ~ 2GB의 데이터를 백업합니다.

1. 어플라이언스 관리 인터페이스로 돌아갑니다(데스크톱 클라이언트를 닫지 마십시오).
2. 데이터베이스 백업을 저장하기 위해 원격 파일 시스템에 필요한 공간을 다음과 같이 결정합니다.

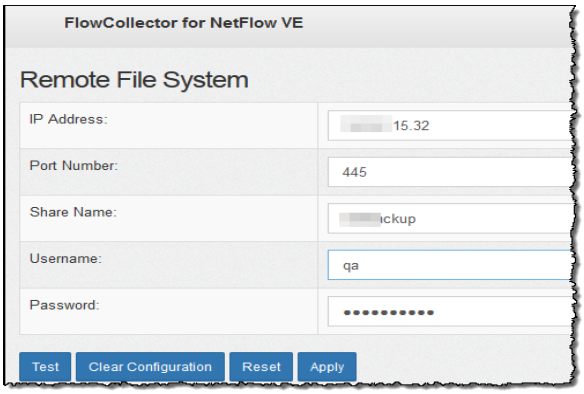
   - **Home(홈)**을 클릭합니다.
   - **Disk Usage(디스크 사용량)** 섹션을 찾습니다.
   - **/lancope/var** 파일 시스템의 **Used(byte)(사용됨: 바이트 기준)** 열을 검토합니다. 데이터베이스 백업을 저장하려면 최소한 이 공간과 원격 파일 시스템에 15 % 더 많은 공간이 필요합니다.



Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G

3. **Configuration(컨피그레이션)> Remote File System(원격 파일 시스템)**을 클릭합니다.



4. 백업 파일을 저장할 원격 파일 시스템의 설정을 사용하여 필드를 완료합니다.

   파일 공유는 SMB(Server Message Block)라고도 하는 CIFS(Common Internet File System) 프로토콜을 사용합니다.

5. **Apply(적용)**를 클릭하여 구성 파일에 설정을 저장합니다.

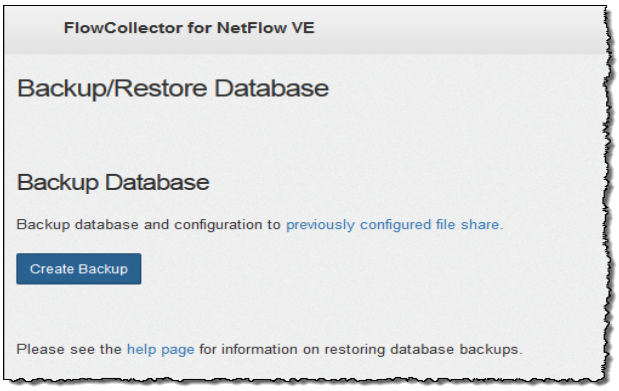
   비밀번호를 입력한 후 Apply(적용) 버튼이 활성화되지 않은 경우 Remote File System(원격 파일 시스템) 페이지의 빈 영역을 한 번 클릭하여 활성화합니다.

6. **Test(테스트)**를 클릭하여 어플라이언스와 원격 파일 시스템이 서로 통신할 수 있는지 확인합니다.

   테스트가 완료되면 Remote File System(원격 파일 시스템) 페이지의 하단에 다음 메시지를 확인해야 합니다.

   File sharing appears to be properly configured.

7. **Support(지원) > Backup/Restore Database(데이터베이스 백업/복원)**를 클릭합니다. 다음 예와 같이 Backup Database(데이터베이스 백업) 페이지가 열립니다.



8. **Create Backup(백업 생성)**을 클릭합니다. 이 프로세스는 시간이 오래 걸릴 수 있습니다.

- 백업 프로세스가 시작되면 프로세스를 중단하지 않고 페이지에서 마우스를 이동할 수 있습니다. 그러나 백업이 진행되는 동안 **Cancel(취소)**을 클릭하면 어플라이언스를 재시작하지 않고 백업을 다시 시작하지 못할 수 있습니다.
- 백업이 완료될 때까지 화면의 지시를 따릅니다.
- 백업 프로세스의 세부 정보를 보려면 **View Log(로그보기)**를 클릭합니다.

9. 진행 창을 닫으려면 **Close(닫기)**를 클릭합니다.

> 백업이 완료되기 전에 취소하는 경우에는 데이터베이스 스냅샷을 다시 삭제해야 합니다. **4. 데이터베이스 스냅샷 삭제**을 삭제하십시오.

4. 데이터베이스 스냅샷 삭제

백업 파일을 저장한 후 다음 지침에 따라 매니저 및 플로우 컬렉터 데이터베이스에서 스냅샷을 삭제합니다.

> 매니저 및 플로우 컬렉터 데이터베이스 스냅샷을 삭제해야 합니다. 이 단계는 성공적인 업데이트에 중요합니다.

1. 매니저 또는 플로우 컬렉터 어플라이언스 데이터베이스 콘솔에 **admin**로 로그인합니다.
2. **스냅샷 확인:** 다음을 입력:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

3. **스냅샷 삭제(있는 경우):** 다음을 입력:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot('StealthWatchSnap1');"
   ```

4. **스냅샷 폴더가 제거될 때까지 기다립니다.** 다음을 확인합니다.

   ```
   ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
   ```

   결과가 비어 있지 않으면 계속 기다립니다. 데이터베이스의 크기에 따라 몇 분 정도 기다려야 폴더가 제거될 수 있습니다.

5. 1 ~ 4단계를 반복하여 저장된 모든 매니저 및 플로우 컬렉터 데이터베이스 스냅샷을 삭제합니다.

데이터베이스 백업 복원(비데이터스토어 도메인)

매니저 및 플로우 컬렉터 데이터베이스를 복구하려면 다음 지침을 사용합니다. 데이터 저장소를 복원하려면 **데이터스토어 백업 복원** 복원을 참조합니다.

개요

> 데이터베이스를 복구하기 전에 Cisco 지원팀에 문의하는 것이 좋습니다.

데이터베이스 복원 작업은 현재 데이터베이스 및 구성을 이전 백업의 내용으로 **덮어씁니다.** 기존 네트워크 설정을 덮어쓰지 않습니다.

- **동일한 버전:** 이전 버전의 Secure Network Analytics 어플라이언스에서 백업 파일을 사용하여 어플라이언스 데이터베이스를 복원할 수 없습니다. 백업 파일 버전이 어플라이언스 버전과 일치하는지 확인합니다.
- **복원 이전 백업:** 명령줄 인터페이스를 사용하여 데이터베이스의 이전 백업을 복원할 수 있습니다. 백업된 데이터베이스는 이전에 구성된 원격 파일 시스템(파일 공유)에 있는 데이터베이스입니다.
- **기본값:** 복원할 데이터베이스의 이름을 지정하지 않은 경우, 기본 이름(시스템의 일련 번호)이 사용됩니다.

데이터베이스 복원

> 데이터베이스 복원 작업은 현재 데이터베이스 및 구성을 이전 백업의 내용으로 덮어씁니다. 기존 네트워크 설정을 덮어쓰지 않습니다.
>
> 복원 프로세스가 시작된 후에는 중단하지 마십시오.

작업이 시작된 후 페이지에서 나갈 수 있으며("마우스 이동") 프로세스가 중단 없이 계속됩니다. 돌아오면 상태가 업데이트됩니다.

1. 루트 쉘에 액세스하려면 어플라이언스 콘솔에 sysadmin으로 로그인합니다ㅅ
2. **sysadmin**을 입력하고 **Enter**를 누릅니다.
3. 비밀번호 프롬프트가 표시되면 **lan1cope**를 입력하고 **Enter**를 누릅니다.
4. 시스템 구성 메뉴에서 **Advanced(고급)**을 선택하고 **Enter**를 누릅니다.
5. **RootShell(루트쉘)**을 선택하고 **Enter**를 누릅니다.
6. 새 루트쉘 비밀번호를 입력한 다음 **Enter**를 누릅니다.
7. 다음 명령을 실행합니다.

```
cd /var/tmp
nohup doDbRestore -c -q &
```

이 도구로 사용할 수 있는 스위치를 보려면 `doDbRestore -h` 명령을 입력합니다.

> 복원할 데이터베이스의 이름을 지정하지 않은 경우, 기본 이름(시스템의 일련 번호)이 사용됩니다.

8. 진행 중인 복원 작업의 상태를 확인하기 위해 두 파일을 표시할 수 있습니다.

   /lancope/var/logs/VerticaRestore.log

   /lancope/var/logs/DatabaseRestore.log

   시스템이 복원 작업을 완료하면, 재부팅되고 데이터 수집이 시작됩니다.

데이터 저장소 데이터베이스

Secure Network Analytics을 데이터스토어로 구성한 경우, Central Management의 데이터스토어 탭에 액세스할 수 있습니다.

> 데이터스토어을 구성에 추가하려면 **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**와 **비데이터 저장소 구축에 데이터 저장소 추가**를 참조하십시오.

데이터 저장소 탭

Central Management에서 데이터스토어 탭을 사용하여 다음을 수행할 수 있습니다.

- **상태:** 데이터베이스 또는 모든 데이터 노드의 상태를 봅니다. 자세한 내용은 **데이터스토어 데이터베이스 상태 보기**를 참조하십시오.
- **시작 또는 중지:** 또한 데이터베이스 또는 모든 데이터 노드를 시작 또는 중지할 수 있습니다. 자세한 내용은 **데이터스토어 데이터베이스 상태 보기**를 참조하십시오.
- **스토리지 사용량**: 데이터베이스의 현재 스토리지 사용량 통계를 확인합니다. 플로우 인터페이스 데이터의 보존 상태를 수정할 수도 있습니다. 자세한 내용은 **데이터베이스 보존 보기**를 참조하십시오.
- **업데이트 상태:** 업데이트하는 동안 모든 데이터 노드의 상태를 확인합니다. 자세한 내용은 **데이터 노드 업데이트 상태 모니터링**을 참조하십시오.

> 모든 데이터 노드에서 SSH를 활성화합니다. SSH가 모든 데이터 노드에서 활성화되지 않은 경우 일부 데이터베이스 작업을 성공적으로 완료할 수 없습니다.

데이터 저장소 탭 열기

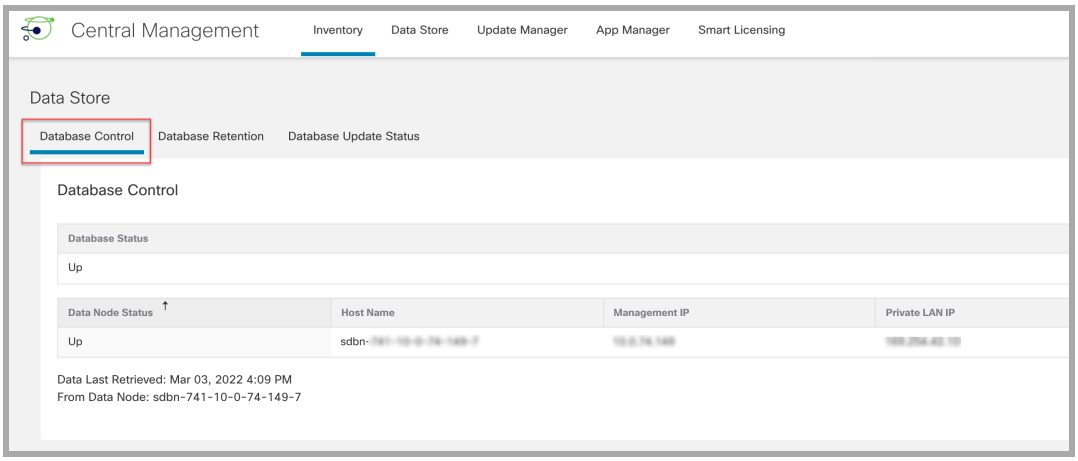
1. 매니저다음에 로그인합니다.
2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
3. **데이터스토어** 탭을 클릭합니다.

데이터스토어 데이터베이스 상태 보기

Central Management에서 데이터스토어 탭을 클릭하면 데이터베이스 제어 페이지가 열립니다. 이 탭에는 데이터베이스 및 각 데이터 노드의 상태가 표시됩니다.

- **정렬:** 이 탭에 있는 데이터 노드은 기본적으로 개인 LAN IP를 기준으로 정렬됩니다. 정렬할 열 헤더를 클릭하여 데이터 노드 노드를 다시 정렬할 수 있습니다.
- **상태:** 정상 상태에서는 데이터베이스 및 모든 데이터 노드가 **Up(작동)** 상태로 표시됩니다. 데이터베이스는 작동 중일 수 있지만 데이터 노드 중 하나의 상태는 중단일 수 있습니다. 실패한 데이터 노드를 복구한 후 데이터베이스가 Up(작동)으로 표시될 수 있지만 새로 복구된 데이터 노드는 "복구 중" 상태가 됩니다.

- **작업 메뉴:** 작업 메뉴를 사용하여 데이터베이스(또는 데이터 노드)를 시작하거나 중지해야 합니다.



작업 메뉴를 사용하여 데이터베이스(또는 데이터 노드)를 시작하거나 중지합니다.

데이터베이스 시작

1. 데이터베이스 제어 탭이 선택되어 있는지 확인합니다.
2. 데이터베이스의 작업 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **Start(시작)**를 선택합니다.
4. 데이터베이스 상태가 Up(작동)으로 표시되는지 확인합니다.

데이터베이스 중지

1. 데이터베이스 제어 탭이 선택되어 있는지 확인합니다.
2. 데이터베이스의 작업 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **Stop(중지)**을 선택합니다.
4. 데이터베이스 상태가 Down(중단)으로 표시되는지 확인합니다.

시작 데이터 노드

데이터 노드를 시작하려면 아래 단계를 수행합니다.

1. 데이터베이스 제어 탭이 선택되어 있는지 확인합니다.
2. 시작할 데이터 노드를 찾습니다. Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **Start(시작)**를 클릭하여 데이터 노드를 시작합니다.
4. 데이터 노드 상태가 Up(작동)으로 표시되는지 확인합니다.

중지 데이터 노드

데이터 노드를 중지하려면 아래 단계를 수행합니다.

1. 데이터베이스 제어 탭이 선택되어 있는지 확인합니다.
2. 중지할 데이터 노드를 찾습니다. Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
3. **Stop(중지)**을 선택하여 데이터 노드를 중지합니다.
4. 데이터 노드 상태가 Down(중단)으로 표시되는지 확인합니다.

마지막 작업 결과 검토

사용자 수에 관계없이 한 번에 하나의 작업만 진행할 수 있습니다. 작업이 진행 중인 경우, 다른 작업을 수행할 수 없습니다. 작업이 완료되면 화면 상단의 배너에 모든 사용자의 완료 상태가 표시됩니다. 아래 단계에 따라 마지막 작업 결과를 검토합니다.

1. 데이터베이스 제어 탭이 선택되어 있는지 확인합니다.
2. 화면 하단의 **Last Action Results(마지막 작업 결과)** 링크를 클릭합니다. Action Results (작업 결과) 배너는 해제할 때까지 화면에 남아 있습니다.

데이터베이스 보존 보기

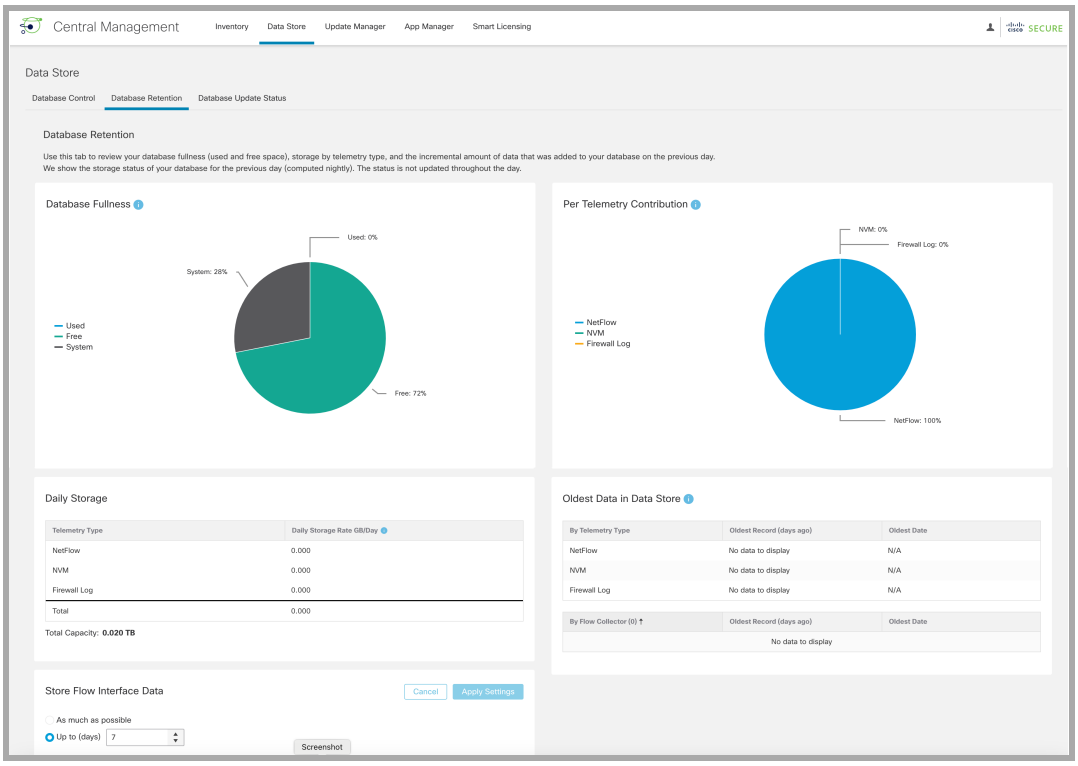
데이터베이스 보존 탭에서는 다음과 같은 질문에 대한 답변을 제공합니다.

- 데이터베이스가 얼마나 가득 찼습니까?
- 이 충족에 기여하는 각 텔레메트리 유형(NetFlow, NVM, 방화벽 로그)은 얼마나 됩니까?
- 어제 데이터베이스에 새로 저장된 데이터의 양은 얼마나 됩니까?
- 데이터베이스의 총 용량은 얼마입니까?

> 이 페이지의 데이터 스토리지 통계 섹션과 모든 차트는 하루에 한 번씩 업데이트됩니다.

데이터 저장소 열기 - 데이터베이스 보존 탭

1. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
2. **데이터스토어** 탭을 클릭합니다.
3. **Database Retention(데이터베이스 보존)** 탭을 클릭합니다.



데이터베이스 충만도 차트

Database Fullness(데이터베이스 충만도) 차트에는 데이터스토어 데이터베이스에 있는 사용된 공간의 크기와 여유 공간이 표시됩니다.

텔레메트리 기여도별 차트

텔레메트리 기여도별 차트에는 데이터스토어 데이터베이스에 있는 데이터에 대한 분석이 표시됩니다.

일일 스토리지

일일 스토리지 섹션에는 전일에 데이터베이스에 추가된 데이터의 증분 양이 표시됩니다. 일일 저장 속도를 모니터링하여 데이터베이스가 얼마나 빨리 채워지는지, 각 텔레메트리 유형이 일일 저장 용량 누계에 얼마나 기여하는지 평가할 수 있습니다.

데이터 저장소의 가장 오래된 데이터

이 표는 가장 오래된 기록이 데이터 저장소에 기록된 이후의 날짜와 일수를 보여줍니다. 이 데이터는 하루에 한 번 업데이트됩니다.

플로우 컬렉터(또는 플로우 컬렉터 데이터베이스)에 로컬로 저장된 데이터는 이 표에 포함되지 않습니다. 비데이터 저장소 흐름 컬렉터를 데이터 저장소 흐름 컬렉터로 전환하고 데이터 보존 정책이 있는 경우, 이 표를 사용하여 데이터 저장소에 새 데이터가 있는 양과 데이터 저장소에 전환을 완료하기에 이상적인 시기를 파악할 수 있습니다.

플로우 인터페이스 데이터 스토리지 변경

플로우 인터페이스 통계에서는 플로우 통계를 더욱 자세히 볼 수 있습니다. 이들은 지정된 플로우에 대해 네트워크에서 여러 밴디지 포인트를 제공하여 최근 플로우 데이터를 조사하고 문제를 해결하는 데 유용합니다. 예를 들어 플로우가 여러 엑스포터 또는 동일한 엑스포터의 여러 인터페이스에서 관찰되면 플로우 인터페이스 통계에 세부 정보가 저장됩니다.

데이터스토어는 데이터를 최대한 오랫동안 보존하며, 보존 시간은 시스템의 수집 속도에 따라 결정됩니다. 데이터스토어가 전체 용량에 도달하면 가장 오래된 데이터를 자동으로 삭제하기 시작합니다.

플로우 인터페이스 통계는 더 빠른 속도로 스토리지를 사용하므로, 다른 중요한 데이터(예: 플로우 통계)를 보존할 수 있는 시간이 단축될 수 있습니다.

> 여기서 플로우 인터페이스 데이터 스토리지 기간을 변경하면 시스템에서 공간을 차지하는 데이터의 NetFlow 부분에만 영향을 미칩니다. 기본값은 7일입니다. 필요에 따라 보존 일수를 늘리거나 줄일 수 있습니다.

1. 스토어 플로우 인터페이스 데이터 섹션에서 **가능한 한 많이** 또는 **최대 일수**를 선택합니다(위쪽 또는 아래쪽 화살표를 클릭하여 일수 변경).
2. **설정 적용**을 클릭합니다.

   - 보존을 더 긴 기간으로 변경하는 경우, 차이나는 시간만큼 기다려서 저장되는 데이터가 보존 설정에 정확하게 일치하게 됩니다. 그 때까지 데이터는 가장 낮은 해상도(가장 거침)로 표시됩니다. 예를 들어 보존 기간을 3일에서 10일로 변경하면 저장되는 데이터가 보존 설정에 정확히 일치하게 될 때까지 7일을 기다려야 합니다.
   - 디스크 사용량에 따라 데이터가 중요한 곳에서 잘리므로, 선택한 보존 기간보다 빨리 데이터가 삭제될 수 있습니다. 가능한 한 오랫동안 데이터를 저장하도록 선택하는 경우 데이터스토어이 전체 용량에 도달하면 가장 오래된 데이터부터 삭제합니다.

데이터 노드 업데이트 상태 모니터링

Central Management 업데이트 관리자에서 데이터 노드의 업데이트를 시작한 후 데이터베이스 업데이트 상태 탭을 사용하여 각 데이터 노드의 데이터베이스 서비스 업데이트 진행 상황을 모니터링합니다.

데이터 저장소 열기 - 데이터베이스 업데이트 상태 탭

1. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
2. **데이터스토어** 탭을 클릭합니다.
3. **데이터베이스 업데이트 상태** 탭을 클릭합니다.

데이터베이스 업데이트 상태 모니터링

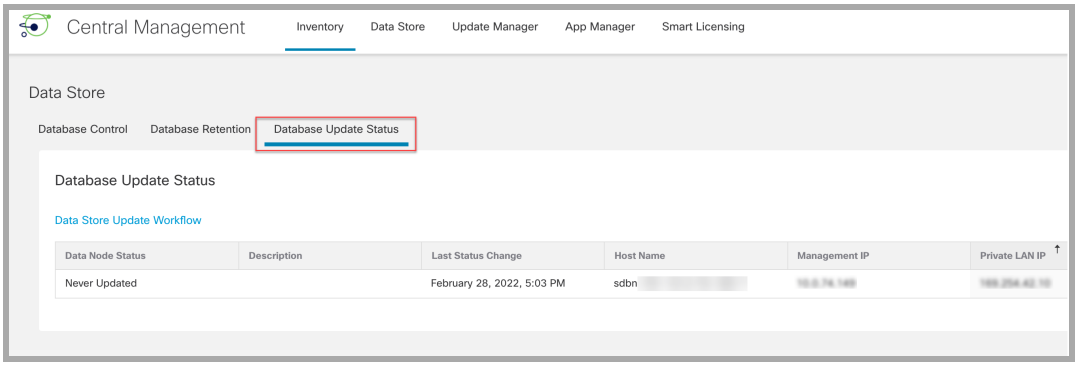
각 는데이터 노드 업데이트 중에 일련의 상태를 통해 진행됩니다. 업데이트 프로세스의 시각적 표현을 보려면 데이터 저장소 업데이트 워크플로우 링크를 클릭합니다(아래 표시).

업데이트에 성공하려면 Cisco Secure Network Analytics시스템 업데이트 가이드의 업데이트 순서와 지침을 따르십시오.

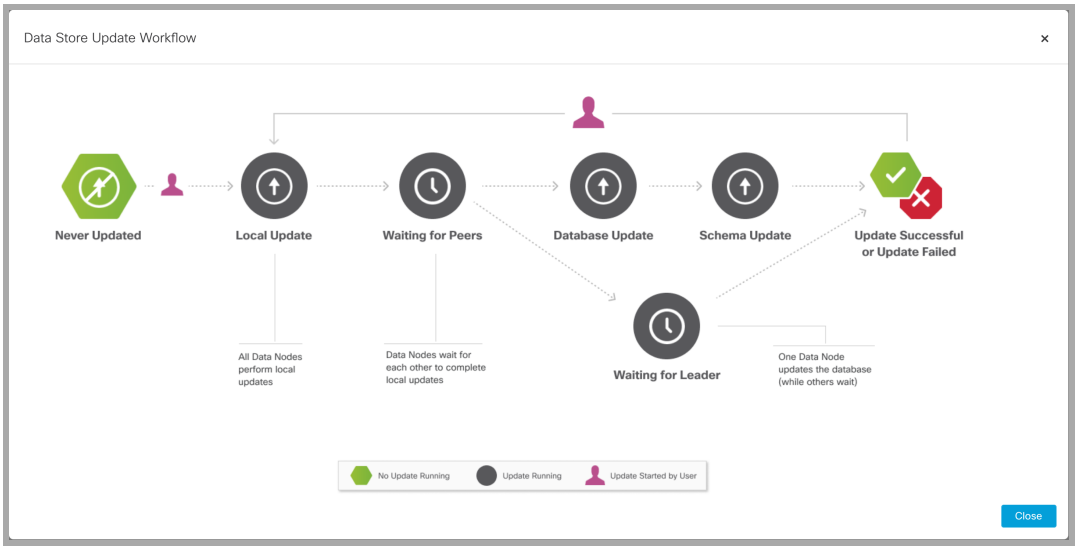
아래 이미지에 표시된 상태 전환 중 일부는 업데이트 과정 중에 매우 빠르게 발생하므로 화면을 새로 고침하는 동안에는 발생하는 것을 확인할 수 없습니다.

데이터베이스 업데이트 상태 탭에는 데이터 노드의 현재 업데이트 상태가 표시됩니다. 업데이트 매니저에서 소프트웨어 업데이트(업그레이드 또는 패치)를 시작한 후 이 데이터베이스 업데이트 탭을 사용하여 각 데이터 노드의 상태를 모니터링하여 업데이트가 완료되었는지 확인합니다. 업데이트 워크플로우를 시각적으로 보려면 **View Diagram(뷰 다이어그램)**을 클릭합니다.

업데이트가 완료되면 **데이터 저장소 데이터베이스**으로 이동하여 데이터베이스 상태가 Up(작동)인지 확인합니다. 추가 정보는 업데이트 가이드를 참조하십시오.



다음 이미지는 데이터스토어 업데이트 워크플로우를 보여줍니다.



데이터스토어 백업 생성

> 이러한 작업을 계획하고 구현하는 데 도움이 필요하면 Cisco 전문 서비스팀에 문의하십시오.

데이터스토어를 백업하려면 다음 절차를 완료하십시오.

1. **백업 호스트 스토리지 요구 사항 추정**
2. **백업 호스트 준비**를 준비합니다. 백업 호스트에 Python v3.7 및 rsync v3.0.5를 설치합니다.

> Secure Network Analytics 어플라이언스와 별도의 Linux 기반 호스트를 사용하십시오.

3. **dbadmin에 대한 비밀번호 없는 SSH 액세스 활성화**에 대해 비밀번호 없는 SSH 액세스를 활성화합니다. 모든 데이터 노드가 비밀번호 없는 SSH 액세스를 사용하여 백업 호스트에 연결할 수 있는지 확인합니다.
4. **백업 호스트에서 백업 디렉토리 초기화**
5. **데이터스토어 데이터베이스**

1. 백업 호스트 스토리지 요구 사항 추정

1. 데이터 노드콘솔에 `root`로 로그인합니다.
2. 다음 명령을 복사하여 명령줄에 붙여넣은 다음 Enter를 눌러 vSQL을 사용하는 데이터베이스에 연결하고 쿼리를 실행합니다. 프롬프트에서 비밀번호를 입력합니다. 결과를 참고하십시오.

```
/opt/vertica/bin/vSQL -U dbadmin -c "SELECT SUM(used_bytes) FROM
storage_containers;"
```

3. 이 합계에 2를 곱하여 백업 호스트에 필요한 스토리지 공간의 양을 추정합니다.

2. 백업 호스트 준비

1. **1. 백업 호스트 스토리지 요구 사항 추정**을 추정하고, 네트워크에서 Linux를 실행하는 호스트를 식별하여 백업을 저장하거나, 필요한 스토리지 요구 사항을 갖춘 Linux를 실행하는 호스트를 구축합니다.

> Secure Network Analytics 어플라이언스와 별도의 Linux 기반 호스트를 사용하십시오.

2. 백업 호스트 콘솔에 `root`로 로그인합니다.
3. 명령 프롬프트에서 `python3 --version`을 입력하고 Enter를 눌러 설치된 Python 버전을 확인합니다. 다음과 같은 옵션이 있습니다.

   - Python 3.7 이상이 설치된 경우 6단계로 이동합니다.
   - 그렇지 않은 경우 4단계부터 Python 3.7을 설치합니다.

4. `sudo apt-get update`를 입력하고 Enter를 눌러 Python을 비롯한 업데이트된 패키지 버전을 다운로드합니다. 프롬프트에서 비밀번호를 입력합니다.
5. `sudo apt-get install python3.7`을 입력하고 Enter를 눌러 Python 3.7을 설치합니다(다른 버전을 설치하려면 명령 수정).
6. 명령 프롬프트에서 `rsync --version`을 입력하고 Enter를 눌러 설치된 rsync의 버전을 확인합니다. 다음과 같은 옵션이 있습니다.

   - rsync 3.0.5 이상이 설치된 경우 9단계로 계속합니다.
   - 그렇지 않으면, rsync 3.0.5를 설치합니다. 7단계로 진행합니다.

7. `sudo apt-get update`를 입력하고 Enter를 눌러 rsync를 포함한 패키지의 업데이트된 버전을 다운로드합니다. 프롬프트에서 비밀번호를 입력합니다.
8. `udo apt-get install rsync`를 입력하고 Enter를 눌러 rsync를 설치합니다.
9. 명령 프롬프트에서 `getent passwd | grep dbadmin`을 입력하고 Enter를 눌러 이 호스트에 `dbadmin` 사용자 어카운트가 있는지 확인합니다. 다음과 같은 옵션이 있습니다.

   - `dbadmin` 사용자 계정이 있으면 백업 호스트가 준비된 것입니다. **3. dbadmin에 대한 비밀번호 없는 SSH 액세스 활성화**에 대한 비밀번호 없는 SSH 액세스 활성화
   - 그렇지 않으면 이 호스트에서 `dbadmin` 사용자 계정을 생성합니다. 10단계로 진행합니다.

10. 명령 프롬프트에서 `adduser dbadmin`을 입력하고 Enter를 눌러 `dbadmin` 사용자 어카운트를 생성합니다.
11. `passwd dbadmin`을 입력하고 Enter를 눌러 `dbadmin`에 비밀번호를 할당합니다.
12. **New password(새 비밀번호)**를 입력하고 Enter를 눌러 `dbadmin` 비밀번호를 설정합니다. 프롬프트에서 비밀번호를 확인합니다.

3. dbadmin에 대한 비밀번호 없는 SSH 액세스 활성화

1. SSH의 경우 백업 호스트와 각 데이터 노드 간에 포트 22/TCP를 열고, rsync의 경우 백업 호스트와 각 데이터 노드간에 포트 50000/TCP를 엽니다.
2. 자세한 내용은 `ssh-copy-id dbadmin@<hostname>`에서 OpenSSH 문서를 참조하십시오.
3. 다음을 입력하여 `dbadmin`으로 먼저 데이터 노드에 로그인합니다.

   ```
   su dbadmin
   ```

4. 다음 명령을 복사하여 일반 텍스트 편집기에 붙여넣습니다.

   `ssh-copy-id dbadmin@[hostname]` 여기서 `[hostname]`은 백업 호스트의 호스트 이름 또는 IP 주소입니다.

5. 업데이트된 명령을 복사하여 명령 프롬프트에 붙여넣은 다음 Enter를 눌러 `dbadmin` SSH 인증 키를 백업 호스트에 복사합니다.
6. 다음 명령을 복사하여 일반 텍스트 편집기에 붙여넣습니다.

   `ssh 'dbadmin@[hostname]'` 여기서 `[hostname]`은 백업 호스트의 호스트 이름 또는 IP 주소입니다.

7. 업데이트된 명령을 복사하여 명령 프롬프트에 붙여넣은 다음 Enter를 눌러 이 데이터 노드에서 비밀번호 없이 SSH를 통해 원격 호스트의 콘솔에 로그인할 수 있는지 확인합니다.

4. 백업 호스트에서 백업 디렉토리 초기화

1. 먼저 데이터 노드 콘솔에 `root`로 로그인합니다.

> 백업 디렉토리를 초기화할 때 사용하는 데이터 노드를 참고십시오. 동일한 데이터 노드를 사용하여 이후 절차(**5. 데이터스토어 데이터베이스** 백업).

2. `su - dbadmin`을 입력하고 Enter를 눌러 `dbadmin` 사용자로 다음 명령을 실행합니다.
3. `ssh [backup-host]`를 입력합니다. 여기서 [backup host]는 백업 서버의 호스트 이름 또는 IP 주소입니다. 이렇게 하면 비밀번호를 입력하라는 메시지가 표시되지 않고 백업 호스트의 인터페이스에 `dbadmin`으로 로그인할 수 있어야 합니다. 백업 호스트에서 비밀번호를 입력하라는 메시지가 표시되면 설정을 확인합니다.
4. `cd /home/dbadmin`을 입력하고 Enter를 눌러 디렉토리를 변경합니다.
5. `mkdir backups`를 입력하고 Enter를 눌러 백업 디렉토리를 만듭니다.
6. `exit`를 입력하고 Enter를 눌러 데이터 노드의 명령줄 프롬프트로 돌아갑니다.
7. `vi pw.ini`를 입력하고 Enter를 눌러 `pw.ini` 백업 비밀번호 파일을 만들고 편집합니다.

> setup-sw-datastore-secure-connectivity 스크립트를 사용하여 dbadmin 비밀번호를 업데이트한 경우 pw.ini 백업 비밀번호 파일에 저장된 비밀번호도 업데이트해야 합니다. 그렇지 않으면 백업에 실패합니다.

8. 다음 줄을 일반 텍스트 편집기에 복사합니다.

```
[Passwords]
dbPassword = [dbadmin-password]
```

9. `[dbadmin-password]`를 데이터스토어 `dbadmin` 비밀번호로 업데이트합니다.
10. 업데이트된 줄을 복사하여 `pw.ini` 패스워드 백업 파일에 붙여넣습니다.

11. Esc를 누르고 `:wq`를 입력하고 Enter를 눌러 변경 사항을 저장하고 종료합니다.
12. `chmod 640 pw.ini`를 입력하고 Enter를 눌러 `dbadmin` 사용자가 파일을 읽고 수정할 수 있도록 `pw.ini` 파일 권한을 변경합니다.
13. 다음 줄을 복사하여 일반 텍스트 편집기에 붙여넣습니다.

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1

[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

14. `vi config.ini`를 입력하고 Enter를 눌러 `config.ini` 백업 구성 파일을 만들고 편집합니다.
15. 15단계에서 일반 텍스트 편집기에 붙여넣은 텍스트를 복사하여 `config.ini` 파일에 붙여 넣습니다.
16. *backup-host-ip*는 백업 호스트의 IP 주소로 바꿉니다.
17. `[Mapping]`(매핑) 아래의 호스트 이름이 데이터 노드와 일치하지 않는 경우 해당 호스트 이름을 업데이트합니다. 데이터 노드 노드 이름을 결정하려면 다음을 수행합니다.

    - 아무 데이터 노드 콘솔에 `root`로 연결합니다.
        - `su dbadmin`을 입력합니다.
        - `admintools -t node_map`을 입력합니다.
    - `[Mapping(매핑)]` 항목에 대해 "NODENAME" 열에 노드 이름을 사용합니다.

    예:

```
dbadmin@sdBN-742-10-0-56-133-5:/root$ admintools -t node_map
데이터베이스     | 노드이름                | 호스트이름
-------------------------------------------------------
sw          | v_sw_node0001           | 169.254.42.10
```

```
sw          | v_sw_node0002          | 169.254.42.12
sw          | v_sw_node0003          | 169.254.42.15
```

18. 환경에 3개 이상을 구축한 경우 각 데이터 노드에 대한 항목이 있어야 합니다. 단일 데이터 노드만 있는 경우 단일 데이터 노드에 하나의 라인만 남겨두고 추가 `[Mapping]` 라인을 제거합니다.
19. Esc를 누르고 `:wq`를 입력하고 Enter를 눌러 변경 사항을 저장하고 종료합니다.
20. `vbr -t init -c config.ini`를 입력하고 Enter를 눌러 데이터스토어 백업을 수신하도록 백업 호스트의 `/home/dbadmin/backup` 디렉토리를 초기화합니다.

5. 데이터스토어 데이터베이스 백업

> 전체 다중 노드 데이터베이스를 백업하려면 하나의 데이터 노드에서 backup 명령을 실행하면 됩니다.

1. **4. 백업 호스트에서 백업 디렉토리 초기화**에서 백업 디렉토리 초기화
2. `su - dbadmin`을 입력하고 Enter를 눌러 `dbadmin` 사용자로 다음 명령을 실행합니다.
3. `vbr -t backup -c config.ini --debug 3 --dry-run`을 입력하고 Enter를 눌러 백업을 생성하지 않은 채 백업 테스트를 수행합니다. 다음 옵션을 이용할 수 있습니다.
   - 백업 테스트가 성공적으로 해결되면 데이터스토어을 백업하고 4단계로 진행합니다.
   - 백업 테스트에서 장애가 발생하면 스냅샷 파일이 생성된 것일 수 있으므로 제거해야 합니다. 제거 지침은 데이터 저장소 백업 실패를 참조하십시오. 백업 테스트를 해결하지 못하면 `/tmp/vbr` 디렉토리의 디버그 로그 파일을 검토하고 근본 원인을 해결한 다음 백업을 다시 테스트합니다. 도움이 더 필요하면 Cisco 지원팀에 문의해 주십시오.
4. `vbr -t backup -c config.ini`를 입력하고 Enter를 눌러 백업 호스트의 `/home/dbadmin/backup` 디렉토리에 데이터스토어를 백업합니다.

데이터스토어 백업 실패

데이터스토어 백업에 실패하는 경우 다른 백업을 시도하기 전에 데이터베이스 스냅샷을 제거하십시오. 데이터스토어 데이터베이스 스냅샷을 제거하려면 다음 단계를 수행합니다.

1. **vSQL**을 사용하여 데이터스토어 데이터베이스 클러스터에 연결합니다.
2. 다음 명령을 실행하여 스냅샷 목록을 검색합니다.

   ```
   select * from database_snapshots;
   ```

3. 제거할 스냅샷의 이름으로 'snapshot_name'을 대체하고 다음 명령을 실행합니다.

   ```
   select remove_database_snapshot('snapshot_name');
   ```

4. 다음 명령을 실행하여 종료합니다.

```
\q
```

데이터스토어 백업 복원

> 이러한 작업을 계획하고 구현하는 데 도움이 필요하면 Cisco 전문 서비스팀에 문의하십시오.

데이터스토어를 백업하려면 다음 절차를 완료하십시오.

1. **백업 이름 및 소프트웨어 버전 검토**
2. **데이터스토어 데이터베이스**
3. **백업에서 데이터스토어 복원**
4. **시작 데이터스토어**
5. **카탈로그 스냅샷 제거**
6. **복구된 데이터베이스 검토**

> 데이터스토어 백업을 가져온 동일한 데이터스토어에만 백업을 복원할 수 있습니다. 한 데이터스토어에서 백업을 만든 다음 다른 데이터스토어로 복원할 수는 없습니다. 데이터스토어 백업을 생성할 경우 아무 데이터 노드를 사용하여 backup 명령을 실행합니다. 데이터스토어 백업을 복원할 때는 restore 명령을 실행하기 위해 아무 데이터 노드를 사용합니다(백업 생성에 사용한 데이터 노드과 동일할 필요는 없음).

1. 백업 이름 및 소프트웨어 버전 검토

1. 데이터스토어 데이터베이스 백업을 확인하고 데이터스토어가 데이터 노드와 동일한 데이터 노드이름과 번호를 가지고 있는지 확인합니다.
2. 데이터스토어 데이터베이스 백업을 확인하고 데이터스토어가 설치된 Secure Network Analytics과 동일한 버전인지 확인합니다.

> 백업 버전과 다른 버전으로 데이터베이스를 복원하는 것은 지원되지 않습니다.

2. 데이터스토어 데이터베이스

중지

1. 매니저다음에 로그인합니다.
2. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
3. **데이터스토어** 탭을 클릭합니다.
4. 데이터베이스를 찾습니다.
5. Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
6. **Stop(중지)**을 선택합니다.
7. 데이터스토어 데이터베이스 제어 탭을 열린 상태로 유지합니다. 이후 절차에서 이를 사용합니다.

3. 백업에서 데이터스토어 복원

> 비교를 위해 데이터베이스가 복원되기 전과 이후에 다음 명령을 실행해야 합니다.
> `/opt/vertica/bin/vsql -U dbadmin -w <'password'> -c "select* from partitions;" >/lancope/var/tcpdump/partitions-full-DBbackup`

1. `setup-sw-datastore-secure-connectivity` 스크립트를 사용하여 `dbadmin` 비밀번호를 업데이트한 경우 `pw.ini` 백업 비밀번호 파일에 저장된 비밀번호도 업데이트해야 합니다. 그렇지 않으면 복원에 실패합니다.
2. `config.ini` 백업 구성 파일을 저장한 데이터 노드를 확인하고 해당 콘솔에 `root`로 로그인합니다. 자세한 내용은 **4. 백업 호스트에서 백업 디렉토리 초기화**를 참조하십시오.
3. `su - dbadmin`을 입력하고 Enter를 눌러 `dbadmin` 사용자로 다음 명령을 실행합니다.
4. 명령 프롬프트에서 vbr --task restore --config-file config.ini를 입력하고 Enter를 눌러 백업 호스트에서 를 복원합니다.데이터스토어

> 전체 다중 노드 데이터베이스를 복원하려면 하나 데이터 노드에서 restore 명령만 실행하면 됩니다.

4. 시작 데이터스토어

1. Central Management의 데이터베이스 제어 탭으로 돌아갑니다.데이터스토어
2. 데이터베이스를 찾습니다.
3. Actions(작업) 열에서 ••• (**줄임표**) 아이콘를 클릭합니다.
4. **Start(시작)**를 선택합니다.

5. 카탈로그 스냅샷 제거

데이터스토어를 재시작한 후 카탈로그라는 이름의 스냅샷을 제거합니다. 복원이 해결된 후에는 이 스냅샷이 필요하지 않으며, 이렇게 하면 Vertica에서 보존 관리가 실행되지 않습니다.

1. 데이터 노드 콘솔에 `root`로 로그인합니다.
2. `su - dbadmin`을 입력하고 Enter를 눌러 `dbadmin` 사용자로 다음 명령을 실행합니다.
3. 다음 명령을 입력하여 `[password]`를 `dbadmin` password로 교체한 다음 Enter 키를 누릅니다. 이렇게 하면 카탈로그 스냅샷이 제거됩니다.

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select
   remove_database_snapshot('catalog');"
   ```

6. 복구된 데이터베이스 검토

> 비교를 위해 데이터베이스가 복원되기 전과 이후에 다음 명령을 실행해야 합니다.
> `/opt/vertica/bin/vSQL -U dbadmin -w<password> -c "select*`

```
frompartitions;" /lancope/var/tcpdump/partitions-full-
DBbackup
```

데이터 저장소 유지 관리

이 섹션에서는 다음 데이터스토어 주제를 다룹니다.

- **데이터 저장소에서 데이터 압축 활성화**
- **데이터 저장소 도메인 추가**
- **데이터스토어가 초기화된 뒤에 보조 매니저 또는 플로우 컬렉터 추가**
- **데이터 노드를 데이터스토어**
- **데이터 노드 교체(하드웨어만 해당)**

> 시작하기 전에 절차를 검토하십시오. 일부 절차에는 Cisco 지원팀에 지원을 요청하는 방법이 포함됩니다.

데이터 저장소에서 데이터 압축 활성화

데이터 압축은 데이터스토어으로 구성된 플로우 컬렉터의 신규 설치에서 기본적으로 활성화됩니다. 이를 사용하여 플로우 컬렉터와 데이터 저장소 간의 대역폭 사용량을 줄일 수 있습니다. 이는 플로우 컬렉터에서 데이터 저장소로의 네트워크 대역폭이 제한된 시나리오에 특히 유용합니다.

압축을 활성화하면 이 대역폭을 최대 90%까지 줄일 수 있습니다. 데이터 압축이 비활성화된 경우 플로우 컬렉터별로 활성화할 수 있습니다. 플로우 컬렉터 인터페이스에서 다음과 같이 구성을 변경하여 데이터스토어로 전송되는 데이터의 압축을 활성화합니다.

1. 플로우 컬렉터 어플라이언스 관리 인터페이스에 로그인합니다.
2. **Support(지원) > Advanced Settings(고급 설정)**을 클릭합니다.
3. ingest_enable_compression 필드에서 다음 중 하나를 입력합니다.

   - 1 - 데이터 압축 활성화
   - 0 - 데이터 압축 비활성화

4. 정보 창에서 **Apply(적용)**를 클릭한 다음 **OK(확인)**를 클릭합니다.

이 페이지의 많은 설정은 잘못 설정할 경우 성능에 부정적인 영향을 줄 수 있지만 데이터 압축을 활성화하면 플로우 컬렉터와 데이터 저장소 간 데이터 전송과 관련하여 시스템 성능을 향상시키기만 합니다.

데이터 저장소 도메인 추가

이 섹션에 표시된 대로 기존 데이터스토어 도메인에 매니저, 플로우 컬렉터, 데이터 노드를 추가할 수 있습니다. 구축에 데이터 저장소 도메인이 없는 경우, **비데이터 저장소 구축에 데이터 저장소 추가**의 지침을 따르십시오.

데이터스토어가 초기화된 뒤에 보조 매니저 또는 플로우 컬렉터 추가

데이터 저장소를 이미 초기화한 경우 다음 지침에 따라 보조 매니저 또는 플로우 컬렉터를 데이터 저장소에 추가하십시오.

보조 매니저 및 페일오버 구성에 대한 자세한 내용은 **3. 매니저 페일오버 관계**

데이터스토어 없이 사용하도록 구성한 기존 플로우 컬렉터가 있는 경우, **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**의 지침에 따라 전환 전 데이터 또는 가시성의 손실 없이 데이터스토어 플로우 컬렉터으로 전환할 수 있습니다.

데이터 노드를 데이터스토어에 추가

> 이러한 작업을 계획하고 구현하는 데 도움이 필요하면 Cisco 전문 서비스팀에 문의하십시오.

요구 사항

데이터 노드을 데이터스토어에 추가하기 전에 다음 요구 사항을 검토합니다.

- 데이터 저장소는 1개 또는 3개 이상의 데이터 노드를 지원합니다. 데이터 노드를 3개 세트로 추가할 수 있습니다.
- 단일 데이터 노드(1)을 구축한 경우, 2개의 데이터 노드를 추가하여 3개 데이터 노드 세트(및 3개의 추가 노드)로 구축을 확장할 수 있습니다.
- 데이터 노드가 2개인 데이터 저장소는 지원하지 않습니다.

시작하기 전에

데이터스토어를 확장할 때 유지 관리 창을 사용하는 것을 고려할 수 있습니다.

데이터스토어를 확장하기 전에 모든 데이터가 데이터 노드에 균등하게 분산됩니다. 예를 들어, 3개의 노드 데이터스토어에서 데이터의 1/3이 각 데이터 노드에 있습니다. 데이터스토어를 확장하면 모든 데이터가 새로 추가된 노드에 균등하게 재배포됩니다. 예를 들어 3노드 데이터 저장소를 총 6개 노드로 확장하는 경우, 각 데이터 노드에 데이터가 1/6씩 재분배됩니다. 단일 노드 데이터스토어를 3개 노드로 확장할 경우 데이터는 각 노드에 1/3씩 재배포됩니다.

데이터 재배포 작업 중에 데이터스토어의 쿼리 성능이 일시적으로 저하될 수 있습니다. 영향 정도 및 지속 시간은 이동해야 하는 데이터의 양 및 데이터 노드 사이의 사설 LAN의 대역폭과 관련이 있습니다. 예를 들어 포트 결합이 있는 데이터스토어 하드웨어는 20GB의 사설 LAN 대역폭을 사용하여 데이터를 이동할 수 있습니다. 데이터베이스는 데이터 재배포 중에도 계속 작동하지만 사용자에 대한 영향을 최소화하려면 유지 관리 기간을 지정하는 것이 좋습니다.

절차

구축에 데이터 노드을 추가하려면 다음 절차를 완료하십시오.

1. 데이터스토어 백업 생성

데이터 노드를 추가하기 전에 데이터스토어를 백업합니다. 자세한 지침은 **데이터스토어 백업 생성**을 참조하십시오.

2. 데이터 노드를 설정하고 Central Management에 추가

1. 네트워크에 데이터 노드를 구축합니다. 지침은 x2xx Series 하드웨어 어플라이언스 설치 가이드, Secure Network Analyticsx3xx Series 하드웨어 설치 가이드 또는 Virtual Edition 어플라이언스 설치 가이드를 참조하십시오.

> 설치 중에 네트워크 어댑터가 2개인 데이터 노드 Virtual Edition을 할당해야 합니다. 최초 설정을 시작할 때 두 번째 네트워크 어댑터를 감지하지 못하면 이 문제를 해결하지 못하며, 이로 인해 상호 데이터 노드 통신을 위해 라우팅할 수 없는 IP 주소를 할당할 수 없습니다.

2. 최초 설정에서 데이터 노드를 구성합니다. 이 절차에서는 라우팅 가능(eth0) 관리 IP 주소를 할당하고 상호 데이터 노드 통신을 구성합니다.
3. 어플라이언스 설정 도구를 사용하여 Central Management에 데이터 노드를 추가합니다.

3. 데이터스토어
에 데이터 노드 추가

1. 매니저 어플라이언스 콘솔에 root로 로그인합니다.
2. `SystemConfig`를 입력하고 Enter를 누릅니다.
3. **데이터스토어**을(를) 선택합니다.
4. **SSH**를 선택합니다. 어플라이언스 전체에서 SSH가 활성화되는 동안 기다립니다.
5. **데이터스토어** 메뉴에서 **새 데이터 노드를 선택합니다**. 화면의 프롬프트를 따르십시오.

    - 프로세스가 완료되면 Central Management에서 어플라이언스 상태가 Connected (연결됨)인지 확인합니다.
    - 데이터스토어 메뉴를 종료하면 이전 SSH 설정이 복원됩니다.

4. 데이터 재조정 데이터스토어

> 데이터 저장소에 데이터 노드를 추가한 후에는 재조정이 필요합니다. 이 프로세스에 대한 지원이 필요하면 시스코 지원에 문의하십시오.

데이터 노드 교체(하드웨어만 해당)

다음 지침에 따라 다음 시나리오에 대해 새 (예비) 데이터 노드을 준비합니다.

- 데이터 노드를 IP 주소가 다른 예비 데이터 노드로 교체
- 응답하지 않는 교체 데이터 노드
- 기존 데이터 노드가 다운된 후 예비 데이터 노드 추가

모든 시나리오에서 새(예비) 데이터 노드를 준비하고 Cisco 지원팀과 협력하여 교체를 완료합니다.

> 이러한 작업을 계획하고 구현하는 데 도움이 필요하면 Cisco 전문 서비스팀에 문의하십시오.

1. 새(예비) 준비 데이터 노드

1. 기존 데이터 노드 어플라이언스와 동일한 랙 설정에 새(예비) 데이터 노드 어플라이언스를 설치합니다. 설치 지침은 x2xx Series 하드웨어 어플라이언스 설치 가이드 또는 Secure Network Analyticsx3xx Series 하드웨어 설치 가이드를 참조하십시오.

   다음을 확인합니다.

   - 새 데이터 노드가 동일한 스위치/포트에 연결되어 있는지 확인합니다.
   - 새 데이터 노드가 기존 데이터 노드에 있는 개인 및 공공 인터페이스와 같은 VLAN에 있는지 확인합니다.

2. 데이터 노드를 전원에 연결하고 전원을 켭니다.
3. 기존 데이터 노드에서 이미 실행 중인 이미지와 일치하도록 새 데이터 노드에서 이미지를 업그레이드합니다. Cisco 지원팀에 도움을 요청하십시오.
4. 최초 설정에서 데이터 노드를 구성합니다. 적절한 eth0 관리 IP 및 개인 IP 주소를 할당하고 기존 데이터 노드 eth0 및 개인 IP와 동일한 VLAN에 있는지 확인합니다.
5. 다음 단계를 수행하여 전체 연결을 확인합니다.

   - 매니저 및 모든 플로우 컬렉터에서 새 데이터 노드의 eth0 IP 주소로 ping을 실행합니다.
   - 모든 기존 데이터 노드에서 새 데이터 노드의 개인 IP로 ping을 실행합니다.
   - 새 데이터 노드에서 매니저 및 모든 플로우 컬렉터의 eth0 관리 IP로 ping을 실행합니다.
   - 새 데이터 노드에서 모든 기존 데이터 노드의 개인 IP로 ping을 실행합니다.

2. 데이터스토어 백업 생성

자세한 지침은 **데이터스토어 백업 생성**을 참조하십시오.

3. Cisco 지원팀에 문의

Cisco 지원팀에 문의하여 교체를 완료하십시오.

비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터

전환

다음 지침에 따라 비 데이터스토어 플로우 컬렉터를 데이터스토어 플로우 컬렉터로 전환합니다. 이 프로세스를 통해, 전환 전 데이터 또는 가시성의 손실 없이 기존 플로우 컬렉터를 전환하여 데이터스토어 데이터베이스를 사용할 수 있습니다. 아래 단계를 완료하면 기존 데이터가 더 이상 필요하지 않을 때까지 보존할 수 있습니다. 비 데이터스토어 플로우 컬렉터를 데이터스토어 플로우 컬렉터로 전환하면 다음과 같은 데이터스토어에서만 사용 가능한 기능을 활용할 수 있습니다.

- **수집 용량 증가:** 데이터스토어 구축은 초당 최대 3백만 플로우로 확장 가능하며 현재 수집 용량 제한을 일부 완화할 수 있습니다. 데이터스토어에서 플로우 컬렉터의 성능이 최대 200% 향상될 수 있습니다.
- **다중 텔레메트리 지원:** 데이터스토어 구축에서 NetFlow, NVM(원격 작업자/엔드 포인트), 방화벽 연결 및 보안 이벤트 텔레메트리를 처리할 수 있습니다.
- **장기 데이터 보존:** 데이터스토어 구축은 확장 가능한 스토리지를 제공하므로, 플로우 컬렉터을 추가하지 않고도 장기 데이터 보존(최대 2년)이 가능합니다.
- **엔터프라이즈급 데이터 복원력:** 텔레메트리 데이터가 데이터 노드에 이중으로 저장됩니다. 이렇게 하면 단일 노드 장애 시 서비스 중단이 발생하지 않습니다.
- **쿼리 및 보고 응답 시간 대폭 개선:** 데이터스토어는 쿼리 성능 및 보고 응답 시간이 대폭 개선됩니다. 경우에 따라 비 데이터스토어 구축 모델에 비해 10배 이상 빠릅니다.
- **애널리틱스:** 애널리틱스는 추가적인 탐지 및 모델링 기능은 물론 보안 문제를 검토하고 우선순위를 정하고 해결하는 데 사용할 수 있는 새로운 인터페이스 기능을 제공합니다. 애널리틱스에서는 다음과 같은 기능을 제공합니다.
  - 자동화된 역할 탐지
  - 추가 알림 기능
  - 실험적 알림 대시보드
  - 지원 디바이스 보고서
- **SAL 텔레메트리:** SAL(Telemetry: Security Analytics and Logging)은 방화벽(FTD 및 ASA)의 로그를 집계하고 네트워크 활동에 대한 직관적인 보기를 제공하여 의사 결정을 간소화합니다. 재량에 따라 SAL을 확장하여 더 오래 보존 및 분석할 수 있으며, 방화벽에서 발견된 잠재적 위협에 대한 알림도 허용할 수 있습니다.

준비

전환을 시작하기 전에 지침을 검토하여 플로우 컬렉터의 전환에 필요한 준비 및 단계를 파악할 수 있습니다.

다음 사항을 참고하십시오.

- **One at a Time(한 번에 하나씩):** 한 번에 하나의 플로우 컬렉터만 전환을 시작할 수 있습니다. 하지만 여러 플로우 컬렉터가 동시에 전환 상태에 있을 수 있습니다.
- **Query Options(쿼리 옵션):** 플로우 컬렉터이 전환 상태에 들어가면 비데이터 저장소 도메인을 통해 전환을 시작하기 전에 수집한 과거 비데이터데이터스토어와 데이터 저장소 도메인을 통해 전환 후 데이터 저장소에서 수집한 새 데이터를 모두 쿼리할 수 있습니다.

구성 파일 백업

> 플로우 컬렉터 상태(비데이터 저장소, 전환 중 또는 데이터 저장소)를 변경한 후에는 반드시 Central Management 구성 파일을 백업하십시오. 플로우 컬렉터이 백업을 수행했을 때와 동일한 상태인 경우에만 시스템을 복원할 수 있습니다.

플로우 컬렉터 전환 요건

플로우 컬렉터를 전환하기 전에 하나 이상의 데이터 노드를 구축했으며 **6. 초기화 데이터스토어** 아직 데이터 노드을 하나 이상 구축하지 않은 경우, x2xx Series 하드웨어 어플라이언스 설치 가이드, x3xx Series 하드웨어 어플라이언스 설치 가이드 또는 Virtual Edition 어플라이언스 설치 가이드에서 지침을 확인하십시오. 데이터 노드 구축이 끝나면 **플로우 컬렉터를 데이터 저장소로 전환 시작** 절차를 수행할 수 있습니다.

플로우 컬렉터를 데이터 저장소로 전환 시작

비데이터스토어 플로우 컬렉터을 데이터스토어 플로우 컬렉터로 전환하려면 다음 단계를 수행합니다.

> 이 프로세스를 시작하면 플로우 컬렉터를 이전 상태로 되돌릴 수 없습니다. 아래 단계에 따라 전환을 완료해야 합니다.

1. 데이터 저장소 도메인 검토

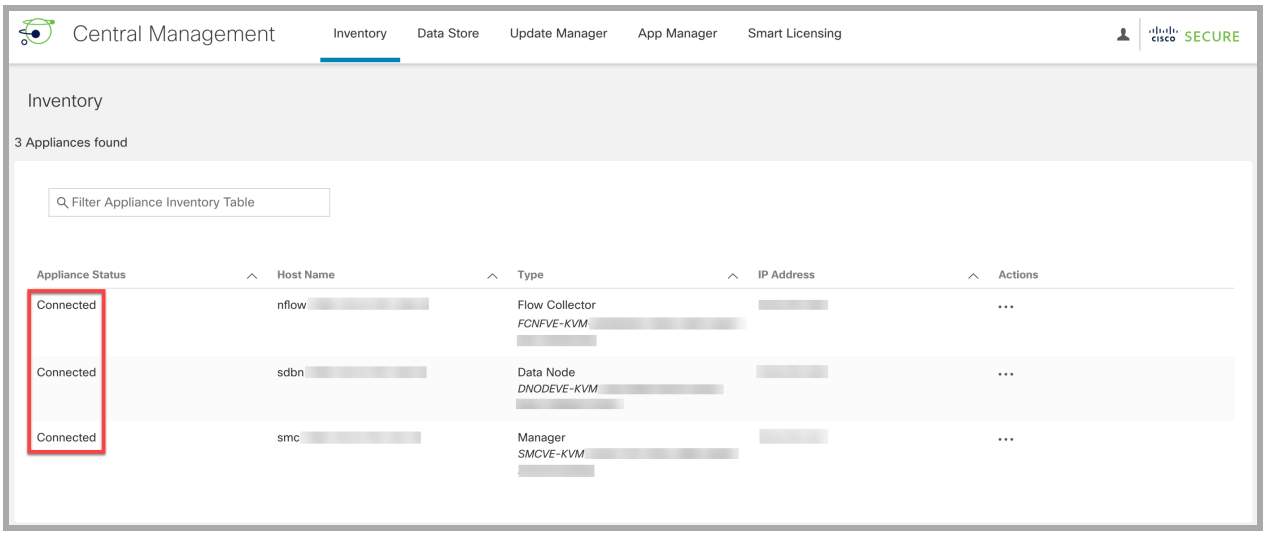
전환할 플로우 컬렉터에 해당하는 데이터스토어 도메인을 확인합니다. 플로우 컬렉터을 이 도메인으로 전환합니다.

- **데이터스토어도메인 추가:** 데이터스토어 도메인을 추가해야 하는 경우 이 가이드의 **도메인 추가 및 구성** 섹션의 지침에 따라 도메인을 생성할 수 있습니다.
- **기존 도메인 가져오기:** 기존 비데이터스토어 도메인에서 설정을 가져오는 경우, 이 가이드의 **기존의 비데이터스토어 도메인 구성을 가져와 데이터 저장소 도메인 생성(선택 사항)** 섹션의 지침을 따라야 합니다.
- **도메인 동기화**: 플로우 컬렉터을 전환하는 동안 전환 전 비데이터스토어 도메인과 데이터 저장소 도메인 간에 설정 및 튜닝을 동기화된 상태로 유지할 수 있습니다. 자세한 내용은 **동기화 데이터스토어 및 비데이터스토어 도메인**를 참조하십시오.

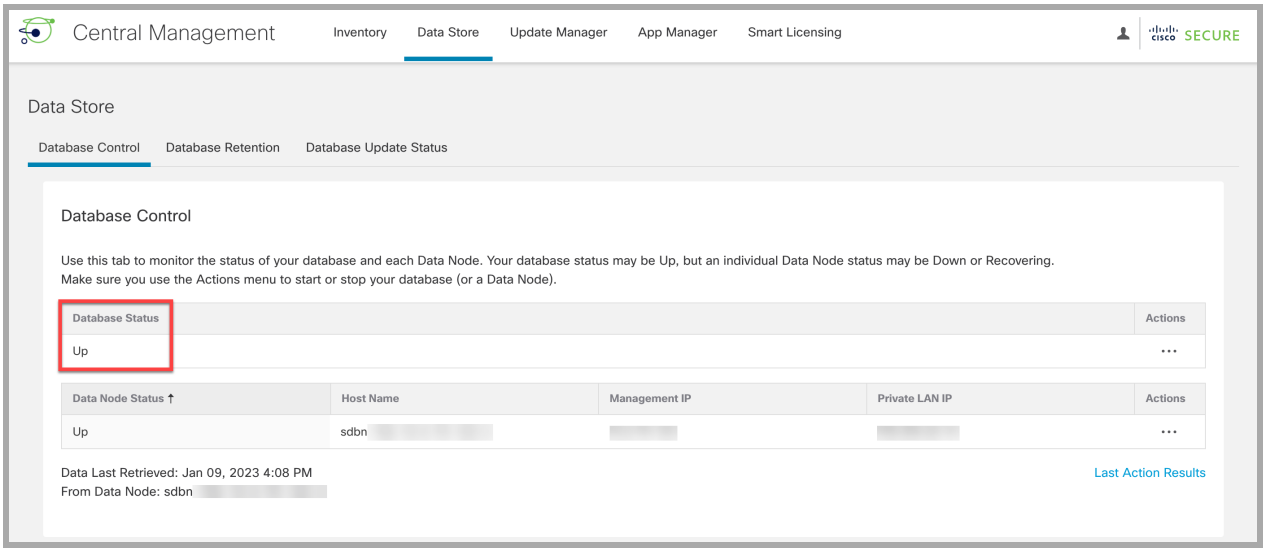
2. 어플라이언스 상태 확인

Central Management 인벤토리 검토

1. **Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**를 선택합니다.
2. 모든 어플라이언스가 **Connected(연결됨)**로 표시되는지 확인합니다. 어플라이언스가 이 상태가 아닌 경우 다음 단계로 진행하기 전에 이 상태로 전환해 보십시오. 어플라이언스를 이러한 상태로 가져올 수 없는 경우, 시스코 지원에 문의하십시오.



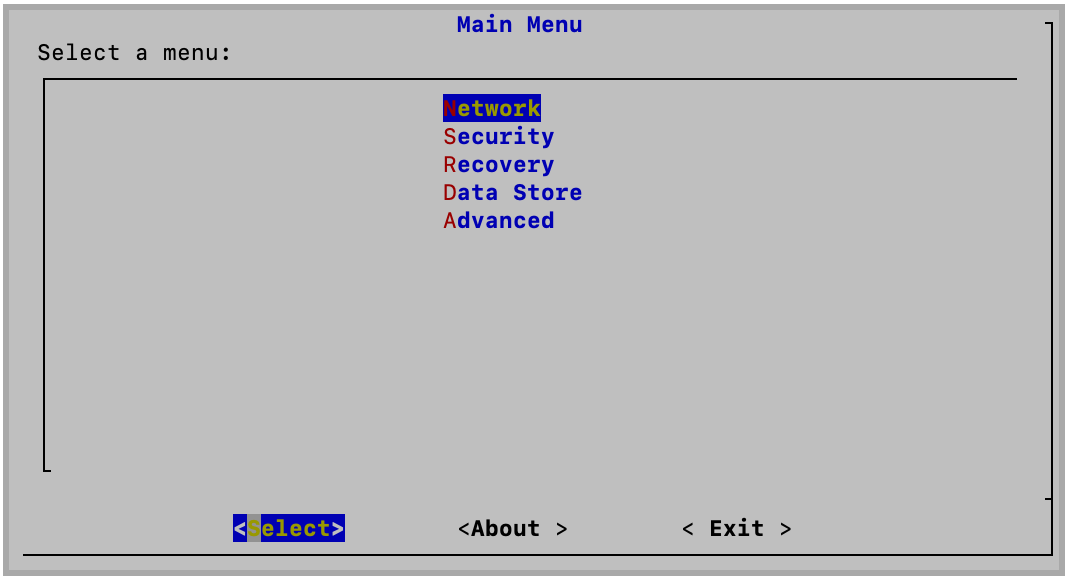
3. **데이터스토어 데이터베이스 제어 탭**을 선택합니다. 데이터베이스 상태가 **Up(작동)**으로 표시되는지 확인합니다.



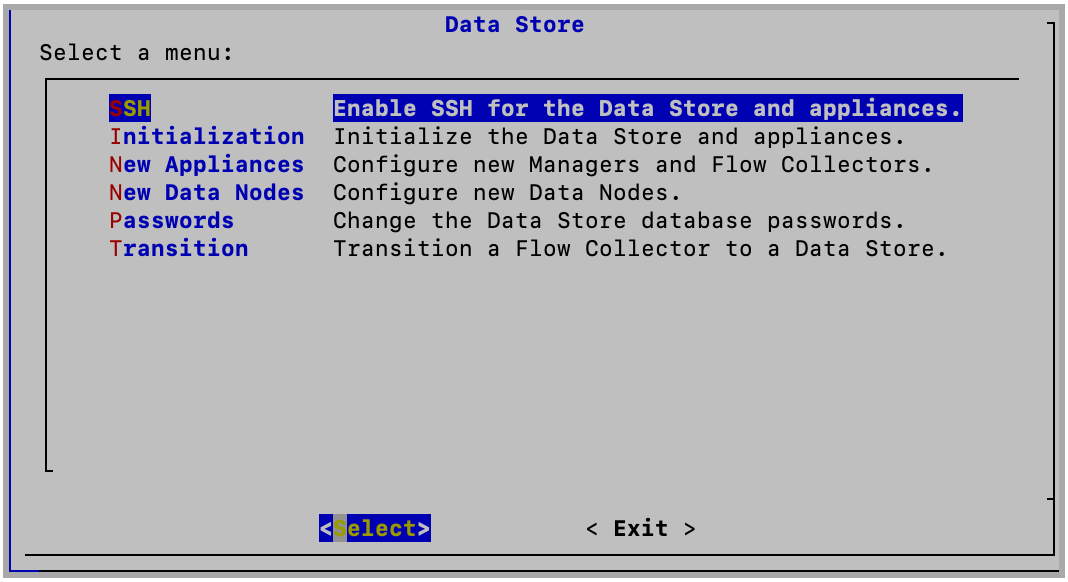
3. 플로우 컬렉터 전환

> 전환 작업 중에 플로우 컬렉터이 재부팅됩니다. 재부팅이 완료되면 플로우 컬렉터가 플로우 컬렉터의 로컬 Vertica 데이터베이스가 아닌 데이터 저장소 데이터베이스에 새 데이터를 저장하기 시작합니다.

1. 매니저 어플라이언스 콘솔(SystemConfig)에 root로 로그인합니다.



2. **Data Store(데이터 저장소) - SSH**를 선택합니다. 이를 통해 SSH가 활성화됩니다.



> 데이터스토어 메뉴가 표시되지 않으면 데이터스토어 도메인이 있는지 확인합니다. 추가 정보는 **1. 데이터 저장소 도메인 검토**

3. 데이터 저장소 메뉴에서 **Transition(전환) - Initiate Transition(전환 시작)**을 선택합니다.
4. 전환할 플로우 컬렉터를 선택합니다.
5. Data Store Domains(데이터 저장소 도메인) 화면에서 1에서 식별한(또는 생성한) 데이터 저장소 도메인을 선택합니다. 데이터 저장소 도메인 검토. 전환된 데이터 저장소의 플로우 컬렉터 데이터는 데이터스토어 데이터베이스로 라우팅되며, 이전의 비데이터스토어

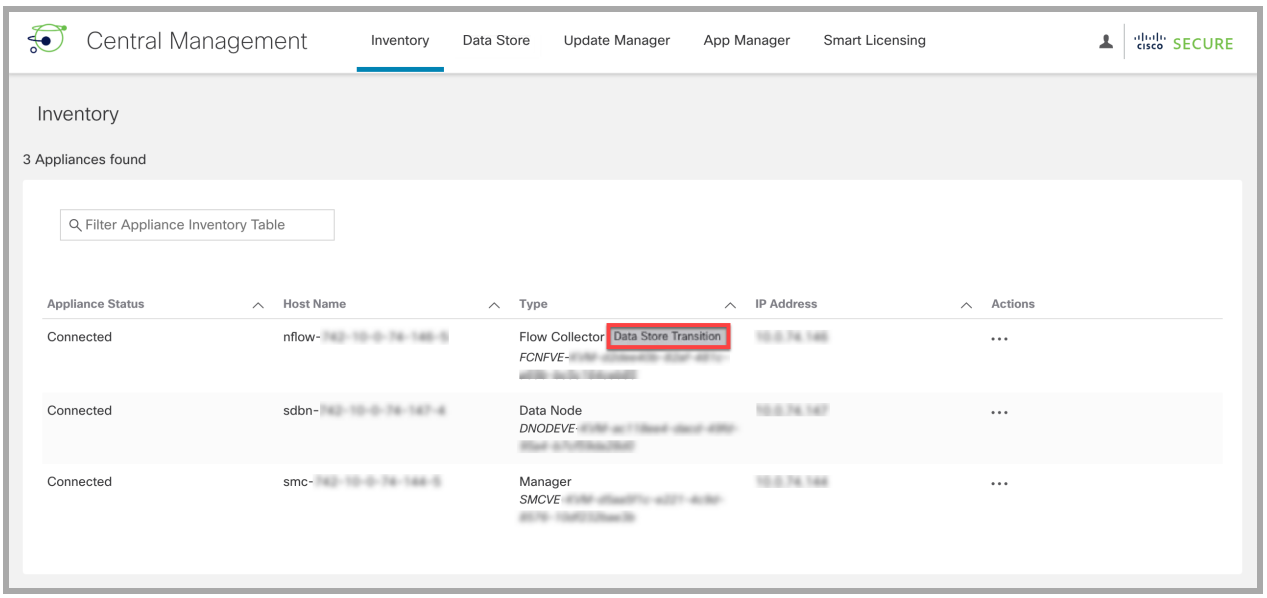
도메인 대신 이 새 도메인을 통해 액세스할 수 있습니다.

6. 화면의 지시에 따라 전환을 확인합니다.

> 전환 시작 절차를 완료하면 이 과정에서 기록 데이터가 삭제되므로 플로우 컬렉터에 로컬로 저장된 기록 데이터가 더 이상 필요하지 않다는 것을 확인하기 전까지는 플로우 컬렉터 전환을 완료하지 마십시오. 자세한 내용은 **데이터 저장소 플로우 컬렉터 전환 완료**를 참조하십시오.

7. Central Management 인벤토리를 검토합니다(**Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**).

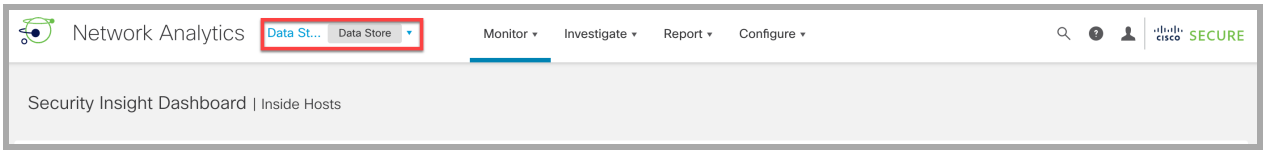
   전환한 플로우 컬렉터에 **Data Store Transition(데이터 저장소 전환)** 태그가 표시되는지 확인합니다.



4. 통신 확인

데이터스토어에서 플로우를 수신하는지 확인합니다.

1. 보안 정도 대시보드로 돌아갑니다.
2. 화면 상단의 도메인 메뉴에서 데이터스토어 도메인이 선택되었는지 확인합니다.



3. **Report(보고서)** 메뉴를 선택합니다.
4. **Report Builder(보고서 작성기)**를 선택합니다.
5. **Create New Report(새 보고서 생성)**를 클릭합니다.

6. **Flow Database Ingest Trend Report(플로우 데이터베이스 수집 트렌드 보고서)** 템플릿을 클릭합니다.
7. 필요에 따라 파라미터를 선택합니다. **Run(실행)**을 클릭합니다.
8. 보고서를 검토하여 데이터베이스 또는 데이터스토어이 플로우를 수신하는지 확인합니다.

플로우 데이터베이스 수집 트렌드 보고서를 실행하는 것 외에도 다음을 수행하여 데이터스토어에서 플로우를 수신하고 있음을 확인할 수 있습니다.

- **플로우 컬렉터 추세 테이블:** 보안 정보 대시보드로 이동하여 플로우 컬렉터 추세 테이블을 검토합니다. 데이터스토어에서 플로우를 수신하는 경우 여기에 표시됩니다.
- **데이터베이스 보존:** Central Management(Configure(구성) > GLOBAL Central Management(전역 중앙 관리))를 열고 Data Store(데이터 저장소) > Database Retention (데이터베이스 보존) 탭에서 정보를 검토합니다. 이 페이지의 데이터스토어 표에 있는 가장 오래된 데이터는 가장 오래된 기록이 데이터스토어에 작성된 날짜와 일수를 추적하는 데 도움이 됩니다. 이 테이블의 데이터는 하루에 한 번만 업데이트되므로 전환 당일에는 이 테이블에 데이터가 표시되지 않습니다. 자세한 내용은 이 가이드의 **데이터베이스 보존 보기** 섹션을 참조하십시오.

플로우 검색 실행

도메인별로 플로우 쿼리를 실행하려면 Investigate(조사) > Flow Search(플로우 검색)를 선택합니다. 맞춤 날짜 범위를 사용하여 결과를 맞춤화합니다.

- **전환 전 쿼리:** 비데이터스토어 도메인에서 전환 전 기록 데이터를 쿼리하려면 플로우 컬렉터 전환 날짜보다 이전의 종료 날짜를 선택해야 합니다.
- **전환 후 쿼리:** 모든 전환 후 데이터스토어 데이터를 쿼리하려면, 플로우 컬렉터를 전환한 날짜 또는 그 이후에 시작하는 시작 날짜를 선택해야 합니다.

Central Manager 인벤토리에서 전환하는 플로우 컬렉터 제거

> Central Manager 인벤토리에서 전환 중인 플로우 컬렉터를 제거하지 마십시오. 이 경우 Cisco 지원팀의 도움을 받아 전환 프로세스를 완료해야 합니다.

플로우 컬렉터 동작 전환

플로우 컬렉터를 전환하면 다음과 같은 동작이 발생합니다.

- **새 데이터:** **플로우 컬렉터를 데이터 저장소로 전환 시작** 절차를 완료한 후 전환하는 플로우 컬렉터에서 모든 새 텔레메트리가 데이터 노드의 데이터스토어데이터베이스로 전송됩니다. **1. 데이터 저장소 도메인 검토**을 검토하면 로컬 전환 전 데이터가 비데이터스토어 도메인에 계속 존재합니다.
- **전환 전 데이터:** 플로우 컬렉터는 데이터에 대한 액세스를 유지하려는 한 전환 전 데이터를 로컬로 계속 저장합니다. 전환 전 데이터가 더 이상 필요하지 않을 때 이를 제거하는 방법에 대한 지침은 **데이터 저장소 플로우 컬렉터 전환 완료**를 참조하십시오.

- **시스템 성능:** 플로우 컬렉터 전환 중 시스템 성능은 전환 전 성능과 유사합니다. 전환이 완료되면 데이터스토어 플로우 컬렉터과 함께 성능 향상이 표시됩니다.

동기화 데이터스토어 및 비데이터스토어 도메인

플로우 컬렉터 전환 중에 구성 및 튜닝을 전환 전 비데이터스토어 도메인과 데이터 저장소 도메인 간에 동기화된 상태로 유지하고 싶을 수도 있습니다. 이 섹션에서는 비데이터스토어 도메인을 관련 데이터스토어 도메인과 동기화하는 프로세스에 대해 설명합니다

> You need administrator access for this procedure.

Synchronized Properties

The following properties will be synchronized between domains:

- Data Store domain specific configuration as well as alert configuration (if enabled). Domain configuration includes:
  - Host Group Management
  - Alarm Severity
  - Policy Management
  - Services, Applications
  - Exporter SNMP profiles (not including passwords)
  - Domain AS Numbers.

Recommended Synchronization Frequency

While you can synchronize your domains as often as you like, we recommend that you limit your synchronizations to only after you perform a group of changes or once a day or week. This is because the synchronization process requires the use of resources that take away from daily processing.

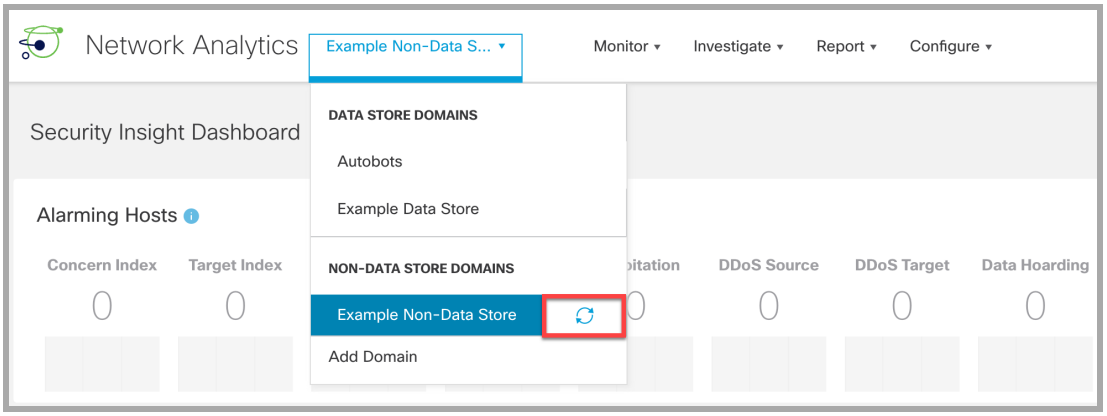
Synchronizing Domains Procedure

Follow these steps to synchronize your Non-데이터스토어 domain (Source) with your 데이터스토어 domain (Target).

1. From the menu bar, choose the Non-데이터스토어 domain that you want to synchronize with your 데이터스토어 domain.
2. From the main menu, choose **Configure > SYSTEM Domain Properties**.
3. Select the **Edit** button.
4. Choose the Data Store domain that you want to synchronize this domain with in the **Target Domain to Synchronize** drop-down menu.

> You can only synchronize your target 데이터스토어 domain with one source Non-데이터스토어 domain. If you attempt to synchronize your target Data Store domain with more then one source Non-데이터스토어 domain, you will receive an error.

5. Click the **Save** button to save your changes. A synchronize button appears next to the Non-데이터스토어 domain that you selected to synchronize with your 데이터스토어 domain.



플로우 컬렉터전환 완료

전환 전 데이터가 더 이상 필요하지 않게 되면 **데이터 저장소 플로우 컬렉터 전환 완료**의 단계에 따라 플로우 컬렉터 전환을 완료할 수 있습니다.

> 플로우 컬렉터에 로컬로 저장된 기록 데이터가 더 이상 필요하지 않음을 확인할 때까지 플로우 컬렉터 전환을 완료하지 마십시오. 이 프로세스 중에 삭제됩니다.

데이터 저장소 플로우 컬렉터 전환 완료

비데이터스토어 플로우 컬렉터를 데이터스토어 플로우 컬렉터로 전환하는 프로세스를 수행한 경우 로컬에 저장된 비데이터데이터스토어를 유지할 필요가 없는 경우, 데이터스토어 플로우 컬렉터 전환을 완료할 수 있습니다.

비데이터스토어 플로우 컬렉터 를 데이터스토어 플로우 컬렉터로 전환하는 데에는 두 가지 주요 절차가 필요합니다.

1. **플로우 컬렉터를 데이터 저장소로 전환 시작** 절차의 단계에 따라 전환 프로세스를 시작합니다. 이렇게 하면 플로우 컬렉터가 **플로우 컬렉터 동작 전환** 에서 설명하는 데이터스토어 전환 상태로 전환됩니다.
2. 전환 프로세스를 완료합니다. 이로 인해 플로우 컬렉터가 단독으로 데이터스토어 플로우 컬렉터가 됩니다. 이 플로우 컬렉터가 저장하는 모든 기존 비데이터데이터스토어가 삭제되고 리소스가 복구되어 플로우 컬렉터의 성능이 향상됩니다.

요구 사항

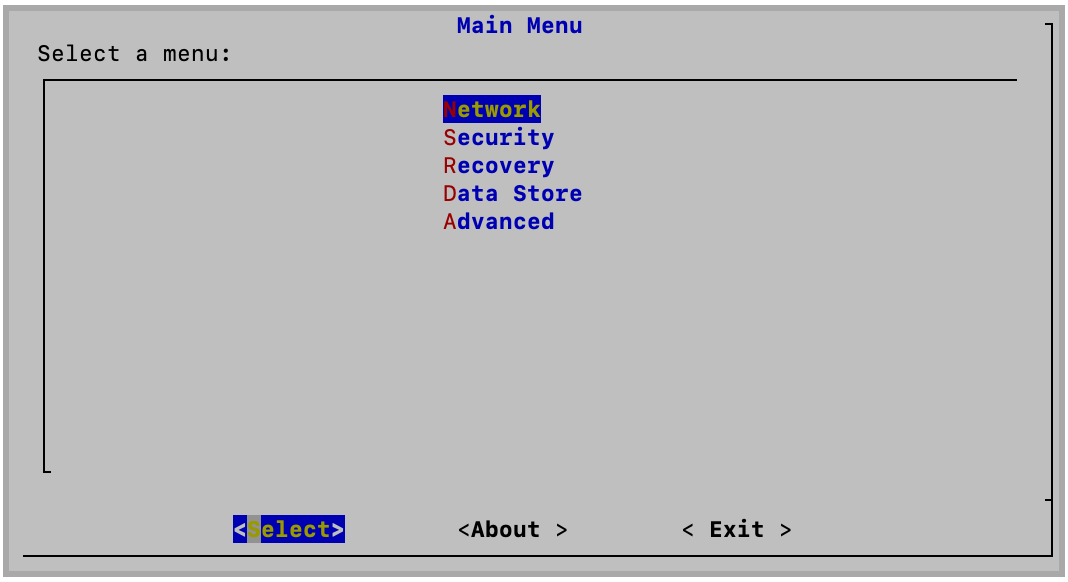
데이터 저장소 플로우 컬렉터 전환을 완료하기 전에 다음을 검토하십시오.

- **전환 시작:** **플로우 컬렉터를 데이터 저장소로 전환 시작** 절차를 완료했는지 확인합니다.
- **기록 데이터:** 플로우 컬렉터에 로컬로 저장된 기록 데이터가 더 이상 필요하지 않은지 확인합니다. 이 프로세스 중에는 삭제됩니다. 비데이터데이터스토어에 대한 데이터 보존 정책이 있으며 데이터스토어 전환을 완료하기 전에 데이터스토어에 새 데이터가 얼마나 있는지 확인하려면 데이터 저장소에 있는 가장 오래된 데이터 표를 검토합니다. 추가 정보는 **데이터베이스 보존 보기**를 참조하십시오.

플로우 컬렉터를 데이터 저장소로 전환 완료

데이터스토어 플로우 컬렉터 전환을 완료하려면 다음 단계를 수행합니다.

1. 매니저 어플라이언스 콘솔(SystemConfig)에 root로 로그인합니다.



2. **데이터스토어 > Transition(전환) > Complete Transition(전환 완료)**를 선택합니다.
3. 플로우 컬렉터를 선택하여 데이터스토어로 전환을 완료할 수 있습니다.
4. 화면의 지시에 따라 전환을 완료합니다.
5. Central Management 인벤토리를 검토합니다(**Configure(구성) > GLOBAL Central Management(전역 중앙 관리)**).

   전환한 플로우 컬렉터에 **Data Store(데이터 저장소)** 태그가 표시되는지 확인합니다.

완료 후 참고

플로우 컬렉터를 데이터 저장소로 전환 완료 절차를 완료한 후,

- 비데이터스토어 도메인에서 플로우 컬렉터에 대한 플로우 쿼리에 더 이상 NetFlow 레코드가 표시되지 않습니다.
- 이전 비데이터스토어 도메인에 플로우 컬렉터이 없는 경우, 해당 도메인을 삭제할 수 있습니다. 자세한 내용은 **도메인 삭제**를 참조하십시오.
- 이 플로우 컬렉터가 저장한 모든 기존 비데이터데이터스토어가 삭제되고 리소스가 복구되어 플로우 컬렉터의 성능이 향상되었습니다.
- 전환된 플로우 컬렉터에서 디스크 공간 사용량이 크게 감소한 것을 확인할 수 있습니다. 시스템 통계, 서비스, 디스크 사용량 및 도커 서비스를 확인하려면 어플라이언스 관리 인터페이스에 로그인합니다.

1. Central Management 인벤토리 페이지에서 어플라이언스용 ••• (**줄임표**) 아이콘을 클릭합니다.
2. **어플라이언스 통계 보기**를 선택합니다.
3. **Home(홈)**을 선택하여 통계를 검토합니다.

비데이터 저장소 구축에 데이터 저장소 추가

이 지침을 사용하기 전에 이미 비 데이터스토어 도메인이 있는 Secure Network Analytics 시스템에서 작업하고 있는지 확인합니다. 지침은 **시스템 구성 계획**을 참조하십시오.

적절한 지침을 사용하여 비 데이터스토어 구축에 데이터스토어를 추가합니다.

- **비데이터 저장소 구축에 데이터 저장소 추가**
- **비데이터 저장소 구축에 데이터 저장소 추가**

> 데이터스토어 호환성 정보는 Secure Network Analytics 하드웨어 및 소프트웨어 버전 지원 매트릭스를 참조하십시오.

기존 플로우 컬렉터

에

추가데이터스토어

데이터스토어를 기존 플로우 컬렉터에 추가하려면 **비데이터 저장소 구축에 데이터 저장소 추가 및 플로우 컬렉터**을 참조하십시오. 이 프로세스를 통해, 전환 전 데이터 또는 가시성의 손실 없이 기존 플로우 컬렉터를 전환하여 데이터스토어 데이터베이스를 사용할 수 있습니다.

새 플로우 컬렉터

로

추가데이터스토어

아래 단계에 따라 데이터스토어에 새 플로우 컬렉터를 추가합니다.

1. 플로우 컬렉터 및 어플라이언스가 모두 동일한 소프트웨어 버전에서 실행되고 있는지 확인합니다. Secure Network Analytics 업데이트 가이드의 지침을 따르십시오.
2. Secure Network Analytics에 플로우 컬렉터과 연결할 데이터스토어 도메인을 생성했는지 확인합니다. 자세한 내용은 이 가이드의 데이터 저장소 도메인 생성 섹션을 참조하십시오.
3. 하드웨어 또는 가상 플로우 컬렉터를 구축 및 설치합니다. 자세한 내용은 x2xx Series 하드웨어 어플라이언스 설치 가이드, Secure Network Analyticsx3xx Series 하드웨어 설치 가이드 또는 Virtual Edition 어플라이언스 설치 가이드를 참조하십시오.
4. 플로우 컬렉터에서 최초 설정을 실행하고 플로우 컬렉터을 데이터스토어의 일부로 구축합니다.
5. 플로우 컬렉터를 Central Manager에 추가합니다. 52xx 플로우 컬렉터가 있는 경우 플로우 컬렉터 데이터베이스 및 플로우 컬렉터 엔진을 이 순서대로 추가해야 합니다. 플로우 컬렉터가 속할 데이터 저장소 도메인을 선택합니다.
6. 데이터스토어에 추가하려는 모든 플로우 컬렉터에 대해 위 단계를 반복합니다.
7. 매니저 어플라이언스 콘솔(SystemConfig)에 로그인하고 **Data Store(데이터 저장소) > New Appliances(새 어플라이언스)**를 선택하여 플로우 컬렉터를 데이터스토어에 추가합니다.

문제 해결

애널리틱스 작업이 지연되고 있습니다.

다음 두 인스턴스 모두에서 "애널리틱스 성능이 저하되었습니다." 시스템 알람이 트리거됩니다.

보조 매니저가 기본 매니저로 승격되었습니다.

기본 매니저의 역할을 보조 매니저의 역할로 변경하고 원래 기본 매니저가 복구되어 기본 역할에 다시 할당되기까지 5시간 이상이 경과한 경우 "애널리틱스 성능이 저하되었습니다." 시스템 알람이 트리거됩니다. 애널리틱스에서는 원래 기본 매니저가 중단된 지난 6시간 동안 발생한 작업을 복구 및 실행합니다. 시스템에서 지난 6시간의 모든 작업을 처리하고 실시간으로 작업을 처리하기 시작할 때까지 작업 성능이 계속 지연됩니다.

성능 저하로 인해 어플라이언스가 다운되었습니다.

시스템에서 성능 저하가 발생하는 경우(일반적으로 CPU 또는 메모리와 같은 리소스 부족으로 발생) 작업이 지연되기 시작합니다. 이 지연이 5시간을 초과하면 "애널리틱스 성능이 저하되었습니다." 시스템 알람이 트리거됩니다. 이 시점에서는 결과가 불완전하며 신뢰할 수 없습니다.

이 실패의 가능한 원인은 초당 플로우를 설정에서 지원되는 것 이상으로 늘린 경우입니다. 이를 해결하려면 초당 플로우를 줄여보거나 매니저, 데이터 저장소 또는 둘 다의 리소스를 늘려보십시오. 문제를 해결할 수 없는 경우, 고객 지원팀에 문의하십시오.

어플라이언스 상태: 구성 채널 다운

인벤토리 페이지에서 어플라이언스 상태가 **구성 채널 다운**으로 표시되는 경우 다음을 확인합니다.

- **통신 설정:** 네트워크 통신 설정을 확인합니다.
- **Trust Store:** 어플라이언스 ID 인증서가 올바른 Trust Store에 저장되었는지 확인합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.
- **인증서:** 어플라이언스 ID 인증서를 변경한 경우 절차를 확인하고 인증서가 올바른 Trust Store에 저장되었는지 확인합니다. 매니지드 어플라이언스 가이드의 SSL/TLS 인증서의 지침을 따르십시오.
- **어플라이언스 제거:** 설정 채널이 중단된 상태에서 Central Management에서 어플라이언스를 제거하는 경우 시스템 설정에서도 어플라이언스가 제거되었는지 확인합니다.
  - 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
  - **SystemConfig**를 입력합니다. Enter를 누릅니다.
  - **Recovery(복구)** > **RemoveAppliance(어플라이언스 제거)**를 선택합니다.

어플라이언스 상태: 데이터 저장소가 초기화되지 않음

Secure Network Analytics 시스템 구성을 완료해야 합니다.

모든 관리자, 플로우 컬렉터 및 데이터 노드를 Central Management 인벤토리에 추가한 후 관리자에서 시스템 설정을 열고 데이터 저장소를 초기화합니다. 자세한 내용은 **6. 초기화 데이터스토어**

어플라이언스 상태: 데이터 저장소가 구성되지 않음

데이터스토어에 새 매니저, 플로우 컬렉터 또는 데이터 노드를 추가한 경우, 시스템 구성을 완료해야 합니다. 지침은 **데이터 저장소 유지 관리**를 참조하십시오.

어플라이언스 관리 인터페이스 열기

Central Management 또는 어플라이언스 직접 로그인을 통해 어플라이언스 관리 인터페이스에 액세스할 수 있습니다.

문제 해결을 위해 Central Management에서 매니저를 제거한 경우, 어플라이언스 관리자에 로그인해야 할 수 있습니다.

1. 브라우저 주소 표시줄에 다음과 같이 어플라이언스 IP 주소를 입력합니다.

   https://<IPAddress>

   - **관리자:** IP 주소 뒤에 **/Manager/Index.html**을 추가합니다.
   - **예:** https://xx.xxx.xx.xxx/Manager/index.html

어플라이언스 ID 교체

각 Secure Network Analytics version 7.x 어플라이언스는 고유한 자체 서명 어플라이언스 ID 인증서를 사용해 설치됩니다. 어플라이언스 ID 인증서를 인증 기관의 인증서로 교체하려면 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 참조하십시오.

> 인증서는 시스템 보안에 중요합니다. 인증서를 부적절하게 수정하면 Secure Network Analytics 어플라이언스 통신이 중단되며 데이터 손실이 발생할 수 있습니다.

Central Manager에서 데이터스토어 어플라이언스 제거

Central Manager(매니저, 플로우 컬렉터, 데이터 노드)에서 데이터스토어어플라이언스를 제거하는 경우, 데이터스토어 자체에서 제거되지는 않습니다. 수작업으로 정리해야 합니다.

- **관리자 및 플로우 컬렉터:** 매니저 및 플로우 컬렉터의 경우, **/lancope/var/services/data-store/config-datastore-inventory-snapshot** 디렉토리에서 제거할 수 있습니다.
- **데이터 노드:** 데이터 노드를 삭제하는 프로세스는 더 복잡하므로 Cisco 지원팀에 지원을 요청하십시오.

호스트 이름, 네트워크 도메인 이름 또는 IP 주소 변경

어플라이언스를 설치하고 구성한 후에 어플라이언스 호스트 이름, 네트워크 도메인 이름 또는 IP 주소를 변경하려면, 매니지드 어플라이언스용 SSL/TLS 인증서 가이드의 지침을 따르십시오.

이 절차의 일환으로 Central Management에서 일시적으로 어플라이언스를 제거하면 어플라이언스 ID 인증서가 자동으로 교체됩니다.

> 어플라이언스 ID 인증서는 이 절차 중 자동 대체됩니다.
>
> **어플라이언스에서 사용자 지정 인증서를 사용하는 경우,** Cisco 지원팀에 문의하여 이러한 설정을 변경하십시오. 여기에 나와 있는 지침은 사용하지 마십시오. 사용자 지정 인증서 및 개인 키의 복사본이 있는지 확인합니다.

도메인 속성 열기

메인 메뉴에서 **Configure(구성) > SYSTEM Domain Properties(시스템 도메인 속성)**을 선택합니다.

추가 정보는 **도메인**을 참조하십시오.

데스크탑 클라이언트 도메인 삭제

> 삭제하려는 도메인에 대해 수집된 모든 데이터에 액세스할 수 없게 되므로 삭제할 데스크톱 클라이언트 도메인을 결정할 때는 주의하십시오.
> **해결 방법**: 실수로 데스크톱 클라이언트에서 모든 도메인을 삭제하고 관리자 웹 애플리케이션에서 잠긴 경우 데스크톱 클라이언트에서 데이터 저장소가 아닌 새 도메인을 생성합니다. 이렇게 하면 매니저 웹 애플리케이션에 다시 액세스할 수 있습니다. 도메인 생성에 대한 자세한 내용은 데스크톱 클라이언트 도움말의 Add Domain(도메인 추가) 항목을 참조하십시오.

어플라이언스 설정 도구 열기

어플라이언스를 구성한 뒤 어플라이언스 설정 도구를 열려면 다음 지침을 따르십시오.

> 어플라이언스 설정 툴을 사용해 호스트 이름, 네트워크 도메인 이름 또는 IP 주소를 변경하면 어플라이언스 ID 인증서가 자동으로 교체됩니다.
>
> **어플라이언스에서 사용자 지정 인증서를 사용하는 경우,** Cisco 지원팀에 문의하여 이러한 설정을 변경하십시오. 여기에 나와 있는 지침은 사용하지 마십시오. 사용자 지정 인증서 및 개인 키의 복사본이 있는지 확인합니다.

1. 어플라이언스 브라우저 주소 표시줄에서 IP 주소 다음에 URL의 끝을 /lc-ast로 변경합니다.

https://<IPAddress>/lc-ast

2. Enter를 누릅니다.
3. 추가 정보는 **1. 최초 설정을 사용하여 환경 구성**

구성 개요

새로운 메뉴 구조로 시스템 구성이 업데이트되었습니다. 시스템 설정에는 종종 문제 해결이 포함됩니다. 도움이 필요할 경우 Cisco 지원팀에 문의하십시오.

- **사용자:** 사용 가능한 메뉴는 root, sysadmin 또는 admin으로 로그인하는지에 따라 결정됩니다.
- **SSH:** 메뉴에 액세스하려면 SSH를 활성화해야 할 수 있습니다.

1. 어플라이언스 콘솔다음에 로그인합니다.
2. **SystemConfig**를 입력합니다. Enter를 누릅니다.
3. 기본 메뉴에서 메뉴를 선택합니다.

- **Network(네트워크):** 어플라이언스 관리 포트 네트워크, 신뢰할 수 있는 호스트 및 네트워크 인터페이스(eth0 구성, MTU 등)를 변경하려면 Network(네트워크)를 선택합니다.
- **Security(보안):** 비밀번호를 변경 또는 재설정(**비밀번호** 참조)하고 시스템 로그 컴플라이언스를 관리하려면 Security(보안)를 선택합니다.
- **Recovery(복구):** Central Management에서 어플라이언스를 제거하거나 공장 기본값을 재설정하거나, 진단 팩을 생성하거나, 이미지를 새로 고치려면 Recovery(복구)를 선택합니다.
- **Advanced(고급):** 루트 쉘을 열거나, 관리자 사용자 어카운트를 관리하거나, SSO(Single Sign-On)를 구성하거나, 재부팅 또는 종료하려면 Advanced(고급)를 선택합니다.
- **Data Store(데이터 저장소):** 이 메뉴는 데이터스토어와 함께 사용하도록 구성된 매니저에서 사용 가능합니다. 이 메뉴를 사용하여 SSH 활성화, 초기화, 데이터 저장소에 신규 관리자 및 플로우 컬렉터 추가, 데이터 저장소에 데이터 노드 추가, 데이터 저장소 데이터베이스 비밀번호 변경 및 플로우 컬렉터를 데이터 저장소로 전환을 수행합니다.

신뢰할 수 있는 호스트 변경

시스템 설정을 사용해 어플라이언스 기본값에서 신뢰할 수 있는 호스트 목록을 변경할 수 있습니다. 그러나 신뢰할 수 있는 호스트를 변경하기 전 Cisco 지원팀에 문의하십시오.

> 신뢰할 수 있는 호스트를 변경하기 전 Cisco 지원팀에 문의하십시오.

기본값에서 신뢰할 수 있는 호스트 목록을 변경하는 경우, 각 Secure Network Analytics 어플라이언스는 구축되어 있는 모든 기타 Secure Network Analytics 어플라이언스를 대상으로 하는 신뢰할 수 있는 호스트 목록에 포함되어 있어야 합니다. 그렇지 않을 경우, 어플라이언스가 서로 통신할 수 없습니다.

1. 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
2. **Network(네트워크)** > **Trusted Hosts(신뢰할 수 있는 호스트)**를 선택합니다.
3. 화면에 표시되는 메시지에 따라 신뢰할 수 있는 호스트를 변경합니다.

MTU(Maximum Transmission Unit, 최대 전송 단위) 구성

다음 지침에 따라 어플라이언스 eth0 네트워크 인터페이스에 대한 MTU(최대 전송 단위)를 구성합니다. 이 숫자는 eth0 인터페이스가 트랜잭션당 전송할 수 있는 최대 패킷 크기를 설정합니다.

> MTU는 네트워크 처리에 영향을 미칩니다. 이 숫자를 변경하는 경우 네트워크에서 일관되게 구성되어 있는지 확인합니다.

1. 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
2. **Network(네트워크)** > **Interface(인터페이스)**를 선택합니다.
3. **eth0**을 선택합니다.
4. **1500**(기본값), **9000** 또는 네트워크 구성 요구 사항에 맞는 숫자를 입력합니다.

> 방화벽 로그의 경우 8,192바이트, NetFlow, sFlow 및 NVM 플로우의 경우 9,216바이트의 최대 MTU 설정을 지원합니다. Security Analytics and Logging(온프레미스) 및 다른 텔레메트리 유형을 사용하여 방화벽 로그를 수집하는 경우 8,192바이트보다 큰 MTU 설정을 구성하지 마십시오.

5. **Confirm(확인)**을 선택합니다.
6. 화면에 표시되는 지시에 따라 변경 사항을 저장합니다.

진단 팩 생성

Cisco 지원팀과 협력하여 문제를 해결해야 하는 경우 진단 팩이 있으면 큰 도움이 됩니다. 다음 지침에 따라 개별 어플라이언스의 진단 팩을 생성합니다.

1. 어플라이언스 콘솔에 root로 로그인합니다.
2. **Recovery(복구)**를 선택합니다.
3. **Diagnostics Pack(진단 팩)**을 선택합니다.
4. 진단 팩을 사용자 정의하려면 메뉴를 선택하고 **Edit(편집)**를 클릭합니다.

메뉴	설명
파일명 접두사	진단 팩의 파일명 접두사를 추가합니다(최대 127자).

비밀번호	진단 팩의 파일 비밀번호를 생성합니다. 파일 비밀번호를 생성하지 않은 경우 기본 방법(Cisco 키)을 사용하여 진단 팩을 암호화합니다.
컨피그레이션 백업	이 옵션을 선택하고 화면의 지시에 따라 진단 팩에 구성 백업을 포함합니다. 백업에 대한 자세한 내용은 도움말에서 백업 구성 파일을 참조하십시오.
모듈	포함할 특정 모듈을 선택하여 진단 팩 콘텐츠를 편집합니다.

5. **마침**을 클릭합니다. 화면의 지시에 따라 진단 팩을 생성합니다.

공장 기본값 재설정

어플라이언스를 공장 기본값(RFD)으로 재설정하려면 다음 지침을 따르십시오. 데이터를 완전히 지우려면 공장 기본값을 두 번 재설정해야 합니다.

- **RFD 두 번**: 데이터를 완전히 지우려면 공장 기본값을 두 번 재설정합니다.
- **Back up Configuration(설정 백업)**: 어플라이언스 설정을 복원하려는 경우 백업 설정 및 데이터베이스 백업 파일을 저장해야 합니다. 자세한 내용은 도움말에서 (Central Management에서) **구성 파일 백업** 및 **데이터베이스 백업/복원(어플라이언스 관리 인터페이스)** 항목을 참조하십시오. RFD 후 백업을 복원하려면 Cisco 지원팀에 문의하십시오.

> 어플라이언스에서 RFD(공장 기본값)를 재설정하면 기존의 모든 데이터 및 설정 정보가 삭제되며 백업을 수행한 경우에만 복원할 수 있습니다.

> 어플라이언스를 공장 기본값으로 재설정하면 중앙 관리를 사용하여 구성을 복원할 수 없습니다. 도움이 필요할 경우 Cisco 지원팀에 문의하십시오.

1. 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
2. **Recovery(복구)** > **Factory Defaults(공장 기본값)**을 선택합니다.
3. 화면에 표시되는 프롬프트에 따라 공장 기본값을 재설정하고 어플라이언스를 재시작합니다.

> 데이터를 완전히 지우려면 각 어플라이언스를 두 번 RFD 해야 합니다.

4. **sysadmin**으로 어플라이언스 콘솔에 로그인하고 화면에 표시되는 프롬프트에 따라 어플라이언스 IP 주소, 호스트 이름, 도메인을 구성합니다. 자세한 지침은 이 가이드의 최초

설정을 사용하여 환경 구성 섹션을 참조하십시오. 이 단계는 RFD할 때 네트워크 설정을 보존하는 경우에도 필요합니다.

5. 어플라이언스 설정 도구에 로그인하여 Central Management에 어플라이언스를 추가합니다. 자세한 내용은 **Central Management(어플라이언스 관리)**를 참조하십시오.

관리자 사용자 활성화/비활성화

기본 관리자 계정을 활성화하거나 비활성화하려면 다음 지침을 따르십시오.

1. 어플라이언스 콘솔에 sysadmin으로 로그인합니다.
2. **고급**을 선택합니다.
3. **Admin User(관리자 사용자)**를 선택합니다.
4. 화면에 표시되는 프롬프트에 따라 Admin User account를 활성화하거나 비활성화합니다.
5. 이 지침을 반복하여 Secure Network Analytics 클러스터의 모든 어플라이언스에 대해 관리자 사용자 계정을 활성화하거나 비활성화합니다.

데이터스토어 구축 문제 해결

하드웨어 구축 문제 해결

어플라이언스 구축 또는 구성 문제의 경우 자세한 정보는 x2xx Series 하드웨어 어플라이언스 설치 가이드 또는 Secure Network Analyticsx3xx Series 하드웨어 설치 가이드를 참조하십시오.

가상 어플라이언스 구축 문제 해결

Virtual Edition 어플라이언스 구축 또는 구성 관련 문제의 경우 Virtual Edition 어플라이언스 설치 가이드를 참조하십시오.

Virtual Edition 최초 설정 및 데이터 노드

설치 중에 데이터 노드의 Virtual Edition에 두 개의 네트워크 어댑터를 할당하지 않는 경우 두 번째 네트워크 어댑터를 검색할 수 없으므로 최초 설정이 실패합니다. 이렇게 하면 상호 데이터 노드 통신을 위해 라우팅할 수 없는 IP를 할당할 수 없습니다. 자세한 내용은 가상 에디션 어플라이언스 설치 가이드를 참고하십시오.

데이터스토어 문제 해결

데이터스토어는 데이터스토어에서 사용 가능한 스토리지 공간의 최대 40%를 유지 관리하기 위해 예약합니다. 총 공간의 최대 60%를 텔레메트리 스토리지에 사용할 수 있습니다.

데이터 노드 전원이 중단되고 재부팅된 후 Vertica Analytics 플랫폼이 자동으로 재시작되지 않음

예기치 않게 데이터 노드에 정전이 발생하여 어플라이언스를 재부팅하는 경우, 데이터가 손상될 수 있으므로 데이터 노드의 Vertica Analytics Platform(Vertica) 인스턴스가 자동으로 다시 시작되지 않을 수 있습니다. 아직 실행 중인 데이터 노드이 충분하여 데이터스토어를 계속 실행할 수 있는 경우, 데이터스토어은 플로우 컬렉터의 데이터를 계속 수집합니다. 그러나 가능한 한 빨리 데이터 노드를 다시 시작하여, 데이터스토어를 다시 조인하여 인접한 데이터 노드에서 누락된 데이터를 검색하고 나머지 데이터 노드를 따라잡을 수 있도록 해야 합니다.

데이터 노드를 재시작하려면 다음 각 방법을 시도해 보십시오.

- Central Management(중앙 관리) > Data Store(데이터 저장소) 탭에서 데이터 노드를 시작합니다. 자세한 내용은 **시작 데이터 노드**을 참조하십시오.
- 데이터 노드가 Data Store(데이터 저장소) 탭에서 시작되지 않는 경우 데이터 노드에 로그인하여 수동으로 Vertica를 재시작합니다. 이렇게 하면 손상된 데이터가 삭제되고 Vertica가 올바르게 재시작됩니다.

데이터 노드 하드웨어 어플라이언스의 경우, 어플라이언스를 재시작하기 전에 데이터 노드의 전원 복원 정책을 업데이트해야 할 수 있습니다. 전원 복원 정책이 전원 끄기로 설정된 경우 전원 손실 후 데이터 노드를 수동으로 재시작해야 합니다. CIMC에서 전원 복원 정책을 구성하는 방법에 대한 자세한 내용은 UCS C-Series GUI 구성 가이드를 참조하십시오.

1. 데이터 노드 어플라이언스 콘솔에 root로 로그인합니다.
2. 다음 명령을 복사하여 텍스트 편집기에 붙여넣습니다.

   ```
   tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
   catalog/ErrorReport.txt
   ```

3. *[node_name]*은 데이터 노드 이름(예: `node0001`)으로 바꿉니다.
4. 업데이트된 명령을 복사하여 명령줄 인터페이스에 붙여넣은 다음 Enter를 눌러 `ErrorReport.txt` 오류 파일의 최신 항목을 검토합니다. 오류 메시지에 데이터 일관성 또는 데이터 손상 문제가 있다는 메시지가 표시되면 다음 단계로 진행하여 Vertica를 강제로 재시작합니다.
5. 다음 명령을 복사하여 텍스트 편집기에 붙여넣습니다.

   ```
   admintools -t restart_node --hosts=[data-node-ip-address] --
   database='sw-datastore' --password="[dbadmin-password]" --force
   ```

6. *[data-node-ip-address]*를 영향을 받는 데이터 노드의 IP 주소로 바꿉니다. **데이터 저장소 탭**에 표시된 개인 IP 주소를 사용해야 합니다. eth0 관리 IP 주소를 사용하지 마십시오.
7. *[dbadmin-password]*는 데이터스토어 `dbadmin` 비밀번호로 바꿉니다.
8. 업데이트된 명령을 복사하여 CLI에 붙여넣은 다음 Enter를 눌러 영향을 받는 데이터 노드에서 Vertica를 강제로 재시작합니다. Vertica는 손상된 데이터를 삭제하고 인접 데이터 노드에서 해당 데이터를 복구합니다.
9. `Do you want to continue waiting?`(계속 대기하시겠습니까?)라는 메시지가 표시되면 `(yes/no)[yes]`로 표시되는 경우 `yes`를 입력하고 Enter를 눌러 대기를 계속합니다.

   Vertica는 인접 데이터 노드에서 영향을 받는 데이터 노드의 정보를 복구하므로, 영향을 받는 데이터 노드가 중단된 동안 데이터 노드이 대량의 플로우 트래픽을 수집한 경우 영향을 받는 데이터 노드의 정보를 복구하는 데 시간이 걸릴 수 있습니다.

10. 데이터 노드에 전원을 공급하기 위한 Cisco의 권장 사항을 검토합니다. 자세한 내용은 x2xx Series 하드웨어 어플라이언스 설치 가이드, Secure Network Analyticsx3xx Series 하드웨어 설치 가이드 또는 Virtual Edition 어플라이언스 설치 가이드를 참조하십시오.

데이터스토어 정전 후 시작되지 않음

Central Management(중앙 관리)의 Data Store(데이터 저장소) 탭에서 데이터베이스 상태를 검토합니다. 여기에서 데이터베이스 또는 데이터 노드를 시작할 수 있습니다. 자세한 내용은 **데이터스토어 데이터베이스 상태 보기**를 참조하십시오.

패치 설치 및 소프트웨어 업데이트

소프트웨어 버전에 대한 최신 패치를 설치하여 Secure Network Analytics를 최신 상태로 유지해야 합니다. 자세한 내용 및 지침은 Cisco Software Central을 참조하십시오.

소프트웨어 업데이트는 Cisco Software Central의 Cisco 스마트 어카운트에도 게시됩니다. 업데이트를 성공적으로 수행하려면 Secure Network Analytics업데이트 가이드의 지침을 따르십시오.

지원 팀에 문의

기술 지원이 필요하면 다음 방법 중 하나를 선택하십시오.

- 현지 Cisco 파트너에게 문의합니다.
- Cisco 지원팀에 문의
- 웹에서 사례를 확인하려면 http://www.cisco.com/c/en/us/support/index.html을 참조합니다.
- 이메일로 사례를 확인하려면 tac@cisco.com을 이용합니다.
- 전화 지원: 1-800-553-2447(미국)
- 월드와이드 지원 번호: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

변경 기록

문서 버전	게시일	설명
1_0	2023년 2월 27일	최초 버전
1_1	2023년 4월 5일	사소한 업데이트
1_2	2023년 4월 6일	사소한 업데이트
1_3	2023년 8월 10일	사소한 업데이트
1_4	2023년 2월 27일	업데이트된 데이터스토어 백업 초기화 절차 끊어진 링크 수정

저작권 정보