시스템 관리

다음 주제에서는 시스템 데이터베이스 업데이트, 시스템 백업 및 복원 등의 시스템 관리 작업을 수행하는 방법을 설명합니다.

소프트웨어 업데이트 설치

시스템 데이터베이스 및 시스템 소프트웨어에 업데이트를 설치할 수 있습니다. 다음 주제에서는 이러한 업데이트를 설치하는 방법을 설명합니다.

시스템 데이터베이스 및 피드 업데이트

시스템에서는 여러 데이터베이스 및 보안 인텔리전스 피드를 사용하여 고급 서비스를 제공합니다. Cisco에서는 보안 정책에서 최신 정보를 사용할 수 있도록 이러한 데이터베이스 및 피드에 대한 업데이트를 제공합니다.

시스템 데이터베이스 및 피드 업데이트 개요

Threat Defense는 다음 데이터베이스 및 피드를 사용하여 고급 서비스를 제공합니다.

침입 규칙

새로운 취약성이 알려지면 Cisco Talos Intelligence Group(Talos)에서 사용자가 가져올 수 있는 침입 규칙 업데이트를 릴리스합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

침입 규칙은 업데이트된 새로운 침입 규칙과 전처리기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 컨피그레이션을 재구축해야 합니다.

침입 규칙 업데이트는 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오. 느린 네트워크에서는 업데이트 시도가 실패할 수 있는데, 이 경우 재시도해야 합니다.

GeoDB(Geolocation database)

Cisco Geolocation Database(GeoDB)는 라우팅 가능 IP 주소와 연결된 지리적 데이터(국가, 도시, 좌표 등)의 데이터베이스입니다.

GeoDB 업데이트는 물리적 위치의 업데이트된 정보를 제공하여 시스템이 라우팅 가능한 탐지된 IP 주소에 연결할 수 있습니다. 지리위치 데이터를 액세스 제어 규칙의 조건으로 사용할 수 있습니다.

GeoDB 업데이트에 필요한 시간은 어플라이언스에 따라 다릅니다. 설치하는 데 일반적으로 30~40분이 소요됩니다. GeoDB 업데이트를 수행해도 지리위치 정보의 지속적인 수집을 비롯한 기타 시스템 기능이 중단되지는 않지만, 업데이트를 완료하는 동안 시스템 리소스가 사용됩니다. 업데이트를 예약하는 경우 이를 고려하십시오.

VDB(Vulnerability Database)

Cisco VDB(Vulnerability Database)는 호스트가 영향을 받기 쉬운 알려진 취약점의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 방화벽 시스템은 지문과 취약점의 상관관계를 지정하므로, 특정 호스트가 네트워크 보안 침해 위험을 증가시키는지를 쉽게 확인할 수 있습니다. Cisco Talos Intelligence Group(Talos)는 VDB에 주기적인 업데이트를 생성합니다.

취약성 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트의 수에 따라 달라집니다. 시스템 다운타임의 영향을 최소화하려면 시스템 사용량이 적은 시간에 업데이트를 예약할 수 있습니다. 네트워크에 있는 호스트의 수를 1000으로 나누면 업데이트를 수행하는 데 걸리는 대략적인 시간(분)이 나옵니다.

VDB를 업데이트한 후에는 컨피그레이션을 재구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

Cisco Talos Intelligence Group(Talos) 보안 인텔리전스 피드

Talos 에서는 보안 인텔리전스 정책에 사용하기 위해 정기적으로 업데이트되는 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 이러한 피드에는 알려진 위협에 대한 주소 및 URL이 포함됩니다. 피드가 업데이트되면 재구축하지 않아도 됩니다. 이후의 연결 평가에는 새 목록이 사용됩니다.

URL 카테고리/평판 데이터베이스

시스템은 Cisco CSI(Collective Security Intelligence)에서 URL 카테고리 및 평판 데이터베이스를 가져옵니다. 카테고리 및 평판을 기준으로 필터링하는 URL 필터링 액세스 제어 규칙을 구성하는 경우에는 요청한 URL과 데이터베이스를 대조하여 일치 여부를 확인합니다. **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)**에서 데이터베이스 업데이트 및

일부 기타 URL 필터링 환경 설정을 구성할 수 있습니다. URL 카테고리/평판 데이터베이스 업데이트는 다른 시스템 데이터베이스용 업데이트를 관리하는 것과 같은 방식으로 관리할 수 없습니다.

시스템 데이터베이스 업데이트

편의상 시스템 데이터베이스 업데이트를 수동으로 검색하여 적용할 수 있습니다. Cisco 지원 사이트에서 업데이트를 검색합니다. 따라서 시스템 관리 주소에서 인터넷으로 이동하는 경로가 있어야 합니다.

또는 인터넷에서 직접 업데이트 패키지를 검색한 다음, 워크스테이션에서 업로드할 수 있습니다. 이 방법은 주로 에어 갭(air-gapped) 네트워크를 위한 것으로, 이 네트워크 환경에는 Cisco에서 업데이트를 검색하기 위한 인터넷 경로가 없습니다. 시스템 소프트웨어 업그레이드를 다운로드할 수 있는 동일한 폴더에서 software.cisco.com의 업데이트를 다운로드합니다.

참고 2022년 5월에 GeoDB를 두 개의 패키지로 분할했습니다. IP 주소를 국가/대륙에 매핑하는 국가 코드 패키지와 라우팅 가능한 IP 주소와 관련된 추가 상황 데이터를 포함하는 IP 패키지입니다. device manager은 IP 패키지의 정보를 사용하거나 사용한 적이 없습니다. 이 분할은 로컬로 관리되는 threat defense 구축에서 상당한 디스크 공간을 절약합니다. Cisco에서 직접 GeoDB를 가져오는 경우 이전 통합형 패키지와 동일한 파일 이름을 가진 국가 코드 패키지(Cisco_GEODB_Update-*date-build*)를 가져와야 합니다.

데이터베이스 업데이트를 검색하고 적용하는 정기적인 일정을 설정할 수도 있습니다. 이러한 업데이트는 크기가 클 수 있으므로 네트워크 활동이 적은 시간에 예약합니다.

참고 데이터베이스 업데이트가 진행 중인 동안에는 사용자 인터페이스가 작업에 응답하는 속도가 느려질 수 있습니다.

시작하기 전에

보류 중인 변경 사항에 영향을 줄 가능성을 방지하려면 이러한 데이터베이스를 수동으로 업데이트하기 전에 컨피그레이션을 디바이스에 구축합니다.

VDB 및 URL 카테고리 업데이트에서 애플리케이션 또는 카테고리를 제거할 수 있다는 점에 유의하십시오. 변경 사항을 구축하기 전에 이러한 사용되지 않는 항목을 사용하는 액세스 제어 또는 SSL 암호 해독 규칙을 업데이트해야 합니다.

프로시저

단계 **1** 디바이스를 선택한 다음, Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 업데이트 페이지가 열립니다. 페이지의 정보에는 각 데이터베이스의 현재 버전과 각 데이터베이스가 업데이트된 마지막 날짜 및 시간이 표시됩니다.

단계 **2** 수동으로 데이터베이스를 업데이트하려면 해당 데이터베이스의 섹션에서 다음 옵션 중 하나를 클릭합니다.

- **Update from Cloud(**클라우드에서 업데이트**)** — device manager이 Cisco Cloud에서 업데이트 패키지를 검색하도록 합니다. 이 방법은 가장 쉽고 신뢰할 수 있는 방법이지만, 이를 사용하려면 인터넷에 연결할 경로가 있어야 합니다.
- **(**아래쪽 화살표**)** > 옵션 — 워크스테이션 또는 워크스테이션에 연결된 드라이브에서 업데이트 패키지를 선택합니다. 이 옵션은 다음 중 하나입니다.
  - **Select File(**파일 선택**)** — VDB 또는 지리위치 패키지를 선택합니다.
  - **Update to Newer Version(**새 버전으로 업데이트**)** — 현재 설치된 패키지보다 새로워진 침입 규칙 패키지를 선택합니다.
  - **Downgrade to Older Version(**이전 버전으로 다운그레이드**)** — 현재 설치된 패키지보다 이전의 침입 규칙 패키지를 선택합니다.

규칙 및 VDB 업데이트를 수행하려면 컨피그레이션 구축 시 이를 활성화해야 합니다. 클라우드에서 업데이트할 때 지금 구축할 것인지 묻는 메시지가 표시되면 **Yes(**예**)**를 클릭합니다. **No(**아니요**)**를 클릭하는 경우 가장 빠른 시일 내에 구축 작업을 시작해야 합니다.

자체 파일을 업로드할 경우에는 항상 수동으로 변경 사항을 구축해야 합니다.

참고 침입 규칙 패키지를 수동으로 업로드할 때는 Snort 버전에 적합한 패키지 유형(Snort 2의 경우 SRU, Snort 3의 경우 LSP)을 업로드해야 합니다. 비 액티브 Snort 버전용 패키지를 업로드할 수 있지만 버전을 전환하지 않으면 활성화되지 않습니다. Snort 버전 전환에 대한 자세한 내용은 Snort 2와 Snort 3 간 전환를 참조하십시오.

단계 **3** (선택 사항) 정기적인 데이터베이스 업데이트 일정을 설정하려면 다음을 수행합니다.

a) 원하는 데이터베이스의 섹션에서 **Configure(**구성**)** 링크를 클릭합니다. 일정이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

데이터베이스의 업데이트 일정은 별개이므로 별도로 일정을 정의해야 합니다.

b) 업데이트 시작 시간을 설정합니다.

- 업데이트 빈도(매일, 매주, 매월)
- 매주 또는 매월의 경우 업데이트를 수행할 요일이나 날짜
- 업데이트를 시작할 시간 지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

c) 규칙 또는 VDB 업데이트의 경우, 시스템에서 데이터베이스 업데이트 시 항상 컨피그레이션을 구축하도록 하려면 **Automatically Deploy the Update(**자동으로 업데이트 구축**)** 체크 박스를 선택합니다.

업데이트는 구축될 때까지 적용되지 않습니다. 자동 구축 시에는 아직 구축되지 않은 다른 컨피그레이션 변경 사항도 구축됩니다.

d) **Save(**저장**)**를 클릭합니다.

참고 반복 예약을 제거하려면 **Edit(**수정**)** 링크를 클릭하여 예약 대화 상자를 연 다음 **Remove(**제거**)** 버튼을 클릭합니다.

Cisco 보안 인텔리전스 피드 업데이트

Cisco Talos Intelligence Group(Talos) 에서는 정기적으로 업데이트되는 보안 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 피드가 업데이트되면 재구축하지 않아도 됩니다. 이후의 연결 평가에는 새 목록이 사용됩니다.

시스템이 인터넷에서 피드를 업데이트할 때 엄격한 제어를 원할 경우, 해당 피드에 대한 자동 업데이트를 비활성화할 수 있습니다. 그러나 자동 업데이트는 가장 연관성 있는 최신 데이터를 지원합니다.

프로시저

단계 **1** 디바이스를 선택한 다음 Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 업데이트 페이지가 열립니다. 페이지의 정보에는 **Security Intelligence Feeds(**보안 인텔리전스 피드**)**의 현재 버전과 피드가 업데이트된 마지막 날짜 및 시간이 표시됩니다.

단계 **2** 피드를 수동으로 업데이트하려면 **Security Intelligence Feeds(**보안 인텔리전스 피드**)** 그룹에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

고가용성 그룹의 유닛 하나에서 피드를 수동으로 업데이트하는 경우에는 일관성을 유지하기 위해 다른 유닛에서도 피드를 수동으로 업데이트해야 합니다.

단계 **3** (선택 사항). 정기적인 업데이트 빈도를 구성하려면 다음을 수행합니다.

a) Cisco Feeds(Cisco 피드)의 섹션에서 **Configure(**구성**)** 링크를 클릭합니다. 일정이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

b) 원하는 빈도를 선택합니다.

기본값은 **Hourly(**매시간**)**입니다. **Daily(**매일**)** 업데이트(시간 지정) 또는 **Weekly(**매주**)** 업데이트(요일 및 시간 선택)로 설정할 수도 있습니다. 지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

자동 업데이트되지 않도록 하려면 **Delete(**삭제**)**를 클릭합니다.

c) **OK(**확인**)**를 클릭합니다.

Threat Defense 소프트웨어 업그레이드

threat defense 소프트웨어 업그레이드는 사용 가능 시 설치할 수 있습니다.

업그레이드는 주 버전(A.x), 유지 보수 릴리스(Axy) 또는 패치(Axyz)일 수 있습니다. 또한 긴급한 특정 문제를 해결하는 사소한 업데이트인 핫픽스도 제공할 수 있습니다. 핫픽스는 시스템 재부팅이 필요하지 않을 수도 있지만 다른 업그레이드 시에는 재부팅이 필요합니다. 재부팅이 필요하면 설치 후에 시스템이 자동으로 재부팅됩니다. 업데이트를 설치할 때는 트래픽이 중단될 수 있으므로 시스템 사용량이 적을 때 설치를 수행하십시오.

섀시에서 FXOS 소프트웨어도 업그레이드해야 하는 경우 이 절차를 수행하기 전에 FXOS 업그레이드를 설치합니다.

고가용성 그룹의 유닛을 업그레이드하는 경우에는 스탠바이 디바이스를 업그레이드하고 모드를 전환하여 액티브/스탠바이 유닛을 교체한 다음 새 스탠바이 디바이스에 업그레이드를 설치합니다. 자세한 내용은 HA 디바이스에서 소프트웨어 업그레이드 설치를 참조하십시오.

이 절차를 통해 디바이스를 재이미징하거나 ASA 소프트웨어에서 threat defense 소프트웨어로 마이그레이션할 수는 없습니다.

참고 업데이트를 설치하기 전에 보류 중인 모든 변경 사항을 구축해야 합니다. 또한 백업을 실행하고 백업 복사본을 다운로드해야 합니다. 핫픽스를 제외한 모든 업그레이드는 시스템에 보관된 모든 백업 파일을 삭제합니다.

시작하기 전에

작업 목록을 확인하고 실행 중인 작업이 없는지 확인하십시오. 데이터베이스 업데이트 등 모든 작업이 완료될 때까지 대기했다가 업그레이드를 설치하십시오. 예약된 작업도 모두 확인하십시오. 예약 작업이 업그레이드 작업과 중복되지 않게 하십시오.

업데이트를 수행하기 전에 더 이상 사용되지 않는 애플리케이션이 애플리케이션 필터, 액세스 규칙 또는 SSL 암호 해독 규칙에 없는지 확인하십시오. 이러한 애플리케이션의 이름 뒤에는 "(사용되지 않음)"이라고 적혀 있습니다. 이러한 개체에는 더 이상 사용되지 않는 애플리케이션을 추가할 수 없으며, 후속 VDB 업데이트를 수행하면 이전에 유효했던 애플리케이션이 더 이상 사용되지 않게 될 수 있습니다. 이러한 상황이 발생하면 업그레이드에 실패하고 디바이스는 사용할 수 없는 상태가 됩니다.

Cisco 지원 및 다운로드 사이트에서 https://www.cisco.com/go/ftd-software 업그레이드 파일을 다운로드합니다.

- 제품군 또는 시리즈의 모든 모델에 동일한 업그레이드 패키지를 사용하십시오. 올바른 버전을 찾으려면 모델을 선택하거나 검색한 다음 해당 버전의 소프트웨어 다운로드 페이지로 이동합니다. 파일 유형이 REL.tar인 적절한 업그레이드 파일을 다운로드해야 합니다. 시스템 소프트웨어 패키지 또는 부트 이미지를 다운로드하지 마십시오.
- 업그레이드 파일의 이름을 바꾸지 마십시오. 이름이 바뀐 파일은 유효하지 않은 것으로 간주됩니다.

- 다운그레이드하거나 패치를 제거할 수는 없습니다.
- 업그레이드에 필요한 베이스라인 이미지를 실행 중인지 확인합니다. 호환성 정보는 *Cisco Secure Firewall* 호환성 가이드 http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html을 참조하십시오.
- 새 버전의 릴리스 노트를 확인합니다. 릴리스 노트는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html에서 확인할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

시스템 업그레이드 섹션에는 현재 실행 중인 소프트웨어 버전과 이미 업로드한 업데이트가 표시됩니다.

단계 **2** 업그레이드 파일을 업로드합니다.

- 업그레이드 파일을 아직 업로드하지 않은 경우 **Browse(**찾아보기**)**를 클릭하고 파일을 선택합니다. 업로드가 완료되면 **Run Upgrade Immediately on Upload(**업로드 즉시 업그레이드 실행**)** 옵션을 선택하여 설치를 시작할 수 있습니다.
- 업로드한 파일이 이미 있지만 다른 파일을 업로드하려는 경우에는 **Upload Another File(**다른 파일 업로드**)** 링크를 클릭합니다. 파일은 하나만 업로드할 수 있습니다. 새 파일을 업로드하면 이전 파일이 교체됩니다.
- 파일을 제거하려면 삭제 아이콘( )을 클릭합니다.

단계 **3** (선택 사항). 업그레이드 준비도 확인을 실행합니다.

수동으로 확인을 실행하지 않는 경우 설치를 시작할 때 자동으로 실행됩니다. 확인에 실패하면 업그레이드가 취소됩니다. 자세한 내용은 업그레이드 준비도 확인 실행, 8 페이지를 참고하십시오.

단계 **4** 설치 프로세스를 시작합니다.

System Upgrade(시스템 업그레이드) 섹션에는 최신 threat defense 버전 및 해당하는 경우 FXOS 버전과 FXOS 호환성에 대한 정보 링크가 표시됩니다. threat defense 업그레이드를 설치하기 전에 적절한 FXOS 버전이 이미 설치되어 있는지 확인하십시오. 이 페이지에서는 FXOS 업그레이드를 설치할 수 없습니다. 섀시 모델에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

설치 버튼 옆의 정보는 디바이스가 설치 중에 재부팅되는지 여부를 나타냅니다. 디바이스가 재부팅되면 시스템에서 자동으로 로그아웃됩니다. 설치에는 30분 이상 소요될 수 있습니다.

a) **Upgrade Now(**지금 업그레이드**)**를 클릭하여 설치 프로세스를 시작합니다.

작업을 확인하라는 메시지가 나타납니다.

b) (선택 사항). Confirmation System Upgrade(시스템 업그레이드 확인) 대화 상자에서 **Automatically cancel on upgrade failure and roll back to the previous version(**업그레이드 실패 시 자동으로 취소하고 이전 버전으로 롤백**)**을 선택합니다. 이 옵션은 주요 및 유지 보수 릴리스 업그레이드에만 사용할 수 있습니다. 이 범주는 기본적으로 활성화되어 있습니다.

이 옵션을 선택하고 업그레이드에 실패하면 업그레이드를 시작할 때 디바이스의 이전 상태로 돌아갑니다.

이 옵션을 선택하지 않으면 설치 프로세스가 실패할 경우 설치 프로세스를 재시작할 수 있습니다. 여전히 수동으로 이전 릴리스로 되돌릴 수 있는 옵션이 있으므로 이 대화 상자의 설정에 따라 되돌리기가 자동으로 수행되는지 여부가 결정됩니다.

c) **Continue(**계속**)**를 클릭하여 설치 작업을 시작합니다.

자동으로 로그오프되고 상태 페이지로 이동되며, 여기서 설치 진행 상황을 확인할 수 있습니다. 이 페이지에는 설치를 취소하는 옵션이 포함되어 있습니다. 재부팅이 필요한 경우 재부팅 중에 페이지에 액세스할 수 없게 됩니다. 그러나 페이지를 다시 로드하지 않을 경우 페이지가 계속 작동하여 결국 로그인 페이지로 자동 재로드됩니다.

설치에 실패하면 상태 페이지는 설치를 다시 시도하거나 실패한 작업을 취소하여 이전의 주 버전으로 되돌리는 옵션을 제공합니다.

단계 **5** (선택 사항). 시스템 데이터베이스를 업데이트합니다.

지리위치, 규칙 및 VDB(Vulnerability Database)에 대해 자동 업데이트 작업을 구성하지 않으면 지금 이러한 항목을 업데이트하는 것이 좋습니다.

업그레이드 준비도 확인 실행

시스템은 업그레이드를 설치하기 전에 준비도 확인을 실행하여 시스템에 대해 업그레이드가 유효한지 확인하고, 업그레이드에 방해가 되는 다른 항목을 확인합니다. 준비도 확인에서 실패하면 설치를 다시 시도하기 전에 문제를 해결해야 합니다. 확인에 실패하면 다음에 설치를 시도할 때 실패 메시지가 표시되며, 원하는 경우 강제 설치 옵션이 제공됩니다.

업그레이드를 시작하기 전에 이 절차에서 설명한 대로 준비도 확인을 수동으로 실행할 수도 있습니다.

시작하기 전에

확인할 업그레이드 패키지를 업로드합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

시스템 업그레이드 섹션에는 현재 실행 중인 소프트웨어 버전과 이미 업로드한 업데이트가 표시됩니다.

단계 **2** **Readiness Check(**준비도 확인**)** 섹션을 참조하십시오.

- 업그레이드 확인을 아직 수행하지 않은 경우, **Run Upgrade Readiness Check(**업그레이드 준비도 확인 실행**)** 링크를 클릭합니다. 이 영역에 확인 진행 상황이 표시됩니다. 프로세스를 완료하는 데 약 20초가 소요됩니다.
- 업그레이드 확인이 이미 실행된 경우, 이 섹션에 성공 또는 실패 여부가 표시됩니다. 확인이 실패할 경우, **See Details(**세부 사항 보기**)**를 클릭하면 준비도 확인에 대한 추가 정보가 표시됩니다. 문제를 해결한 후 다시 확인을 실행합니다.

단계 **3** 준비도 확인이 실패하는 경우, 업그레이드를 설치하기 전에 문제를 해결해야 합니다. 세부 정보에는 표시된 문제를 해결하는 방법에 대한 도움말이 포함되어 있습니다. 실패한 스크립트의 경우, **Show Recovery Message(**복구 메시지 표시**)**를 클릭하여 정보를 확인합니다.

다음은 몇 가지 일반적인 문제입니다.

- FXOS 버전 비호환 - FXOS 업그레이드를 별도로 설치하는 시스템(예: Firepower 4100/9300)에서 업그레이드 패키지에 현재 실행 중인 threat defense 소프트웨어 버전과 다른 최소 FXOS 버전이 필요할 수 있습니다. 이 경우, threat defense 소프트웨어를 업그레이드하려면 먼저 FXOS를 업그레이드해야 합니다.
- 지원되지 않는 디바이스 모델 - 이 디바이스에는 업그레이드 패키지를 설치할 수 없습니다. 잘못된 패키지를 업로드했거나 디바이스가 새 threat defense 소프트웨어 버전에서 더 이상 지원되지 않는 이전 모델입니다. 디바이스 호환성을 확인하고 사용 가능하면 지원되는 패키지를 업로드하십시오.
- 디스크 공간 부족 - 사용 가능한 공간이 충분하지 않으면 시스템 백업 등을 통해 불필요한 파일을 삭제하십시오. 직접 생성한 파일만 삭제합니다.

업그레이드 상태 모니터링 및 소프트웨어 업그레이드 취소 또는 재시작

다음 방법을 사용하여 threat defense 소프트웨어 업그레이드의 상태를 확인할 수 있습니다.

- device manager 로그인 화면에는 업그레이드 실패 여부를 포함하여 현재 업그레이드 상태가 표시됩니다. 이 화면에서 **Cancel Upgrade(**업그레이드 취소**)**를 클릭하여 진행 중인 주요 업그레이드를 취소할 수 있습니다. 업그레이드가 실패할 경우 **Cancel Upgrade(**업그레이드 취소**)**를 클릭하여 작업을 중지하고 업그레이드 전의 디바이스의 상태로 돌아갈 수 있습니다. 또는 **Continue(**계속**)**를 클릭하여 업그레이드를 재시작합니다. 업그레이드 취소는 유지 보수 또는 패치 업그레이드가 아닌 주요 업그레이드에만 사용할 수 있습니다.
- threat defense 명령줄에 대한 SSH 세션에서 **show upgrade status** 명령을 사용할 수 있습니다. 만들어진 로그 항목을 확인하려면 **continuous** 키워드를 추가하고 자세한 정보를 보려면 **detail** 키워드를 추가합니다. 두 키워드를 모두 추가하여 지속적인 상세정보를 얻을 수 있습니다.

- 업그레이드를 취소하려면 **upgrade cancel** 명령을 사용합니다. 업그레이드 취소는 유지 보수 또는 패치 업그레이드가 아닌 주요 업그레이드에만 사용할 수 있습니다.
- 업그레이드를 재시도하려면 **upgrade retry** 명령을 사용합니다.
- 디바이스의 이전 상태로 되돌리려면 **upgrade revert** 명령을 사용합니다. 어떤 버전으로 되돌릴지 확인하려면 **show upgrade revert-info** 명령을 사용합니다. 명령에 "No revert information available(사용 가능한 되돌리기 정보 없음)"이 표시되면 되돌릴 수 있는 버전이 없는 것입니다.

완료된 **Threat Defense** 소프트웨어 업그레이드 되돌리기

설치된 주요 업그레이드가 예상대로 작동하지 않는 것으로 확인되면 업그레이드 직전의 상태로 디바이스를 되돌릴 수 있습니다.

프로세스가 완료되면 되돌리기된 릴리스를 설치한 후 변경한 컨피그레이션을 다시 실행해야 합니다.

다음 절차에서는 device manager에서 되돌리는 방법을 설명합니다. device manager을 시작할 수 없는 경우, **upgrade revert** 명령을 사용하여 SSH 세션의 threat defense 명령줄에서 되돌릴 수 있습니다. **show upgrade revert-info** 명령을 사용하여 시스템이 어떤 버전으로 되돌아갈지 확인할 수 있습니다.

시작하기 전에

유닛이 고가용성 쌍의 일부인 경우 두 개의 유닛을 모두 되돌려야 합니다. 페일오버 문제 없이 컨피그레이션을 되돌릴 수 있도록 두 개의 유닛에서 동시에 되돌리기를 시작하는 것이 가장 좋습니다. 두 개의 유닛으로 세션을 열고 각 유닛에서 되돌리기가 가능한지 확인한 다음 프로세스를 시작합니다. 되돌리기 중에는 트래픽이 중단되므로, 가능하면 바쁘지 않은 시간에 수행하십시오.

Firepower 4100/9300 섀시의 경우, 주요 Firepower 버전에는 특별히 검증 및 권장된 컴패니언 FXOS 버전이 있습니다. 즉, threat defense 소프트웨어를 되돌린 후에는 권장되지 않는 버전의 FXOS(너무 새로운 버전)를 실행 중일 수 있습니다. 최신 버전의 FXOS는 이전 버전의 threat defense 버전과 호환되지만, 권장되는 조합에 대해서는 향상된 테스트가 실시됩니다. FXOS를 다운그레이드할 수는 없습니다. 따라서 이러한 상황에 처한 경우 권장 조합을 실행하려면 디바이스에서 이미지를 재설치해야 합니다.

프로시저

단계 **1** 디바이스를 선택한 다음 **Updates(**업데이트**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **System Upgrade(**시스템 업그레이드**)** 섹션에서 **Revert Upgrade(**업그레이드 되돌리기**)** 링크를 클릭합니다.

현재 버전 및 시스템이 되돌아갈 버전을 보여주는 확인 대화 상자가 표시됩니다. 되돌아갈 버전이 없으면 **Revert Upgrade(**업그레이드 되돌리기**)** 링크가 없습니다.

단계 **3** 대상 버전이 마음에 들고 사용 가능한 경우 **Revert(**되돌리기**)**를 클릭합니다.

되돌린 후에는 Smart Software Manager에 디바이스를 다시 등록해야 합니다.

디바이스 재이미징

디바이스를 재이미징할 때는 디바이스 컨피그레이션을 없애고 새 소프트웨어 이미지를 설치합니다. 재이미징은 공장 기본 컨피그레이션을 사용하여 소프트웨어를 새로 설치하기 위한 작업입니다.

다음과 같은 상황에서 디바이스를 재이미징합니다.

- 시스템을 ASA 소프트웨어에서 threat defense 소프트웨어로 변환하려는 경우. ASA 이미지를 실행하는 디바이스를 threat defense 이미지를 실행하는 디바이스로 업그레이드할 수는 없습니다.
- 디바이스가 정상적으로 작동하지 않으며 모든 컨피그레이션을 수정하려는 시도에 실패한 경우

디바이스를 재이미징하는 방법에 대한 자세한 내용은 사용 중인 디바이스 모델의 *Cisco ASA* 또는 *Threat Defense* 디바이스 재이미징 또는 *Threat Defense* 빠른 시작 가이드를 참조하십시오. 이러한 가이드는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html 에서 확인할 수 있습니다.

시스템 백업 및 복원

잘못된 후속 컨피그레이션 또는 물리적 사고로 인해 컨피그레이션이 손상된 경우 디바이스를 복구할 수 있도록 시스템 컨피그레이션을 백업할 수 있습니다.

두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(같은 시기에 릴리스되었을 뿐만 아니라 빌드 번호도 동일해야 함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 간에 컨피그레이션을 복사하지 마십시오. 백업 파일은 어플라이언스를 고유하게 식별하는 정보를 포함하므로 이러한 방식을 통해 공유할 수 없습니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다. 또한 백업에는 라이선싱 또는 클라우드 등록 정보도 포함되지 않으므로 복구 시 존재하는 모든 라이선스 또는 클라우드 등록 상태가 유지됩니다.

백업은 컨피그레이션만 포함하며 시스템 소프트웨어는 포함하지 않습니다. 디바이스를 재이미징해야 하는 경우에는 소프트웨어를 다시 설치해야 하며, 그 이후에 백업을 업로드하고 컨피그레이션을 복구할 수 있습니다.

컨피그레이션 데이터베이스는 백업하는 동안 잠겨 있습니다. 백업 중에는 정책, 대시보드 등을 볼 수는 있지만 컨피그레이션을 변경할 수는 없습니다. 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

백업 및 복원 페이지의 표에는 시스템에서 사용 가능한 모든 기존 백업 복사본과 백업의 파일 이름, 백업이 생성된 날짜와 시간 및 파일 크기가 나열됩니다. 백업의 유형(수동, 예약, 반복)은 해당 백업 복사본을 생성하도록 시스템에 명령한 방법을 기준으로 합니다.

팁 백업 복사본은 시스템 자체에 생성됩니다. 수동으로 백업 복사본을 다운로드하여 안전한 서버에 저장해야 재해 복구에 필요한 백업 복사본을 사용할 수 있습니다. 시스템은 디바이스에 최대 3개의 백업 복사본을 유지합니다. 새 백업이 가장 오래된 백업을 대체합니다.

다음 항목에서는 백업 및 복원 작업을 관리하는 방법을 설명합니다.

시스템 즉시 백업

언제든지 원할 때 백업을 시작할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** **Manual Backup(**수동 백업**)** > **Back Up Now(**지금 백업**)**를 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

백업을 즉시 수행하지 않고 나중에 수행하려는 경우에는 **Schedule(**일정**)**을 대신 클릭하면 됩니다.

단계 **4** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **5** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **6** **Back Up Now(**지금 백업**)**를 클릭합니다.

시스템에서 백업 프로세스를 시작합니다. 백업이 완료되면 백업 파일이 테이블에 표시됩니다. 그러면 백업 복사본을 시스템에 다운로드하고 원하는 경우 다른 위치에 저장할 수 있습니다.

백업을 시작한 후에는 백업 및 복원 페이지에서 나가도 됩니다. 그러나 시스템 속도가 느려질 가능성이 있으므로 백업을 완료할 수 있도록 작업을 일시 중지하는 것을 고려해야 합니다.

또한 백업 중 일부 또는 전체를 수행하는 동안에는 구성 데이터베이스가 잠기므로 백업 프로세스 기간을 변경하는 것을 방지할 수 있습니다.

예약한 시간에 시스템 백업

예약 백업을 설정하여 향후의 특정 날짜와 시간에 시스템을 백업할 수 있습니다. 예약 백업은 한 번만 수행됩니다. 정기적으로 백업을 생성하는 백업 일정을 생성하려면 예약 백업 대신 반복 백업을 구성합니다.

참고 이후 백업 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Scheduled Backup(**예약 백업**)** > **Schedule a Backup(**백업 예약**)**을 클릭합니다.

이미 예약한 백업이 있는 경우 **Scheduled Backup(**예약 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 백업의 날짜와 시간을 선택합니다.

단계 **5** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **6** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **7** **Schedule(**예약**)**을 클릭합니다.

선택한 날짜와 시간이 되면 시스템이 백업을 수행합니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 백업 일정 설정

반복 백업을 설정하여 정기적인 일정으로 시스템을 백업할 수 있습니다. 예를 들어 매주 금요일 자정에 백업을 만들 수 있습니다. 반복 백업 일정을 사용하는 경우 항상 최신 백업 집합을 적용할 수 있습니다.

참고 반복 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Recurring Backup(**반복 백업**)** > **Configure(**구성**)**를 클릭합니다.

이미 반복 백업을 구성한 경우 **Recurring Backup(**반복 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 빈도 및 관련 일정을 선택합니다.

- **Daily(**매일**)** - 시간을 선택합니다. 이 경우 매일 예약된 시간에 백업을 만듭니다.
- **Weekly(**매주**)** - 요일과 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매주 월요일, 수요일, 금요일 23:00(오후 11시)에 백업을 예약할 수 있습니다.
- **Monthly(**매월**)** - 날짜와 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매월 1일, 15일, 28일 23:00(오후 11시)에 백업을 예약할 수 있습니다.

지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

단계 **5** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **6** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

선택한 날짜와 시간이 되면 시스템에서 백업을 만듭니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 일정을 변경하거나 제거할 때까지 해당 일정에 따라 백업이 계속 만들어집니다.

백업 복원

디바이스에서 백업 수행 시 실행하고 있었던 소프트웨어 버전(빌드 번호 포함)과 동일한 버전을 실행하는 한, 필요에 따라 백업을 복원할 수 있습니다. 두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(빌드 번호 포함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다.

그러나 디바이스가 고가용성 쌍의 일부인 경우 백업을 복원할 수 없습니다. 먼저 **Device(**디바이스**)** > **High Availability(**고가용성**)** 페이지에서 HA를 해제해야 백업을 복원할 수 있습니다. 백업이 HA 컨피그레이션을 포함하는 경우 디바이스가 HA 그룹에 다시 조인합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.

복원하려는 백업 복사본이 디바이스에 아직 없으면 복원 전에 백업을 먼저 업로드해야 합니다.

복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다. 또한 백업에는 라이선싱 또는 클라우드 등록 정보도 포함되지 않으므로 복구 시 존재하는 모든 라이선스 또는 클라우드 등록 상태가 유지됩니다.

시작하기 전에

예를 들어 디바이스를 교체할 때와 같이 다른 시스템에서 백업을 복원하는 경우에는 먼저 디바이스를 등록하고 백업 파일에 구성된 기능에 필요한 선택적 라이선스를 활성화하는 것이 가장 좋습니다. 백업 파일에는 라이선스 또는 클라우드 서비스 정보가 포함되지 않으므로 복구 전에 변경한 라이선스 또는 클라우드 등록은 유지됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** 복원하려는 백업 복사본이 사용 가능한 백업 목록에 없으면 **Upload(**업로드**)** > **Browse(**찾아보기**)**를 클릭하여 백업 복사본을 업로드합니다.

단계 **3** 파일의 복원 아이콘( )을 클릭합니다.

복원을 확인하라는 메시지가 나타납니다. 기본값으로, 복원 후에 백업 복사본이 삭제되지만, 복원을 계속하기 전에 복원 후 백업을 제거하면 안 됨을 선택하여 백업을 유지할 수 있습니다.

백업 파일이 암호화된 경우 파일을 열고 암호를 해독하는 데 필요한 **Password(**비밀번호**)**를 입력해야 합니다.

복원이 완료되고 나면 시스템이 재부팅됩니다.

참고 시스템은 재부팅된 후 VDB(Vulnerability Database), 지리위치 및 규칙 데이터베이스 업데이트를 자동으로 확인하여 필요한 경우 다운로드합니다. 이러한 업데이트는 규모가 클 수 있기 때문에 첫 시도는 실패할 수 있습니다. 작업 목록을 확인하고, 다운로드에 실패한 경우 시스템 데이터베이스 업데이트, 3 페이지에 설명된 대로 업데이트를 수동으로 다운로드합니다. 또한 정책도 재구축합니다. 업데이트가 성공할 때까지 모든 후속 구축은 실패합니다.

단계 **4** 필요한 경우 디바이스 > **Smart License(**스마트 라이선스**)** > **View Configuration(**컨피그레이션 보기**)**을 클릭하고, 디바이스를 재등록하고, 필요한 선택적 라이선스를 재활성화합니다.

백업에는 라이선스 또는 클라우드 등록 정보가 포함되지 않습니다. 따라서 새 시스템에 백업을 복구하는 경우(예 : 디바이스를 교체할 때 시스템이 평가 모드에 있는 경우) 이를 등록하고 필요한 라이선스를 활성화해야 합니다. 복구 전에 디바이스를 등록하고 라이선스를 활성화한 경우에는 추가 변경이 필요하지 않습니다.

이전 백업을 동일한 시스템으로 복구하는 경우에는 라이선스 또는 클라우드 등록을 변경할 필요가 없습니다. 그러나 백업이 생성된 후 비활성화한 라이선스가 필요한 기능을 백업에 포함할 수 있으므로 필요한 모든 선택적 라이선스가 활성화되었는지 확인합니다.

ISA 3000 디바이스 교체

ISA 3000에는 분리 후 다른 ISA 3000 디바이스에 삽입할 수 있는 SD 카드가 있습니다. SD 카드에 시스템 백업을 생성하는 경우에는 이 기능을 사용하여 디바이스를 쉽게 교체할 수 있습니다. 문제 있는 디바이스의 SD 카드를 분리하여 새 디바이스에 삽입하기만 하면 됩니다. 그러면 백업을 복원할 수 있게 됩니다.

필요한 백업을 사용할 수 있도록 하려면 SD 카드에 백업을 생성하는 백업 작업을 구성합니다.

백업 파일 관리

새 백업을 생성할 때 백업 파일은 백업 및 복원 페이지에 나열됩니다. 백업 복사본은 무기한 보존되지 않으며, 디바이스의 디스크 공간 사용량이 최대 임계값에 도달하면 새 백업 복사본을 위한 공간 확보를 위해 이전 백업 복사본이 삭제됩니다. 또한 핫픽스 이외의 업그레이드를 설치하면 모든 백업 파일이 삭제됩니다. 따라서 가장 보관 필요성이 높은 특정 백업 복사본을 보관할 수 있도록 백업 파일을 정기적으로 관리해야 합니다.

다음 작업을 수행하여 백업 복사본을 관리할 수 있습니다.

- 보안 스토리지에 파일 다운로드 - 워크스테이션에 백업 파일을 다운로드하려면 해당 파일의 다운로드 아이콘( )을 클릭합니다. 그러면 보안 파일 스토리지로 파일을 이동할 수 있습니다.
- 시스템에 백업 파일 업로드 - 디바이스에서 더 이상 사용할 수 없는 백업 복사본을 복원하려면 **Upload(**업로드**)** > **Browse File(**파일 찾아보기**)**을 클릭하고 워크스테이션에서 해당 복사본을 업로드합니다. 그러면 백업을 복원할 수 있습니다.

참고 업로드한 파일의 이름은 원본 파일 이름과 일치하도록 바꿀 수 있습니다. 또한, 시스템에 3개가 넘는 백업 복사본이 이미 있으면 업로드한 파일을 위한 공간 확보를 위해 가장 오래된 복사본이 삭제됩니다. 이전 소프트웨어 버전에서 생성한 파일은 업로드할 수 없습니다.

- 백업 복원 - 백업 사본을 복원하려면 해당 파일의 복원 아이콘( )을 클릭합니다. 복원 중에는 시스템을 사용할 수 없으며 복원이 완료되면 시스템이 재부팅됩니다. 시스템이 가동 및 실행되고 나면 컨피그레이션을 구축해야 합니다.
- 백업 파일 삭제 - 특정 백업이 더 이상 필요하지 않은 경우, 해당 파일의 삭제 아이콘( )을 클릭합니다. 그러면 삭제를 확인하라는 메시지가 나타납니다. 삭제한 백업 파일은 복구할 수 없습니다.

감사 및 변경 관리

시스템 이벤트 및 사용자가 수행한 작업에 대한 상태 정보를 확인할 수 있습니다. 이 정보를 참조하여 시스템을 감사하고 시스템이 적절하게 관리되고 있는지 확인할 수 있습니다.

감사 로그를 확인하려면 디바이스 > **Device Administration(**디바이스 관리**)** > **Audit Log(**감사 로그**)**를 클릭합니다. 또한 오른쪽 상단 모서리의 **Task List(**작업 목록**)** 또는 **Deployment(**구축**)** 아이콘 버튼을 클릭하여 시스템 관리 정보를 찾을 수도 있습니다.

다음 주제에서는 시스템 감사 및 변경 관리에 대한 몇 가지 주요 개념과 작업을 살펴봅니다.

감사 이벤트

감사 로그는 다음 유형의 이벤트를 포함할 수 있습니다.

Custom Feed Update Event(맞춤형 피드 업데이트 이벤트**), Custom Feed Update Failed(**맞춤형 피드 업데이트 실패**)**

이러한 이벤트는 성공적으로 완료되었거나 맞춤형 보안 인텔리전스 피드에 대한 업데이트가 실패했음을 나타냅니다. 세부 정보에는 업데이트를 시작한 사람과 업데이트 중인 피드에 대한 정보가 포함됩니다.

사용자 지정 규칙 파일 가져오기 요약 이벤트

이러한 이벤트는 하나 이상의 맞춤형 침입 규칙이 포함된 파일을 가져왔음을 나타냅니다. 이벤트에는 추가, 업데이트 및 삭제된 규칙 수의 요약과 가져온 규칙에 대한 세부 사항을 보여주는 차이점 보기가 포함됩니다.

Deployment Completed(구축 완료됨**), Deployment Failed(**구축 실패함**):** 작업 이름 또는 엔터티 이름

이러한 이벤트는 정상적으로 완료되었거나 실패한 구축 작업을 나타냅니다. 세부사항에는 작업을 시작한 사람과 작업 엔터티에 대한 정보가 포함됩니다. 실패한 작업에는 실패 관련 오류 메시지가 포함됩니다.

세부사항에는 **Differences View(**차이 보기**)** 탭도 포함되며, 이 탭에는 작업 시 디바이스에 구축된 변경 사항이 표시됩니다. 여기에는 구축된 엔터티의 모든 엔터티 변경 이벤트가 조합되어 있습니다.

이러한 이벤트를 기준으로 필터링하려는 경우 사전 정의된 **Deployment History(**구축 기록**)** 필터만 클릭하면 됩니다. 이러한 이벤트의 이벤트 유형은 Deployment Event(구축 이벤트)입니다. 완료된 이벤트 또는 실패한 이벤트만 기준으로 하여 필터링할 수는 없습니다.

이벤트 이름에는 사용자 정의 작업 이름(구성하는 경우) 또는 "User(사용자 이름) Triggered Deployment(사용자가 트리거한 구축)"가 포함됩니다. 디바이스 설정 마법사를 실행하는 중에 수행되는 "Device Setup Automatic Deployment(디바이스 설정 자동 구축)" 및 "Device Setup Automatic Deployment (Final Step)(디바이스 설정 자동 구축(최종 단계))" 작업도 있습니다.

Entity Created(엔터티 생성됨**), Entity Updated(**엔터티 업데이트됨**), Entity Deleted(**엔터티 삭제됨**):** 엔터티 이름**(**엔터티 유형**)**

이러한 이벤트는 식별된 엔터티나 개체가 변경되었음을 나타냅니다. 엔터티 세부사항에는 변경을 수행한 사람과 엔터티 이름, 유형, ID가 포함됩니다. 이러한 항목을 기준으로 엔터티를 필터링할 수 있습니다. 세부사항에는 **Differences View(**차이 보기**)** 탭도 포함되며, 이 탭에는 개체에 적용된 변경 사항이 표시됩니다.

HA Action Event(HA 작업 이벤트**)**

이러한 이벤트는 고가용성 컨피그레이션에 대한 작업(사용자가 시작한 작업 또는 시스템이 시작한 작업)과 관련되어 있습니다. 이벤트 유형은 HA Action Event(HA 작업 이벤트)이지만 이벤트 이름은 다음 중 하나입니다.

- **HA Suspended(HA** 일시 중단됨**)** - 시스템에서 HA를 의도적으로 일시 중단했습니다.
- **HA Resumed(HA** 다시 시작됨**)** - 시스템에서 HA를 의도적으로 다시 시작했습니다.
- **HA Reset(HA** 재설정됨**)** - 시스템에서 HA를 의도적으로 재설정했습니다.
- **HA Failover: Unit Switched Modes(HA** 페일오버**:** 유닛 모드 전환됨**)** - 모드를 의도적으로 전환했거나 상태 메트릭 위반으로 인해 시스템에서 페일오버를 실행하였습니다. 메시지에는 액티브 피어가 스탠바이 피어로 전환되었거나 스탠바이 피어가 액티브 피어로 전환되었음이 표시됩니다.

고가용성 동기화 완료됨

액티브 유닛에서 스탠바이 유닛에 컨피그레이션을 동기화했습니다. 이벤트에는 동기화된 버전과 비교한 이전 버전의 변경 정보가 포함됩니다.

Interface List Scanned(스캔된 인터페이스 목록**)**

이 이벤트는 인터페이스 인벤토리에서 변경 사항을 스캔했음을 나타냅니다.

Pending Changes Discarded(보류 중인 변경 사항 취소됨**)**

이 이벤트는 보류 중인 모든 변경 사항을 삭제했음을 나타냅니다. 이 이벤트와 이전 Deployment Completed(구축 완료됨) 이벤트 사이의 Entity Created(엔터티 생성됨), Entity Updated(엔터티 업데이트됨), Entity Deleted(엔터티 삭제됨) 이벤트에 표시된 모든 변경 사항은 제거되며, 영향을 받은 개체의 상태는 마지막으로 구축된 버전으로 되돌아갑니다.

Rules Update Event(규칙 업데이트 이벤트**)**

Snort 3을 실행할 때 LSPUpdateServer 엔티티의 이 이벤트는 새 침입 규칙 패키지를 다운로드하여 설치할 때 추가, 제거 또는 변경된 침입 규칙에 대한 세부 정보를 표시합니다. 이벤트는 100개 규칙으로 제한되므로, 100개보다 많은 항목이 추가, 제거 또는 변경되면 이벤트에 완전한 정보가 포함되지 않습니다. 이 이벤트는 Snort 2 업데이트에는 표시되지 않습니다.

Task Started(작업 시작됨**), Task Completed(**작업 완료됨**), Task Failed(**작업 실패함**)**

작업 이벤트는 시스템이나 사용자가 시작한 작업의 시작과 종료를 나타냅니다. 이 두 이벤트는 작업 목록에서 단일 작업으로 통합됩니다. 이 작업 목록은 오른쪽 상단 모서리에 있는 **Task List(**작업 목록**)** 버튼을 클릭하면 볼 수 있습니다.

작업에는 구축 작업과 수동 또는 예약된 데이터베이스 업데이트와 같은 작업이 포함됩니다. 작업 목록에 있는 모든 항목은 감사 로그의 두 작업 이벤트(작업 시작 표시 및 성공적인 완료 또는 실패)에 부합합니다.

User Logged In(사용자 로그인함**), User Logged Out(**사용자 로그아웃함**):** 사용자 이름

이러한 이벤트에는 사용자의 device manager 로그인 및 로그아웃 시간과 소스 IP 주소가 표시됩니다. User Logged Out(사용자 로그아웃함) 이벤트는 활성 로그아웃과 유휴 시간 초과로 인한 자동 로그아웃 모두에 대해 발생합니다.

이러한 이벤트는 디바이스와 연결을 설정하는 RA VPN 사용자와는 관계가 없습니다. 또한 디바이스 CLI 로그인/로그아웃도 포함하지 않습니다.

감사 로그 보기 및 분석

감사 로그에는 구축 작업, 데이터베이스 업데이트, device manager 로그인/로그아웃과 같은 시스템 시작/사용자 시작 이벤트에 대한 정보가 포함됩니다.

로그에서 확인할 수 있는 이벤트 유형의 설명은 감사 이벤트, 17 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 디바이스를 클릭한 다음 **Device Administration(**디바이스 관리**) > View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

단계 **2** 목차에서 **Audit Log(**감사 로그**)**를 아직 선택하지 않은 경우 클릭합니다.

이벤트는 날짜를 기준으로 그룹화되며 한 날짜 안에서는 시간을 기준으로 그룹화됩니다. 날짜/시간이 가장 최근인 이벤트가 목록 맨 위에 표시됩니다. 처음에는 각 이벤트가 축소되어 있으므로 시간, 이벤트 이름, 이벤트를 시작한 사용자 및 사용자의 소스 IP 주소만 표시됩니다. 사용자 및 IP 주소가 "System(시스템)"이면 디바이스 자체에서 이벤트를 시작한 것입니다.

다음을 수행할 수 있습니다.

- 이벤트 이름 옆의 >를 클릭하여 이벤트를 열고 이벤트 세부사항을 확인합니다. 아이콘을 다시 클릭하면 이벤트가 닫힙니다. 대다수 이벤트에는 이벤트 유형, 사용자 이름, 소스 IP 주소 등의

이벤트 특성이 포함된 단순 목록이 있습니다. 하지만 Entity(엔터티) 및 Deployment(구축) 이벤트에는 다음의 두 탭이 있습니다.

- **Summary(요약)** - 기본적인 이벤트 특성이 표시됩니다.
- **Differences View(차이 보기)** - 이벤트의 일부분으로 수행된 변경과 기존의 "구축된" 컨피그레이션을 비교한 내용이 표시됩니다. 구축 작업의 경우에는 이 보기가 길어서 스크롤해야 할 수도 있습니다. 이 보기에는 구축 작업의 일부로 수행된 Entity(엔터티) 이벤트 변경 사항의 모든 차이가 통합 표시됩니다.

- 필터 필드 오른쪽의 드롭다운 목록에서 다른 시간 범위를 선택합니다. 기본적으로는 지난 2주 동안의 이벤트가 표시되지만 지난 24시간, 7일, 1개월 또는 6개월 동안의 이벤트가 표시되도록 변경할 수 있습니다. **Custom(맞춤형)**을 클릭하고 시작 및 종료 날짜와 시간을 입력해 정확한 범위를 지정합니다.
- 로그의 링크를 클릭하여 해당 항목에 대한 검색 필터를 추가합니다. 그러면 해당 항목을 포함하는 이벤트만 표시되도록 목록이 업데이트됩니다. 또한 **Filter(필터)** 상자만 클릭하면 필터를 직접 작성할 수도 있습니다. 필터 상자 아래에는 사전 정의된 필터 몇 개가 있습니다. 이러한 필터를 클릭하면 관련 필터 기준을 로드할 수 있습니다. 이벤트 필터링에 대한 세부 정보는 감사 로그 필터링, 20 페이지의 내용을 참조하십시오.
- 브라우저 페이지를 다시 로드하여 최신 이벤트로 로그를 새로 고칩니다.

감사 로그 필터링

특정 유형의 메시지만 표시되도록 보기의 범위를 좁히기 위해 감사 로그에 필터를 적용할 수 있습니다. 필터의 각 요소는 정확하고 완전한 일치 항목입니다. 예를 들어 "User = admin"을 사용하는 경우 이름이 **admin**인 사용자가 시작한 이벤트만 표시됩니다.

다음과 같은 기술을 단독으로 사용하거나 조합하여 필터를 작성할 수 있습니다. 필터 요소를 추가할 때마다 목록은 자동으로 업데이트됩니다.

사전 정의된 필터 클릭

Filter(필터) 필드 아래에는 사전 정의된 필터가 있습니다. 링크만 클릭하면 해당 필터가 로드됩니다. 그러면 필터를 확인하라는 메시지가 표시됩니다. 이미 필터를 적용한 경우에는 추가되지 않고 대체됩니다.

강조 표시된 항목 클릭

필터를 작성하는 가장 쉬운 방법은 로그 테이블의 항목 또는 필터링 기준으로 사용할 값이 포함된 이벤트 세부사항을 클릭하는 것입니다. 항목을 클릭하면 해당 값 및 요소의 조합에 대해 올바르게 작성된 요소로 **Filter(필터)** 필드가 업데이트됩니다. 그러나 이 기술을 사용하려면 기존 이벤트 목록에 원하는 값이 포함되어 있어야 합니다.

항목에 대해 필터 요소를 추가할 수 있는 경우 해당 항목 위에 마우스를 가져가면 항목에 밑줄이 표시되며 **Click to Add to Filter(필터에 추가하려면 클릭)** 명령이 나타납니다.

원자성 요소 선택

Filter(필터**)** 필드를 클릭하고 드롭다운 목록에서 원하는 원자성 요소를 선택한 다음 등호 뒤에 일치 값을 입력하고 Enter 키를 눌러 필터를 작성할 수도 있습니다. 필터링 기준으로 사용할 수 있는 요소가 아래에 나와 있습니다. 모든 요소가 모든 이벤트 유형과 관련되어 있는 것은 아닙니다.

- **Event Type(**이벤트 유형**)** - 일반적으로(항상은 아님) 이벤트 이름과 같지만 엔터티 이름이나 사용자 등의 변수 한정자는 없습니다. 구축 이벤트의 경우 이벤트 유형은 Deployment Event(구축 이벤트)입니다. 이벤트 유형에 대한 설명은 감사 이벤트, 17 페이지의 내용을 참조하십시오.
- **User(**사용자**)** - 이벤트를 시작한 사용자의 이름입니다. 시스템 사용자의 경우 모두 대문자로 표시됩니다(예: SYSTEM).
- **Source IP(**소스 **IP)** - 사용자가 이벤트를 시작한 IP 주소입니다. 시스템에서 시작된 이벤트의 소스 IP 주소는 SYSTEM입니다.
- **Entity ID(**엔터티 **ID)** - 엔터티나 개체의 UUID로, 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931과 같이 읽을 수 없는 긴 문자열입니다. 일반적으로 이 필터를 사용하려면 이벤트 세부사항에서 엔터티 ID를 클릭하거나 REST API를 사용하여 관련 GET 호출을 하여 필요한 ID를 검색해야 합니다.
- **Enntity Name(**엔터티 이름**)** - 엔터티 또는 개체의 이름입니다. 사용자 생성 엔터티의 경우에는 보통 개체에 지정한 이름(예: 네트워크 개체의 경우 InsideNetwork)입니다. 시스템 생성 엔터티나 일부 사용자 정의 엔터티의 경우에는 사전 정의되었으나 이해 가능한 이름입니다. 예를 들어 명시적으로 이름을 지정하지 않은 구축 작업의 경우 "User (admin) Triggered Deployment(사용자(관리자)가 트리거한 구축)"입니다.
- **Enntity Type(**엔터티 유형**)** - 엔터티 또는 개체의 종류입니다. 사전 정의되었으나 이해 가능한 이름입니다(예: Network Object(네트워크 개체)). 관련 개체 모델에서 "type(유형)" 값을 확인하여 API Explorer에서 엔터티 유형을 찾을 수 있습니다. API 유형은 일반적으로 모두 소문자이며 공백이 없습니다. 모델에 표시된 것과 똑같이 유형을 입력하는 경우, Enter 키를 누르면 문자열이 더 쉽게 읽을 수 있는 형식으로 변경됩니다. 둘 중 어떤 형식을 입력해도 됩니다. API Explorer를 열려면 More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다.

복잡한 감사 로그 필터에 대한 규칙

여러 원자성 요소가 포함된 복잡한 필터를 작성할 때는 다음 규칙에 주의하십시오.

- 유형이 같은 요소의 경우 해당 유형의 모든 값 간에 OR 관계가 설정됩니다. 예를 들어 "User = admin"과 "User = SYSTEM"을 포함하면 두 사용자 중 한 명이 시작한 이벤트가 일치 항목으로 표시됩니다.
- 유형이 다른 요소의 경우 AND 관계가 설정됩니다. 예를 들어 "Event Type = Entity Updated" 및 "User = SYSTEM"을 포함하면 활성 사용자가 아닌 시스템이 엔터티를 업데이트한 이벤트만 표시됩니다.
- 와일드카드, 정규식, 부분 일치 또는 단순 텍스트 문자열 일치는 사용할 수 없습니다.

구축 및 엔터티 변경 기록 확인

구축 및 엔터티 이벤트의 이벤트 세부사항에는 **Differences View(**차이 보기**)** 탭이 포함되어 있습니다. 이 탭에는 이전 컨피그레이션과 변경 사항을 비교한 내용이 색상 코드가 적용된 상태로 표시됩니다.

- 구축 작업의 경우 구축 전에 디바이스에서 실행 중이었던 컨피그레이션과 실제로 구축된 변경 사항을 비교한 내용이 표시됩니다.
- 엔터티 이벤트의 경우에는 개체의 이전 버전에 적용된 컨피그레이션 변경 사항이 표시됩니다. 이전 버전은 디바이스에서 실제로 사용되었던 버전일 수도 있고 아직 구축되지 않은 개체의 변경 사항일 수도 있습니다.

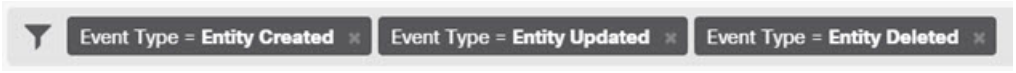
프로시저

단계 **1** 디바이스를 클릭한 다음 **Device Administration(**디바이스 관리**)** > **View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

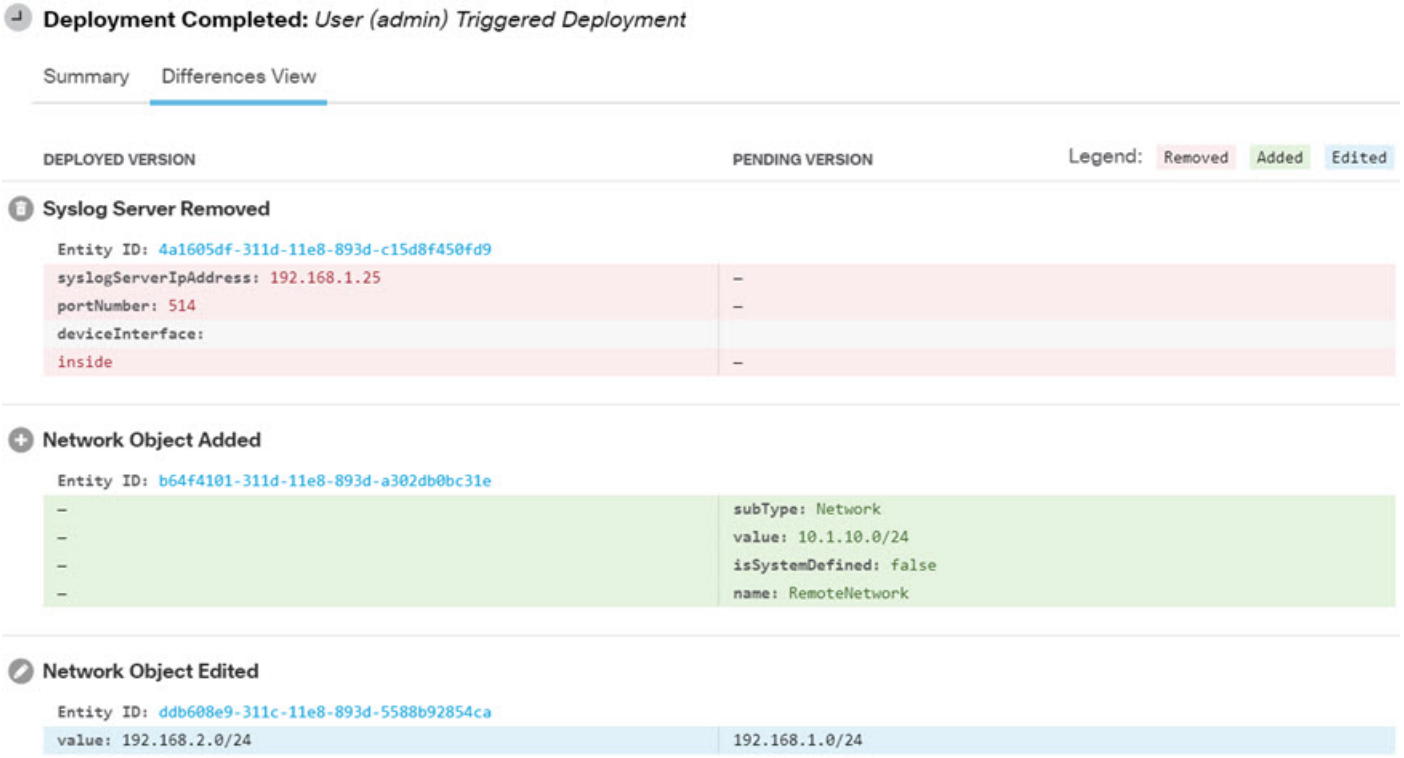
단계 **2** 목차에서 **Audit Log(**감사 로그**)**를 아직 선택하지 않은 경우 클릭합니다.

단계 **3** (선택 사항). 메시지를 필터링합니다.

- 구축 이벤트 - 필터 상자 아래에서 사전 정의된 **Deployment History(**구축 기록**)** 필터를 클릭합니다.
- 엔터티 변경 이벤트 - 원하는 변경 유형에 대해 Event Type(이벤트 유형) 요소를 사용하여 필터를 수동으로 생성합니다. 모든 엔터티 변경 사항을 확인하려면 Entity Created(엔터티 생성됨), Entity Updated(엔터티 업데이트됨) 및 Entity Deleted(엔터티 삭제됨)에 해당하는 3가지 사양을 포함합니다. 그러면 필터가 다음과 같이 표시됩니다.



단계 **4** 이벤트를 열고 **Differences View(**차이 보기**)** 탭을 클릭합니다.



변경 사항에는 색상 코드가 적용되며, 머리글에는 개체 유형과 개체에 대해 수행된 작업 Added(추가됨)(생성됨), Removed(제거됨)(삭제됨) 또는 Edited(수정됨)(업데이트됨)이 표시됩니다. 수정된 개체의 경우 개체에서 변경되었거나 삭제된 특성만 표시됩니다. 구축 작업의 경우에는 변경된 각 엔터티에 대해 개별 머리글이 있습니다. 이 머리글은 개체의 엔터티 유형을 나타냅니다.

모든 보류 중인 변경 사항 취소

아직 구축하지 않은 컨피그레이션 변경 사항이 만족스럽지 않다면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 이렇게 하면 모든 기능이 디바이스에 있는 상태로 되돌아갑니다. 그리고 나면 컨피그레이션 변경을 다시 시작할 수 있습니다.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

보류 중인 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 **2** **More Options(**기타 옵션**)** > **Discard All(**모두 취소**)**을 클릭합니다.

단계 **3** 확인 대화 상자에서 **OK(**확인**)**를 클릭합니다.

시스템이 변경 사항을 취소하며, 프로세스 완료 시에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다. 그리고 Pending Changes Discarded(보류 중인 변경 사항 취소됨) 이벤트가 감사 로그에 추가됩니다.

디바이스 컨피그레이션 내보내기

현재 구축된 컨피그레이션의 복사본을 JSON 형식으로 내보낼 수 있습니다. 해당 파일은 보관 또는 기록 보존용으로 사용할 수 있습니다. 비밀번호 및 비밀 키와 같은 민감한 데이터는 마스크 처리됩니다.

이 디바이스 또는 다른 디바이스로 파일을 가져올 수는 없습니다. 이 기능을 시스템 백업 대신 사용할 수는 없습니다.

구축 작업을 한 번 이상 성공적으로 완료해야 컨피그레이션을 다운로드할 수 있습니다.

프로시저

단계 **1** 디바이스를 선택한 다음 **Device Administration(**디바이스 관리**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Download Configuration(**컨피그레이션 다운로드**)**을 클릭합니다.

단계 **3** **Get Device Configuration(**디바이스 컨피그레이션 가져오기**)**을 클릭하여 파일을 생성하는 작업을 시작합니다.

이전에 파일을 생성한 경우 다운로드 버튼과 **File is ready to download(**파일 다운로드가 준비됨**)** 메시지 및 파일 생성 날짜가 표시됩니다.

컨피그레이션의 크기에 따라서는 파일을 생성하는 데 몇 분 정도 걸릴 수도 있습니다. Export Config(컨피그레이션 내보내기) 작업이 완료되고 파일이 생성될 때까지 작업 목록 또는 감사 로그를 확인하거나 이 페이지를 주기적으로 다시 방문합니다.

단계 **4** 파일이 생성되면 이 페이지로 돌아와 **Download the Configuration File(**컨피그레이션 파일 다운로드**)** 버튼( )을 클릭하여 파일을 워크스테이션에 저장합니다.

Device Manager 및 Threat Defense 사용자 액세스 관리

사용자가 threat defense(HTTPS 액세스)에 로그인할 수 있도록 외부 인증 및 권한 부여 소스를 컨피그레이션할 수 있습니다. 외부 서버는 로컬 사용자 데이터베이스 및 시스템 정의 관리 사용자와 함께 사용하거나 대신 사용할 수 있습니다. device manager 액세스에 대해서는 추가 로컬 사용자 어카운트를 생성할 수는 없습니다.

컨피그레이션을 변경할 수 있는 외부 device manager 사용자 계정이 여러 개일 수는 있지만 이러한 변경 사항을 사용자가 추적할 수는 없습니다. 한 사용자가 변경 사항을 구축하면 모든 사용자가 적용한 변경 사항이 구축됩니다. 잠금은 적용되지 않습니다. 즉, 두 명 이상의 사용자가 같은 개체를 동시에 업데이트하려고 하면 한 사용자만 변경 사항을 저장할 수 있습니다. 또한 사용자를 기준으로 변경 사항을 취소할 수도 없습니다.

device manager에서는 동시 사용자 세션 5개를 허용합니다. 6번째 사용자가 로그인하면 가장 오래된 사용자 세션이 자동으로 로그오프됩니다. 또한 유휴 시간 제한도 적용되므로 20분이 지나면 비활성 사용자가 로그아웃됩니다.

threat defense CLI에 대한 SSH 액세스를 위해 외부 인증 및 권한 부여를 컨피그레이션할 수도 있습니다. 로컬 데이터베이스는 외부 소스를 사용하기 전에 항상 확인되므로 페일세이프 액세스에 대해 추가 로컬 사용자를 생성할 수 있습니다. 로컬 및 외부 소스 모두에서 중복 사용자를 생성하지 마십시오. 관리 사용자를 제외하면 CLI와 device manager에서 겹치는 사용자는 없으며 사용자 어카운트는 완전히 별개입니다.

참고 외부 서버를 사용 중인 경우, 별도 RADIUS 서버 그룹을 설정하거나 특정 threat defense 디바이스 IP 주소에 대해서만 사용자 액세스를 허용하는 RADIUS 서버 내 인증/권한 부여 정책을 생성하여 디바이스의 하위 집합에 대한 사용자의 액세스를 제어할 수 있습니다.

다음 주제에서는 device manager 사용자 액세스와 CLI 사용자 액세스를 컨피그레이션하고 관리하는 방법을 설명합니다.

Device Manager(HTTPS) 사용자를 위한 외부 권한 부여(AAA) 컨피그레이션

외부 RADIUS 서버에서 device manager에 HTTPS 액세스 권한을 제공할 수 있습니다. RADIUS 인증 및 권한 부여를 활성화하면 각기 다른 액세스 권한 레벨을 제공할 수 있으며, 모든 사용자가 로컬 관리자 어카운트를 통해 로그인하지 못하게 할 수 있습니다.

이러한 외부 사용자는 threat defense API 및 API Explorer에 대한 권한을 부여받습니다.

RBAC(역할 기반 액세스 제어)를 제공하려면 RADIUS 서버에서 사용자 어카운트를 업데이트하여 **cisco-av-pair** 특성을 정의합니다. 이는 ISE에서 해당하며, 무료 RADIUS에서는 해당 특성의 철자가 Cisco-AVPair이므로 시스템에서 철자가 올바른지 확인하십시오. 사용자 어카운트에 대해 이러한 속성을 정확하게 정의해야 합니다. 그렇지 않으면 해당 사용자의 device manager 액세스가 거부됩니다. **cisco-av-pair** 특성에 대해 지원되는 값은 다음과 같습니다.

- **fdm.userrole.authority.admin**은 전체 관리자 액세스를 제공합니다. 이러한 사용자는 로컬 관리 사용자가 수행할 수 있는 모든 작업을 수행할 수 있습니다.
- **fdm.userrole.authority.rw**는 읽기-쓰기 액세스를 제공합니다. 이러한 사용자는 읽기 전용 사용자가 수행할 수 있는 모든 작업을 수행할 수 있으며 컨피그레이션 수정 및 구축도 수행할 수 있습니다. 업그레이드 설치, 백업 생성 및 복원, 감사 로그 확인, device manager 사용자의 세션 종료를 포함하는 시스템의 중요 작업만 제한됩니다.

- **fdm.userrole.authority.ro**는 읽기 전용 액세스를 제공합니다. 이러한 사용자는 대시보드 및 컨피그레이션을 볼 수는 있지만 변경할 수는 없습니다. 사용자가 변경을 시도하면 권한이 없음을 설명하는 오류 메시지가 표시됩니다.

사용자가 device manager에 로그인할 때는 페이지 오른쪽 상단에 사용자 이름과 역할이 표시됩니다. 역할은 Administrator(관리자), Read-Write User(읽기-쓰기 사용자) 또는 Read-Only User(읽기 전용 사용자) 중 하나입니다.

RADIUS 서버에서 어카운트를 설정하고 나면 다음 절차를 수행하여 관리 액세스용으로 해당 어카운트를 활성화할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **AAA Configuration(AAA** 컨피그레이션**)** 탭을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** **HTTPS Connection(HTTPS** 연결**)** 옵션을 다음과 같이 컨피그레이션합니다.

- **Server Group for Management/REST API(**관리**/REST API**용 서버 그룹**)** - 기본 인증 소스로 사용할 RADIUS 서버 그룹 또는 로컬 사용자 데이터베이스(LocalIdentitySource)를 선택합니다. 외부 인증을 사용하려는 경우 RADIUS 서버 그룹을 선택해야 합니다.

  서버 그룹이 아직 없으면 **Create New RADIUS Server Group(**새 **RADIUS** 서버 그룹 생성**)** 링크를 클릭하여 지금 생성합니다. 각 서버에 대해 RADIUS 서버 개체도 생성하여 그룹에 추가해야 합니다. 하지만 이 작업은 서버 그룹을 정의할 때 수행할 수 있습니다. RADIUS에 대한 자세한 정보는 RADIUS 서버 및 그룹의 내용을 참조하십시오.

- **Authentication with LOCAL(**로컬로 인증**)** — 외부 서버 그룹을 선택하는 경우 로컬 관리 사용자 어카운트를 포함하는 로컬 ID 소스를 사용하는 방법을 지정할 수 있습니다. 다음 중 하나를 선택합니다.

  - **Before External Server(**외부 서버 전**)** — 시스템이 로컬 소스를 먼저 대조하여 사용자 이름과 비밀번호를 확인합니다.
  - **After External Server(**외부 서버 후**)** — 외부 소스를 사용할 수 없거나 외부 소스에 사용자 어카운트가 없는 경우에만 로컬 소스를 확인합니다.
  - **Never(**사용 안 함**)** — (권장되지 않음.) 로컬 소스를 사용하지 않습니다. 따라서 관리 사용자로 로그인할 수 없습니다.

  주의 **Never(**사용 안 함**)**를 선택하는 경우 관리자 어카운트를 사용하여 device manager에 로그인할 수 없습니다. RADIUS 서버를 사용할 수 없게 되거나 RADIUS 서버에서 어카운트를 잘못 구성하는 경우에는 시스템에서 해당 어카운트를 차단합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Threat Defense CLI(SSH) 사용자를 위한 외부 권한 부여(AAA) 구성

외부 RADIUS 서버에서 threat defense CLI에 SSH 액세스 권한을 제공할 수 있습니다. RADIUS 인증 및 권한 부여를 활성화하면 각 디바이스에 별도 로컬 사용자 계정을 정의하는 대신에 단일 인증 소스에서 다양한 수준의 액세스 권한을 제공할 수 있습니다.

이러한 SSH 외부 사용자는 threat defense API 및 API Explorer에 대한 권한을 부여받지 못합니다. SSH에 대한 권한 부여를 정의하는 데 사용하는 메커니즘은 HTTPS 액세스에 필요한 메커니즘과는 다릅니다. 그러나 SSH 및 HTTPS 두 프로토콜을 통해 특정 사용자가 시스템에 액세스할 수 있도록 SSH 및 HTTPS 권한 부여 기준 모두에서 동일한 RADIUS 사용자를 컨피그레이션할 수 있습니다.

SSH 액세스에 RBAC(Role-Based Access Control)를 제공하려면 RADIUS 서버에서 사용자 계정을 업데이트하여 **Service-Type(**서비스 유형**)** 속성을 정의합니다. 사용자 계정에서 이 속성을 정의해야 합니다. 그러지 않으면 디바이스에 대한 사용자의 SSH 액세스가 거부됩니다. **Service-Type(**서비스 유형**)** 속성에 지원되는 값은 다음과 같습니다.

- **Administrative(**관리**)(6)** — CLI에 대한 **config** 액세스 권한을 제공합니다. 이러한 사용자는 CLI에서 모든 명령을 사용할 수 있습니다.
- **NAS Prompt(NAS** 프롬프트**) (7)** 또는 6 이외의 모든 레벨 - CLI에 대한 기본 액세스 권한을 제공합니다. 이러한 사용자는 모니터링 및 문제 해결을 위해 **show** 명령 같은 읽기 전용 명령을 사용할 수 있습니다.

RADIUS 서버에서 계정을 올바르게 설정하고 나면 이 절차를 수행하여 SSH 관리 액세스용으로 해당 계정을 활성화할 수 있습니다.

참고 로컬 및 외부 소스 모두에서 중복 사용자를 생성하지 마십시오. 중복 사용자 이름을 생성하는 경우, 이 사용자 이름에 동일한 권한 부여 권한이 있는지 확인하십시오. 로컬 사용자 계정에서 권한 부여 권한이 다른 경우에는 외부 버전 사용자 계정의 암호로는 로그인할 수 없고 로컬 암호로만 로그인할 수 있습니다. 권한이 동일한 경우, 사용하는 암호를 통해 외부 사용자와 로컬 사용자 중 어느 사용자로 로그인했는지 알 수 있습니다(암호가 서로 다르다고 가정함). 로컬 데이터베이스를 먼저 검사한다고 하더라도 로컬 데이터베이스에 사용자 이름이 있지만 암호가 올바르지 않을 경우, 외부 서버를 검사합니다. 외부 소스에 대한 암호가 올바른 경우에는 로그인에 성공합니다.

시작하기 전에

기대치를 적절하게 설정하려면 외부에서 정의한 사용자를 다음 동작에 알려주십시오.

- 외부 사용자가 처음 로그인하면 threat defense에서는 필수 구조를 생성합니다. 하지만 이와 동시에 사용자 세션을 생성할 수는 없습니다. 세션을 시작하려면 사용자는 다시 인증하기만 하면 됩니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "New external username identified(새 외부

사용자 이름이 식별됨). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."

- 이와 마찬가지로 Service-Type(서비스 유형)에 정의된 사용자의 권한 부여가 마지막 로그인 후 변경된 경우, 사용자는 다시 인증해야 합니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "Your authorization privilege has changed(귀하의 권한 부여 권한이 변경되었습니다). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **AAA Configuration(AAA** 컨피그레이션**)** 탭을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** **SSH Connection(SSH** 연결**)** 옵션을 다음과 같이 컨피그레이션합니다.

- **Server Group(**서버 그룹**)** - 기본 인증 소스로 사용할 RADIUS 서버 그룹 또는 로컬 사용자 데이터베이스(LocalIdentitySource)를 선택합니다. 외부 인증을 사용하려는 경우 RADIUS 서버 그룹을 선택해야 합니다.

  서버 그룹이 아직 없으면 **Create New RADIUS Server Group(**새 **RADIUS** 서버 그룹 생성**)** 링크를 클릭하여 지금 생성합니다. 각 서버에 대해 RADIUS 서버 개체도 생성하여 그룹에 추가해야 합니다. 하지만 이 작업은 서버 그룹을 정의할 때 수행할 수 있습니다. RADIUS에 대한 자세한 정보는 RADIUS 서버 및 그룹의 내용을 참조하십시오.

  SSH 연결에서는 그룹에서만 첫 서버 2개를 사용한다는 점에 유의하십시오. 3개 이상의 서버에서 그룹을 사용하는 경우, 추가 서버는 시도되지 않습니다. 또한 **Dead Time(**비활성 시간**)** 및 **Maximum Failed Attempts(**최대 실패 시도**)** 그룹 속성은 사용되지 않습니다.

- **Authentication with LOCAL(**로컬로 인증**)** - 외부 서버 그룹을 선택하는 경우, 로컬 ID 소스를 사용하는 방법을 지정할 수 있습니다. SSH 액세스의 경우, 로컬 데이터베이스는 항상 외부 서버에 앞서 확인됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Device Manager 사용자 세션 관리

Monitoring(모니터링**)** > **Sessions(**세션**)**를 선택하면 현재 device manager에 로그인되어 있는 사용자 목록을 확인할 수 있습니다. 목록에는 각 사용자가 현재 세션에 로그인되어 있었던 시간이 표시됩니다.

동일한 사용자 이름이 여러 번 표시되는 경우 해당 사용자가 각기 다른 소스 주소에서 세션을 연 것입니다. 사용자 이름과 소스 주소를 기준으로 하여 세션을 개별적으로 추적하며, 각 세션에는 고유한 타임스탬프가 있습니다.

시스템에서는 동시 사용자 세션 5개를 허용합니다. 6번째 사용자가 로그인하면 가장 오래된 현재 세션이 자동으로 로그아웃됩니다. 또한 20분 동안 아무 작업이 없으면 유휴 사용자는 자동으로 로그아웃됩니다.

device manager 사용자가 잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 사용자 어카운트가 잠깁니다. 사용자는 다시 로그인을 시도하기 전에 잠시 기다려야 합니다. device manager 사용자 어카운트의 잠금을 해제할 수 있는 방법은 없으며 재시도 횟수 또는 잠금 시간 제한을 조정할 수도 없습니다. SSH 사용자의 경우 이러한 설정을 조정하고 어카운트의 잠금을 해제할 수 있습니다.

필요한 경우 세션의 삭제 아이콘( )을 클릭하여 사용자 세션을 종료할 수 있습니다. 세션을 삭제하면 세션에서 로그아웃됩니다. 세션을 종료하는 경우의 잠금 기간은 없으며 사용자는 즉시 다시 로그인할 수 있습니다.

대기 HA 유닛에서 외부 사용자에 대한 Device Manager 액세스 활성화

device manager 사용자에 대한 외부 권한 부여를 컨피그레이션하는 경우, 해당 사용자는 고가용성 쌍의 활성 및 대기 유닛에 모두 로그인할 수 있습니다. 그러나 대기 유닛에 처음 로그인하려면 활성 유닛에 로그인하는 것에 비해 몇 가지 추가 단계가 필요합니다.

외부 사용자가 처음으로 활성 유닛에 로그인하면 시스템에서는 사용자 및 사용자의 액세스 권한을 정의하는 개체를 생성합니다. 이때 관리자 또는 읽기-쓰기 사용자는 대기 유닛에 표시할 사용자 개체에 대해 활성 유닛에서 컨피그레이션을 구축해야 합니다.

이러한 구축과 후속 컨피그레이션 동기화가 성공적으로 완료된 후에야 외부 사용자는 대기 유닛에 로그인할 수 있습니다.

관리자 및 읽기-쓰기 사용자는 활성 유닛에 로그인한 후 변경 사항을 구축할 수 있습니다. 그러나 읽기 전용 사용자는 컨피그레이션을 구축할 수 없습니다. 컨피그레이션을 구축하려면 적절한 권한이 있는 사용자에게 요청해야 합니다.

Threat Defense CLI용 로컬 사용자 계정 생성

threat defense 디바이스에서 CLI 액세스를 위한 사용자를 생성할 수 있습니다. 이 어카운트는 관리 애플리케이션에 대한 액세스는 허용하지 않으며 CLI에 대한 액세스만 허용합니다. CLI는 트러블슈팅 및 모니터링에 유용합니다.

로컬 사용자 계정은 한 번에 둘 이상의 디바이스에서 생성할 수 없습니다. 각 디바이스에는 일련의 고유 로컬 사용자 CLI 계정이 있습니다.

프로시저

단계 **1** config 권한이 있는 어카운트를 사용하여 디바이스 CLI에 로그인합니다.

관리자 사용자 어카운트는 필수 권한을 갖고 있지만, config 권한이 있는 모든 어카운트도 괜찮습니다. SSH 세션 또는 콘솔 포트를 사용할 수 있습니다.

특정 디바이스 모델의 경우, 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. threat defense CLI로 이동하려면 **connect ftd** 명령을 사용하십시오.

단계 **2** 사용자 계정을 생성합니다.

configure user add *username* {**basic** | **config**}

다음 권한 레벨을 가진 사용자를 정의할 수 있습니다:

- **config**- 사용자에게 컨피그레이션 액세스 권한을 제공합니다. 이 명령은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.
- **basic**- 사용자에게 기본 액세스 권한을 제공합니다. 이 명령은 사용자가 컨피그레이션 명령을 입력하는 것을 허용하지 않습니다.

예제**:**

다음 예에서는 config 액세스 권한이 있는 joecool이라는 이름의 사용자 어카운트를 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

참고 **configure password** 명령을 사용하여 암호를 변경할 수 있다고 사용자에게 알려주십시오.

단계 **3** (선택 사항). 보안 요건을 충족하도록 어카운트의 특성을 조정합니다.

다음 명령을 사용하여 기본 어카운트 동작을 변경할 수 있습니다.

- **configure user aging** *username max_days warn_days*

  사용자 비밀번호의 만료일을 설정합니다. 비밀번호가 유효한 최대 일수를 지정한 후 며칠 전부터 사용자에게 다가오는 만료일에 대해 경고할지 일수를 지정합니다. 두 값 모두 1~9999 범위이지만, 경고 일수는 최대 일수보다 작아야 합니다. 어카운트를 생성할 때 비밀번호 만료일이 없습니다.

- **configure user forcereset** *username*

  사용자가 다음 로그인 시 강제로 비밀번호를 변경하게 합니다.

- **configure user maxfailedlogins** *username number*

  어카운트를 잠그기 전에 허용되는 연속 실패 로그인의 최대 수를 1~9999 범위로 설정합니다. 계정의 잠금을 해제하려면 **configure user unlock** 명령을 사용하십시오. 새 어카운트에 대한 기본 값은 로그인 5회 연속 실패입니다.

- **configure user minpasswdlen** *username number*

최소 비밀번호 길이를 1~127 범위로 설정합니다.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  비밀번호 강도 검사를 활성화하거나 비활성화합니다. 이 경우 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자의 암호가 만료되거나 **configure user forcereset** 명령을 사용하는 경우, 이 요건은 사용자가 다음번 로그인할 때 자동으로 활성화됩니다.

단계 **4** 필요 시 사용자 어카운트를 관리합니다.

사용자가 자신의 어카운트를 잠글 수 있게 하거나, 어카운트를 제거하거나 다른 문제를 해결해야 합니다. 시스템에서 사용자 어카운트를 관리하려면 다음 명령을 사용합니다.

- **configure user access** *username* {**basic** | **config**}

  사용자 어카운트에 대한 권한을 변경합니다.

- **configure user delete** *username*

  지정된 어카운트를 삭제합니다.

- **configure user disable** *username*

  지정된 어카운트를 삭제하지 않고 비활성화합니다. 사용자는 어카운트를 활성화할 때까지 로그인할 수 없습니다.

- **configure user enable** *username*

  지정된 어카운트를 활성화합니다.

- **configure user password** *username*

  지정된 사용자에 대한 비밀번호를 변경합니다. 사용자는 일반적으로 **configure password** 명령을 사용하여 자신의 암호를 변경해야 합니다.

- **configure user unlock** *username*

  연속 실패 로그인 시도의 최대 횟수를 초과하므로 잠겨 있는 사용자 어카운트의 잠금을 해제합니다.

시스템 리부팅 또는 종료

필요한 경우 시스템을 리부팅하거나 종료할 수 있습니다.

아래 절차 외에, **reboot** 또는 **shutdown** 명령을 사용하여 SSH 세션 또는 device manager CLI 콘솔을 통해 이러한 작업을 수행할 수도 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **Reboot/Shutdown(**리부팅/종료**)** > 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Reboot/Shutdown(**리부팅/종료**)**을 클릭하면 됩니다.

단계 **2** 필요한 기능을 수행하는 버튼을 클릭합니다.

- **Reboot(**리부팅**)** - 시스템이 올바르게 작동하지 않으며 문제를 해결하기 위한 다른 작업에 실패한 경우에는 디바이스를 리부팅할 수 있습니다. 또한 시스템 소프트웨어를 다시 로드하기 위해 디바이스를 리부팅하도록 요청하는 몇 가지 절차가 있을 수 있습니다.
- **Shut Down(**종료**)** - 전원을 제어되는 방식으로 끄려면 시스템을 종료합니다. 네트워크에서 디바이스를 제거하려는 경우(예: 교체하는 경우) 종료를 사용합니다. 디바이스를 종료한 후에는 하드웨어 On/Off(켜기/끄기) 스위치에서만 되돌릴 수 있습니다.

단계 **3** 작업이 완료될 때까지 기다립니다.

시스템이 리부팅되거나 종료되는 동안에는 device manager 또는 CLI에서 다른 작업을 수행할 수 없습니다.

리부팅이 완료되면 device manager 페이지가 새로 고침되며 로그인 페이지로 이동됩니다. 리부팅이 완료되기 전에 페이지를 새로 고치면 웹 브라우저에서는 해당 시점의 device manager 웹 서버의 작동 상태에 따라 503 또는 404 오류를 반환할 수 있습니다.

종료 시에는 시스템이 결국 전혀 응답할 수 없게 되며 404 오류가 발생합니다. 종료는 시스템을 완전히 끄는 것이기 때문에 이는 정상적인 결과입니다.

시스템 문제 해결

다음 항목에서는 일부 시스템 레벨 트러블슈팅 작업과 기능에 관해 설명합니다. 액세스 제어와 같은 특정 기능의 트러블슈팅에 대한 자세한 내용은 해당 기능 관련 장을 참조하십시오.

주소 **ping**을 통해 연결 테스트

ping은 특정 주소가 활성 상태이고 응답할 수 있는지 확인하는 간단한 명령입니다. 기본 연결이 작동 중인 것입니다. 그러나 디바이스에서 실행 중인 다른 정책 때문에 특정 트래픽 유형이 디바이스를 통과하지 못할 수도 있습니다. **ping** CLI 콘솔을 열거나 디바이스 CLI에 로그인하면 사용할 수 있습니다.

참고 시스템에는 여러 인터페이스가 있으므로 주소 ping에 사용되는 인터페이스를 제어할 수 있습니다. 중요한 연결을 테스트할 수 있도록 적절한 명령을 사용해야 합니다. 예를 들어 시스템에서는 가상 관리 인터페이스를 통해 Cisco 라이선스 서버에 연결할 수 있어야 하므로, **ping system** 명령을 사용하여 연결을 테스트해야 합니다. **ping**을 사용하는 경우에는 데이터 인터페이스를 통해 특정 주소에 연결할 수 있는지를 테스트하게 되므로 결과가 달라질 수도 있습니다.

일반 ping은 ICMP 패킷을 사용하여 연결을 테스트합니다. 네트워크에서 ICMP를 금지하는 경우에는 TCP ping을 대신 사용할 수 있습니다(데이터 인터페이스 ping에만 해당함).

IP 주소 또는 정규화된 호스트 이름(FQDN)을 ping할 수 있습니다. FQDN에서 ping이 작동하려면 관리 또는 데이터 인터페이스용으로 구성된 DNS 서버가 성공적으로 IP 주소를 반환해야 합니다. 관리 및 데이터 인터페이스에 대해 별도로 DNS 서버를 구성해야 합니다. 특정 인터페이스에 대해 DNS 서버가 구성되지 않은 경우 **dig** 명령을 사용하여 지정된 FQDN의 IP 주소를 조회합니다.

네트워크 주소 ping에 사용되는 주요 옵션은 다음과 같습니다.

가상 관리 인터페이스를 통해 주소 **ping**

ping system 명령을 사용하십시오.

ping system 호스트

호스트는 IP 주소일 수도 있고 www.example.com과 같은 FQDN(Fully-Qualified Domain Name)일 수도 있습니다. 데이터 인터페이스를 통해 수행하는 ping과는 달리 시스템 ping에는 기본 횟수가 없습니다. 즉, Ctrl+C를 사용하여 중지할 때까지 ping은 계속 실행됩니다. 예를 들면 다음과 같습니다.

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

라우팅 테이블을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping 명령을 사용하십시오. 이 경우 인터페이스를 지정하지 않고 시스템이 호스트에 대한 경로를 일반적으로 찾을 수 있는지를 테스트하게 됩니다. 시스템은 보통 이 방법을 통해 트래픽을 라우팅하므로 일반적으로 이 테스트를 수행하면 됩니다.

ping 호스트

예를 들면 다음과 같습니다.

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

참고 시간 제한, 반복 횟수, 패킷 크기 및 전송할 데이터 패턴을 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

특정 데이터 인터페이스를 통해 주소 **ping**

특정 데이터 인터페이스를 통한 연결을 테스트하려는 경우, **ping interface** *if_name* 명령을 사용합니다. 이 명령을 사용하여 진단 인터페이스를 지정할 수도 있지만, 가상 관리 인터페이스는 지정할 수 없습니다.

ping interface *if_name host*

예를 들면 다음과 같습니다.

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping tcp 명령을 사용하십시오. TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다.

ping tcp [**interface** *if_name*] *host port*

호스트 및 TCP 포트를 지정해야 합니다.

원하는 경우 인터페이스(ping을 전송하는 데 사용할 인터페이스가 아닌 ping의 소스 인터페이스)를 지정할 수 있습니다. 이 ping 유형은 항상 라우팅 테이블을 사용합니다.

TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다. 예를 들면 다음과 같습니다.

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

참고 TCP ping의 시간 제한, 반복 횟수 및 소스 주소를 지정할 수도 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

호스트에 대한 경로 추적

어떤 IP 주소에 트래픽을 보내는 데 문제가 있을 경우 호스트까지의 경로를 추적하여 네트워크 경로에 문제가 있는지 확인할 수 있습니다. 경로 추적(traceroute)은 잘못된 포트의 UDP 패킷이나 ICMPv6 에코를 목적지로 전송하는 방식입니다. 이러한 패킷이나 에코를 목적지로 전송하는 과정에서 라우터는 ICMP 시간 초과 메시지로 응답하고 경로 추적에 해당 오류를 보고합니다. 각 노드는 3개의 패킷을 수신하므로 노드당 정보 결과를 가져올 수 있는 3번의 기회가 있습니다. **traceroute** CLI 콘솔을 열거나 디바이스 CLI에 로그인하면 사용할 수 있습니다.

참고 데이터 인터페이스(**traceroute**) 또는 가상 관리 인터페이스(**traceroute system**)를 통해 경로를 추적할 수 있는 별도의 명령이 있습니다. 경우에 따라 적절한 명령을 사용해야 합니다.

다음 표에는 출력에 표시될 수 있는 패킷별 결과에 대한 설명이 나와 있습니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 프로토콜에 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

가상 관리 인터페이스를 통해 경로 추적

traceroute system 명령을 사용하십시오.

traceroute system *destination*

호스트는 IPv4/IPv6 주소일 수도 있고 www.example.com과 같은 FQDN(Fully Qualified Domain Name)일 수도 있습니다. 예를 들면 다음과 같습니다.

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
```

```
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

데이터 인터페이스를 통해 경로 추적

traceroute 명령을 사용하십시오.

traceroute *destination*

데이터 인터페이스에 대해 DNS 서버를 구성한 경우 호스트는 IPv4/IPv6 주소일 수도 있고 www.example.com과 같은 정규화된 호스트 이름(FQDN)일 수도 있습니다. 특정 인터페이스에 대해 DNS 서버가 구성되지 않은 경우 **dig** 명령을 사용하여 지정된 FQDN의 IP 주소를 조회합니다. 예를 들면 다음과 같습니다.

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

참고 시간 제한, TTL(Time to Live), 노드당 패킷 수 및 경로 추적의 출발지로 사용할 IP 주소나 인터페이스를 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

트레이스라우트(traceroute)에 Threat Defense 디바이스가 표시되도록 설정

기본적으로 threat defense 디바이스는 트레이스라우트에 홉으로 나타나지 않습니다. 디바이스를 표시하려면 디바이스를 통과하는 패킷에서 TTL(Time to Live)을 줄이고 ICMP 연결 불가 메시지의 속도 제한을 늘려야 합니다. 이렇게 하려면 필요한 서비스 정책 규칙과 기타 옵션을 구성하는 FlexConfig 개체를 생성해야 합니다.

서비스 정책 및 트래픽 클래스의 자세한 설명은 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html에서 제공되는 *Cisco ASA Series* 방화벽 컨피그레이션 가이드를 참조하십시오.

참고 TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다. 트래픽 클래스를 정의할 때는 다음 사항을 고려하십시오.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** TTL을 줄이는 개체를 생성합니다.

a) **+** 버튼을 클릭하여 새 개체를 생성합니다.

b) 개체의 이름을 입력합니다. 예를 들어 **Decrement_TTL**을 입력합니다.

c) **Template(**템플릿**)** 편집기에서 들여쓰기를 포함하여 다음 줄을 입력합니다.

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

명령을 활성화하려면 상위 명령을 포함해 명령에 대해 정확한 하위 모드를 입력해야 하는 것과 마찬가지로, 무효화 템플릿에도 해당 명령을 포함해야 합니다.

무효화 템플릿은 이 개체를 정상적으로 구축한 후에 FlexConfig 정책에서 제거하는 경우에 적용되며, 실패한 구축 중에도 컨피그레이션을 이전 상태로 재설정하기 위해 적용됩니다.

그러므로 이 예시에서 무효화 템플릿은 다음과 같습니다.

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **4** FlexConfig 정책에 개체를 추가합니다.

FlexConfig 정책에서 선택한 개체만 구축됩니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 **+**를 클릭합니다.

c) Decrement_TTL 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

NTP 트러블슈팅

시스템은 시스템이 올바르게 작동하고 이벤트 및 기타 데이터 포인트가 정확하게 처리되도록 정확하고 일관된 시간을 사용합니다. 시스템에서 항상 신뢰할 수 있는 시간 정보를 유지하려면 1개 이상의 NTP(Network Time Protocol) 서버(이상적으로는 3개)를 구성해야 합니다.

디바이스 요약 연결 다이어그램(기본 메뉴에서 **Device(**디바이스**)** 클릭)은 NTP 서버에 대한 연결 상태를 보여줍니다. 이 상태가 노란색 또는 주황색인 경우, 구성된 서버에 연결하는 데 문제가 있는 것입니다. 연결 문제가 지속될 경우(일시적인 문제가 아님), 다음을 수행하십시오.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **NTP**에서 3개 이상의 NTP 서버를 구성합니다. 이것은 요건은 아니지만 3개 이상의 NTP 서버가 있는 경우 신뢰성이 매우 향상됩니다.
- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에 정의되어 있는 관리 인터페이스 IP 주소와 NTP 서버 간의 네트워크 경로가 있는지 확인합니다.
  - 관리 인터페이스 게이트웨이가 데이터 인터페이스인 경우, 기본 경로가 적절하지 않으면 **Device(**디바이스**)** > **Routing(**라우팅**)**에서 NTP 서버에 대한 고정 경로를 구성할 수 있습니다.
  - 명시적 관리 인터페이스 게이트웨이를 설정한 경우, 디바이스 CLI에 로그인하고 **ping system** 명령을 사용하여 각 NTP 서버에 대한 네트워크 경로가 있는지 테스트합니다.
- 디바이스 CLI에 로그인하고 다음 명령을 사용하여 NTP 서버의 상태를 확인합니다.
  - **show ntp**— 이 명령은 NTP 서버와 가용성에 대한 기본 정보를 표시합니다. 단, device manager의 연결 상태는 상태를 나타내는 추가 정보를 사용합니다. 따라서 이 명령이 표시하는 항목과 연결 상태 다이어그램이 표시하는 항목 간에 불일치가 있을 수 있습니다. 이 명령은 CLI 콘솔에서도 실행할 수 있습니다.
  - **system support ntp** - 이 명령에는 **show ntp**의 출력과 함께 표준 NTP 명령인 **ntpq**의 출력(NTP 프로토콜에 문서화됨)도 포함됩니다. NTP 동기화를 확인해야 하는 경우 이 명령을 사용합니다.

    'ntpq -pn 결과' 섹션을 검색합니다. 예를 들면 다음과 같은 내용이 표시될 수 있습니다.

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

    이 예에서 NTP 서버 주소 앞에 있는 +는 잠재적인 후보임을 나타냅니다. 여기에서 별표 *는 현재 시간 소스 피어를 나타냅니다.

    NTPD(NTP 데몬)에서는 각 피어의 8개의 샘플로 구성된 슬라이딩 창을 사용하고 하나의 샘플을 선택하며, 클럭 선택에 따라 올바른 차이머와 잘못된 티커가 결정됩니다. 그런 다음 NTPD에서는 왕복 거리(후보의 오프셋은 왕복 지연의 1/2을 초과하지 않아야 함)를 결정합

니다. 연결 지연, 패킷 손실 또는 서버 문제로 인해 하나 또는 모든 후보가 거부되는 경우, 동기화 시 지연이 길어지며 조정에도 매우 긴 시간이 소요됩니다. 클럭 오프셋과 오실레이터 오류는 클럭 규칙 알고리즘으로 해결해야 하며 이 작업에는 몇 시간이 걸릴 수 있습니다.

참고 refid가 .LOCL인 경우, 이는 피어가 규칙이 없는 로컬 시계임을 나타냅니다. 즉, 시간을 설정하기 위해 로컬 시계만 사용하는 것을 의미합니다. 선택한 피어가 .LOCL인 경우 device manager는 항상 동기화되지 않은 NTP 연결을 노란색으로 표시합니다. 일반적으로, NTP는 더 나은 후보를 사용할 수 있는 경우 .LOCL 후보를 선택하지 않으므로 3개 이상의 서버를 구성해야 합니다.

관리 인터페이스용 **DNS** 문제 해결

관리 인터페이스에서 사용할 DNS 서버를 하나 이상 설정해야 합니다. 이 서버는 스마트 라이선싱, 데이터베이스 업데이트(예: GeoDB, 규칙 및 VDB), 그리고 도메인 이름을 확인해야 하는 기타 작업 등의 서비스에 대한 클라우드 연결용으로 필요합니다.

DNS 서버를 구성하는 과정은 비교적 간단합니다. 디바이스를 처음 구성할 때 사용하는 DNS 서버의 IP 주소만 입력하면 됩니다. 해당 IP 주소는 나중에 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 페이지에서 변경할 수 있습니다.

그러나 시스템은 네트워크 연결 문제 또는 DNS 서버 자체의 문제로 인해 FQDN(Fully Qualified Domain Name)을 확인하지 못할 수 있습니다. 시스템에서 DNS 서버를 사용할 수 없는 경우 문제 식별 및 해결을 위한 다음 작업을 고려하십시오. 일반 DNS 문제 문제 해결도 참조하십시오.

프로시저

단계 **1** 문제가 있는지 확인합니다.

a) SSH를 사용하여 디바이스 CLI에 로그인합니다.

b) **ping system www.cisco.com**을 입력합니다. 다음과 같은 "unknown host(알 수 없는 호스트)" 메시지가 표시되는 경우 시스템이 도메인 이름을 확인할 수 없는 것입니다. ping이 성공하는 경우에는 확인이 완료되었으며 DNS가 작동 중인 것입니다. ping을 중지하려면 Ctrl+C를 누릅니다.

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

참고 중요한 것은 **ping** 명령에 **system** 키워드가 포함되어야 한다는 것입니다. **system** 키워드에서는 관리 IP 주소(관리 DNS 서버를 사용하는 유일한 인터페이스)를 통해 ping을 전송합니다. www.cisco.com에 대해 ping을 실행하는 것도 유용한 옵션입니다. 스마트 라이선싱 및 업데이트를 수행하려면 해당 서버로의 경로가 필요하기 때문입니다.

단계 **2** 관리 인터페이스의 컨피그레이션을 확인합니다.

a) **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 다음을 확인합니다. 변경을 수행하는 경우 **Save(**저장**)**를 클릭하면 변경 사항이 즉시 적용됩니다. 관리 주소를 변경하는 경우 다시 연결하여 다시 로그인해야 합니다.

- 관리 네트워크에 대한 게이트웨이 IP 주소가 정확합니다. 게이트웨이로 데이터 인터페이스를 사용 중이라면 후속 단계에서는 해당 컨피그레이션을 확인합니다.
- 게이트웨이로 데이터 인터페이스를 사용하고 있지 않다면 관리 IP 주소/서브넷 마스크와 게이트웨이 IP 주소가 같은 서브넷에 있는지 확인합니다.

b) 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 클릭하고 올바른 DNS 서버가 구성되어 있는지 확인합니다.

네트워크 에지에서 디바이스를 구축하는 경우 사용 가능한 DNS 서버에 대한 서비스 제공자의 특정 요구 사항이 있을 수 있습니다.

c) 게이트웨이로 데이터 인터페이스를 사용 중이라면 필요한 경로가 있는지 확인합니다.

0.0.0.0의 경우 기본 경로가 필요합니다. 기본 경로에 대해 게이트웨이를 통해 DNS 서버를 사용할 수 없는 경우에는 추가 경로가 필요할 수 있습니다. 기본적으로 발생 가능한 상황은 다음의 두 가지입니다.

- DHCP를 사용하여 외부 인터페이스의 주소를 가져오는 경우 **Obtain Default Route using DHCP(DHCP**를 사용하여 기본 경로 얻기**)** 옵션을 선택했다면 device manager에 기본 경로가 표시되지 않습니다. SSH에서 **show route**(을)를 입력하고 0.0.0.0에 대한 경로가 있는지 확인합니다. 이 컨피그레이션은 외부 인터페이스의 기본 컨피그레이션이므로 기본적으로는 이 상황이 발생할 가능성이 높습니다. 외부 인터페이스의 컨피그레이션을 확인하려면 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동합니다.
- 외부 인터페이스에서 고정 IP 주소를 사용 중이거나 DHCP에서 기본 경로를 얻지 않는 경우에는 **Device(**디바이스**)** > **Routing(**라우팅**)**을 엽니다. 기본 경로에 대해 정확한 게이트웨이를 사용하고 있는지 확인합니다.

기본 경로를 통해 DNS 서버에 연결할 수 없는 경우에는 **Routing(**라우팅**)** 페이지에서 해당 서버로의 정적 경로를 정의해야 합니다. 직접 연결된 네트워크(시스템의 데이터 인터페이스에 직접 연결된 네트워크)의 경우에는 경로를 추가하면 안 됩니다. 시스템은 해당 네트워크로 자동 라우팅할 수 있기 때문입니다.

또한 잘못된 인터페이스를 통해 서버로 트래픽을 잘못 전송하는 정적 경로가 없는지도 확인합니다.

d) 구축 버튼에 구축하지 않은 변경 사항이 있음이 표시되는 경우 지금 구축하고 구축이 완료될 때까지 기다립니다.

e) **ping system www.cisco.com**을 다시 테스트합니다. 문제가 계속 발생하면 다음 단계로 계속 진행합니다.

단계 **3** SSH 세션에서 **dig www.cisco.com**을 입력합니다.

- **dig** 실행 시 DNS 서버에서 응답을 받았음을 표시하는데 서버가 이름을 찾을 수 없는 경우, DNS는 정확하게 컨피그레이션되어 있지만 사용 중인 DNS 서버에 FQDN의 주소가 없는 것입니다. 이 오류는 NXDOMAIN 상태로 표시됩니다. 응답은 다음과 같이 표시됩니다.

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

  해결 방법: 이 경우 다른 DNS 서버를 구성하거나 확인해야 하는 FQDN을 확인할 수 있도록 현재 DNS 서버를 업데이트해야 합니다. 네트워크 관리자나 ISP와 협의하여 네트워크에 대해 작동하는 DNS 서버의 IP 주소를 얻으십시오.

- 연결 시간 초과가 발생한 경우 시스템이 DNS 서버에 연결할 수 없거나, 모든 DNS 서버가 현재 중단되어 응답하지 않는 것입니다(가능성은 낮음). 다음 단계를 계속합니다.

단계 **4** **traceroute system** *DNS_server_ip_address* 명령을 사용하여 DNS 서버로의 경로를 추적합니다.

예를 들어 DNS 서버가 10.100.10.1인 경우 다음 명령을 입력합니다.

```
> traceroute system 10.100.10.1
```

발생 가능한 결과는 다음과 같습니다.

- traceroute가 완료되고 DNS 서버에 연결됩니다. 이 경우 DNS 서버로의 경로가 실제로 있으며 시스템이 DNS 서버에 연결할 수 있는 것입니다. 따라서 라우팅 문제는 없습니다. 하지만 이 서버에 대한 DNS 요청에서 응답은 수신되지 않습니다.

  해결 방법: 경로 내에 있는 라우터나 방화벽이 UDP/53(DNS에 사용되는 포트) 트래픽을 삭제하고 있을 수 있습니다. 다른 네트워크 경로에서 DNS 서버에 연결해 볼 수 있습니다. 트래픽을 차단하는 노드를 확인한 다음 시스템 관리자와 협의하여 액세스 규칙을 변경해야 하므로, 이 문제는 해결하기가 어렵습니다.

- traceroute가 어떤 노드에도 연결할 수 없습니다. 이 경우 결과는 다음과 같이 표시됩니다.

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
```

```
 1  * * *
 2  * * *
 3  * * *
(and so forth)
```

해결 방법: 이 경우에는 시스템 내에 라우팅 문제가 있는 것입니다. 게이트웨이 IP 주소에 **ping system**을 실행해 보십시오. 이전 단계에서 설명한 것처럼 관리 인터페이스의 컨피그레이션을 다시 확인하여 필요한 게이트웨이와 경로가 구성되어 있는지 확인합니다.

- traceroute가 노드 몇 개를 통과한 후 경로를 더 이상 확인하지 못합니다. 이 경우 결과는 다음과 같이 표시됩니다.

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
 2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
 3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
 4  * * *
 5  * * *
 6  * * *
```

해결 방법: 이 경우에는 마지막 노드에서 라우팅에 장애가 발생하는 것입니다. 그러므로 시스템 관리자와 협의하여 해당 노드에 정확한 경로를 설치해야 할 수 있습니다. 그러나 해당 노드를 통과하여 DNS 서버에 연결하는 경로를 의도적으로 삭제한 경우에는 게이트웨이를 변경하거나 DNS 서버로 트래픽을 라우팅할 수 있는 라우터를 가리키도록 정적 경로를 직접 생성해야 합니다.

CPU 및 메모리 사용량 분석

CPU 및 메모리 사용량에 대한 시스템 레벨 정보를 보려면 **Monitoring(**모니터링**)** > **System(**시스템**)**을 선택하고 CPU 및 메모리 막대 그래프를 찾습니다. 이 그래프에는 CLI에서 **show cpu system** 및 **show memory system** 명령을 사용해 수집한 정보가 표시됩니다.

CLI 콘솔을 열거나 CLI에 로그인하면 이러한 명령의 추가 버전을 사용하여 다른 정보를 확인할 수 있습니다. 일반적으로는 사용량과 관련하여 지속적인 문제가 발생하는 경우나 Cisco TAC(Technical Assistance Center)의 지침이 있는 경우에만 이 정보를 확인하면 됩니다. 자세한 정보는 대부분 복잡하므로 TAC의 해석이 필요합니다.

검사할 수 있는 몇 가지 주요 정보는 다음과 같습니다. 이러한 명령에 대한 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html의 Cisco Firepower Threat Defense 명령 참조에서 확인할 수 있습니다.

- **show cpu** 데이터 플레인 CPU 사용률을 표시합니다.
- **show cpu core** 각 CPU 코어의 사용량을 개별적으로 표시합니다.
- **show cpu detailed** 코어당/전체 데이터 플레인 CPU 사용량을 추가로 표시합니다.
- **show memory** 데이터 플레인 메모리 사용량을 표시합니다.

참고 위에 나와 있지 않은 일부 키워드의 경우 **cpu** 또는 **memory** 명령을 사용하여 프로파일링 또는 기타 기능을 먼저 설정해야 합니다. 이러한 기능은 TAC 지침에 따라 사용하십시오.

로그 보기

시스템은 다양한 작업에 대한 정보를 로깅합니다. **system support view-files** 명령을 사용하여 시스템 로그를 열 수 있습니다. Cisco TAC(Technical Assistance Center)와 작업할 때 이 명령을 사용하면 TAC에서 출력 해석을 지원할 수 있으며 확인해야 하는 적절한 로그를 선택할 수 있습니다.

이 명령을 실행하면 로그 선택을 위한 메뉴가 표시됩니다. 다음 명령을 사용하여 마법사를 탐색합니다.

- 하위 디렉터리로 변경하려면 디렉터리의 이름을 입력하고 Enter 키를 누릅니다.
- 볼 파일을 선택하려면 프롬프트에서 **s**를 입력합니다. 그러면 파일 이름을 입력하라는 메시지가 표시됩니다. 대소문자를 구분하여 전체 이름을 입력해야 합니다. 파일 목록에는 로그의 크기가 표시됩니다. 매우 큰 로그의 경우 열기 전에 크기를 고려해야 합니다.
- --More(자세히)--가 표시될 때 스페이스바를 누르면 다음 로그 항목 페이지가 표시되고 Enter 키를 누르면 다음 로그 항목만 표시됩니다. 로그의 끝에 도달하면 메인 메뉴로 이동됩니다. --More(자세히)-- 줄에는 로그의 크기와 로그를 확인한 빈도가 표시됩니다. 전체 로그 페이지를 확인하지 않으려는 경우 **Ctrl+C**를 사용하여 로그를 닫고 명령을 종료합니다**.**
- 메뉴의 구조에서 한 레벨 위로 이동하려면 **b**를 입력합니다.

새로 추가되는 메시지를 확인할 수 있도록 로그를 열어 두려면 **system support view-files** 대신 **tail-logs** 명령을 사용합니다.

다음 예에서는 시스템 로그인 시도를 추적하는 cisco/audit.log 파일을 확인하는 방법을 보여줍니다. 파일 목록은 맨 위의 디렉터리에서 시작되며, 그 아래에는 현재 디렉터리의 파일 목록이 표시됩니다.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
```

```
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

트러블슈팅 파일 생성

문제 보고서를 제출할 때는 Cisco TAC(Technical Assistance Center) 담당자가 시스템 로그 정보 제출을 요청할 수 있습니다. 담당자는 이 정보를 통해 문제를 보다 쉽게 진단할 수 있습니다. 별도의 요청이 없으면 진단 파일을 제출하지 않아도 됩니다.

다음 절차에서는 진단 파일을 생성하고 다운로드하는 방법을 설명합니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** **Troubleshooting(**트러블슈팅**)**에서 **Request file to be Created(**파일 생성 요청**)** 또는 **Re-Request File to be Created(**파일 생성 재요청**)**(이전에 파일 생성을 요청한 경우)를 클릭합니다.

시스템에서 진단 파일 생성이 시작됩니다. 다른 페이지로 이동했다가 돌아와서 상태를 확인할 수 있습니다. 파일이 준비되면 파일 생성 날짜와 시간이 다운로드 버튼과 함께 표시됩니다.

단계 **3** 파일이 준비되면 다운로드 버튼을 클릭합니다.

브라우저 표준 다운로드 방법을 통해 파일이 워크스테이션에 다운로드됩니다.

일반적이지 않은 관리 작업

다음 항목에서는 수행하더라도 자주 수행하지는 않는 작업에 관해 설명합니다. 이러한 모든 작업을 수행하면 디바이스 컨피그레이션이 지워집니다. 이러한 변경을 수행하기 전에 디바이스가 현재 프로덕션 네트워크에 중요한 서비스를 제공하고 있지 않은지 확인합니다.

방화벽 모드 변경

threat defense 방화벽은 라우팅 모드 또는 투명 모드에서 실행될 수 있습니다. 라우팅 모드 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

로컬 device manager는 라우팅 모드만 지원합니다. 그러나 투명 모드에서 디바이스를 실행해야 하는 경우에는 방화벽 모드를 변경하고 management center를 사용하여 디바이스 관리를 시작할 수 있습니다. 반면 투명 모드 디바이스는 라우팅 모드로 변환할 수 있으며, 그 후에는 로컬 관리자를 사용하여 해당 디바이스를 구성할 수 있습니다. management center를 사용하여 라우팅 모드 디바이스를 관리할 수도 있습니다.

로컬 또는 원격 관리와 관계없이 모드를 변경하려면 디바이스 CLI를 사용해야 합니다.

다음 절차에서는 로컬 관리자를 사용 중이거나 사용하려는 경우 모드를 변경하는 방법을 설명합니다.

⚠

주의 방화벽 모드를 변경하면 디바이스 컨피그레이션이 지워지며 시스템이 기본 컨피그레이션으로 돌아갑니다. 그러나, 관리 IP 주소 및 호스트 이름은 유지됩니다.

시작하기 전에

투명 모드로 변환하는 경우 방화벽 모드를 변경하기 전에 management center를 설치합니다.

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하고 원격 관리로 전환하기 전에 device manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화의 내용을 참조하십시오.

디바이스가 고가용성으로 컨피그레이션된 경우에는 먼저 디바이스 관리자(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 컨피그레이션을 해제해야 합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** SSH 클라이언트를 사용하여 관리 **IP** 주소에 대한 연결을 열고 구성 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

관리 IP 주소에 연결되어 있는 동안에는 이 프로세스를 따라야 합니다. device manager를 사용할 때는 데이터 인터페이스의 IP 주소를 통해 디바이스를 관리할 수 있습니다. 그러나 디바이스를 원격으로 관리하려면 관리 물리적 포트 및 관리 IP 주소를 사용해야 합니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. device manager의 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 에서 주소와 게이트웨이를 구성합니다. (CLI에서는 **configure network ipv4/ipv6 manual** 명령을 사용하십시오.)

  참고 관리 IP 주소에 대해 외부 게이트웨이를 사용하고 있는지 확인합니다. 원격 관리자를 사용할 때는 데이터 인터페이스를 게이트웨이로 사용할 수 없습니다.

단계 **2** 라우팅 모드에서 투명 모드로 변경하고 원격 관리를 사용하려면 다음을 수행합니다.

a) 로컬 관리를 비활성화하고 관리자 모드로 진입하지 않습니다.

활성 관리자가 있으면 방화벽 모드를 변경할 수 없습니다. 관리자를 제거하려면 **configure manager delete** 명령을 사용합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 방화벽 모드를 투명으로 변경합니다.

configure firewall transparent

예제:

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 원격 관리자를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}에서는 이 디바이스를 관리하는 management center의 DNS 호스트 이름이나 IP 주소(IPv4 또는 IPv6)를 지정합니다. management center의 주소를 직접 지정할 수 없으면 **DONTRESOLVE**(을)를 사용합니다. **DONTRESOLVE**(을)를 사용하는 경우 *nat_id*가 필요합니다.
- *regkey*는 디바이스를 management center에 등록하는 데 필요한 고유 영숫자 등록 키입니다.
- *nat_id*는 management center와 장치 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다.

예를 들어 등록 키 **secret**을 사용하여 192.168.0.123에서 관리자를 사용하려면 다음과 같이 입력합니다.

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

d) management center에 로그인하여 디바이스를 추가합니다.

자세한 내용은 management center 온라인 도움말을 참조하십시오.

단계 **3** 투명 모드에서 라우팅 모드로 변경하고 로컬 관리로 변환하려면 다음을 수행합니다.

a) management center에서 디바이스를 등록 취소합니다.

b) threat defense 디바이스 CLI에 액세스합니다. 콘솔 포트에서 액세스하는 것이 좋습니다.

모드를 변경하면 컨피그레이션이 지워지므로 관리 IP 주소는 기본값으로 되돌아갑니다. 따라서 모드를 변경한 후에는 관리 IP 주소에 대한 SSH 연결이 끊길 수 있습니다.

c) 방화벽 모드를 라우팅으로 변경합니다.

configure firewall routed

예제**:**

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) 로컬 관리자를 활성화합니다.

configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

컨피그레이션 재설정

컨피그레이션을 처음부터 다시 시작하려는 경우 시스템 컨피그레이션을 공장 기본값으로 재설정할 수 있습니다. 컨피그레이션을 직접 재설정할 수는 없지만 관리자를 삭제했다가 추가하면 컨피그레이션이 지워집니다.

컨피그레이션을 지우고 백업을 복구하려는 경우에는 복원할 백업 복사본을 이미 다운로드한 상태여야 합니다. 시스템을 재설정한 후에 백업을 복원할 수 있도록 해당 복사본을 업로드해야 합니다.

시작하기 전에

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하기 전에 device manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화의 내용을 참조하십시오.

장치가 고가용성으로 구성된 경우에는 먼저 device manager(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 구성을 해제해야 합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** SSH 클라이언트를 사용하여 관리 IP 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

단계 **2** 관리자를 제거하려면 **configure manager delete** 명령을 사용합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **3** 로컬 관리자를 구성합니다.

configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다. 컨피그레이션을 지우면 디바이스 설정 마법사를 완료하라는 메시지가 표시됩니다.

Secure Firewall 3100에서 SSD 핫스왑

SSD 2개를 설치한 경우 부팅 시 RAID를 형성합니다. 방화벽의 전원이 켜져 있는 동안 threat defense CLI에서 다음 작업을 수행할 수 있습니다.

- SSD 중 하나를 핫 스왑 - SSD에 결함이 있는 경우 교체할 수 있습니다. SSD가 하나뿐인 경우 방화벽이 켜져 있는 동안에는 SSD를 제거할 수 없습니다.
- SSD 중 하나 제거 - SSD가 2개인 경우 하나를 제거할 수 있습니다.
- 두 번째 SSD 추가 - SSD가 한 개인 경우 두 번째 SSD를 추가하여 RAID를 구성할 수 있습니다.

⚠

주의 이 절차를 사용하여 RAID에서 SSD를 먼저 분리하지 않은 상태에서 SSD를 분리하지 마십시오. 데이터가 손실될 수 있습니다.

프로시저

단계 **1** SSD 중 하나를 분리합니다.

a) RAID에서 SSD를 분리합니다.

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 키워드는 RAID에서 SSD를 제거하고, 자체 암호화 디스크 기능을 비활성화하며, SSD의 보안 기반 초기화를 수행합니다. RAID에서 SSD만 제거하고 데이터를 그대로 유지하려는 경우 **remove** 키워드를 사용할 수 있습니다.

예제**:**

```
> configure raid remove-secure local-disk 2
```

b) SSD가 인벤토리에 더 이상 표시되지 않을 때까지 RAID 상태를 모니터링합니다.

show raid

SSD가 RAID에서 제거되면 작동성 및 드라이브 상태가 저하됨으로 표시됩니다. 두 번째 드라이브는 더 이상 멤버 디스크로 나열되지 않습니다.

예제:

```
> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 operable
Presence:                    equipped
Lifecycle:                   available
Drive State:                 optimal
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    0
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                 nvme1n1
Disk State:                  in-sync
Disk Slot:                   2
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 degraded
Presence:                    equipped
Lifecycle:                   available
Drive State:                 degraded
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    1
Sync Speed:                  none

RAID member Disk:
```

```
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 섀시에서 SSD를 물리적으로 분리합니다.

단계 **2** SSD를 추가합니다.

a) SSD를 빈 슬롯에 물리적으로 추가합니다.

b) RAID에 SSD를 추가합니다.

configure raid add local-disk {**1** | **2**}

방화벽이 완전히 작동하는 동안 새 SSD를 RAID에 동기화하는 작업을 완료하는 데 몇 시간이 걸릴 수 있습니다. 재부팅해도 전원이 켜지면 동기화가 계속됩니다. **show RAID** 명령을 사용하여 상태를 표시합니다.

이전에 다른 시스템에서 사용된 SSD를 설치했지만 여전히 잠겨 있는 경우 다음 명령을 입력합니다.

configure raid add local-disk {**1** | **2**} *psid*

*PSID*는 SSD 후면에 부착된 레이블에 인쇄되어 있습니다. 또는 시스템을 재부팅할 수 있습니다. 그러면 SSD가 다시 포맷되고 RAID에 추가됩니다.