Cisco FXOS 릴리스 노트, 2.1(1)

최초 발행일: 2017년 1월 23일 화요일
최종 수정: 2017년 6월 14일

이 문서는 Cisco Firepower eXtensible 운영 체제 2.1(1)에 대한 릴리스 정보를 제공합니다.

이 릴리스 노트는 설명서 로드맵에 있는 다른 문서의 보충 자료로 활용하십시오.

http://www.cisco.com/go/firepower9300-docs

http://www.cisco.com/go/firepower4100-docs

참고: 사용자 설명서의 온라인 버전은 최초 릴리스 이후 때때로 업데이트됩니다. 따라서 Cisco.com에 있는 설명서의 내용이 제품과 함께 제공된 상황별 도움말의 내용에 우선합니다.

이 문서는 다음 섹션으로 구성되었습니다.

도입

Cisco Firepower Security Appliance는 네트워크 및 콘텐츠 보안 솔루션을 위한 차세대 플랫폼입니다. Cisco Firepower Security Appliance는 Cisco ACI(Application Centric Infrastructure) 보안 솔루션에 포함되며 확장성, 제어 일관성 및 관리 간소화를 위해 구축된 민첩한 개방형 보안 플랫폼을 제공합니다.

Cisco Firepower Security Appliance에서 제공하는 기능은 다음과 같습니다.

- 모듈형 섀시 기반 보안 시스템 - 고성능의 유연한 입/출력 컨피그레이션 및 확장성을 제공합니다.
- Firepower Chassis Manager - 그래픽 사용자 인터페이스에서 현재 섀시 상태를 간결하게 시각적으로 보여주며, 간단하게 섀시 기능을 구성할 수 있도록 지원합니다.
- FXOS CLI - 명령 기반 인터페이스에서 각종 기능을 구성하고 섀시 상태를 모니터링하며 고급 트러블슈팅 기능에 액세스할 수 있습니다.
- FXOS REST API - 사용자가 프로그래밍 방식으로 섀시를 구성하고 관리할 수 있습니다.

새로운 기능

FXOS 2.1.1.83의 새로운 기능

Cisco Firepower eXtensible 운영 체제 2.1.1.83은 이전 릴리스의 기능과 함께 다음 기능도 새롭게 제공합니다.

- 보안 모듈 어댑터 검증을 추가로 지원할 뿐 아니라 어댑터의 부팅 이미지를 보고 업데이트하기 위한 CLI 명령을 제공합니다.

  참고: FXOS 2.1.1.83을 설치하면 보안 모듈 어댑터의 펌웨어를 업데이트하라는 중대한 오류 메시지가 나타날 수 있습니다. 자세한 내용은 어댑터 부트로더 업그레이드, 5페이지 섹션을 참조해 주십시오.

- Cisco Interactive Debug라고도 하는 Secure Unlock은 새로운 서비스 편의성 기능으로서 Firepower 9300 및 Firepower 4100 Series 보안 어플라이언스의 Supervisor Module에서 안전하게 Linux 프롬프트에 액세스할 수 있는 방법을 구현합니다.

  참고: Secure Unlock 기능을 사용하려면 먼저 보안 어플라이언스에 펌웨어 패키지 1.0.12 이상이 설치되어야 합니다. 펌웨어 패키지 버전을 확인하고 필요 시 펌웨어를 업그레이드하는 방법에 대해서는 *Cisco FXOS CLI 컨피그레이션 가이드 2.1(1)* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드2.1(1)* (http://www.cisco.com/go/firepower9300-config)의 "펌웨어 업그레이드" 항목을 참조하십시오.

- 여러 문제점 해결(FXOS 2.1.1.83에서 해결된 버그, 22페이지 참조).

FXOS 2.1.1.77의 새로운 기능

Cisco Firepower eXtensible 운영 체제 2.1.1.77은 이전 릴리스의 기능과 함께 다음 기능도 새롭게 제공합니다.

- 여러 문제점 해결(FXOS 2.1.1.77에서 해결된 버그, 22페이지 참조).

FXOS 2.1.1.73의 새로운 기능

Cisco Firepower eXtensible 운영 체제 2.1.1.73은 이전 릴리스의 기능과 함께 다음 기능도 새롭게 제공합니다.

- 모든 Firepower 4100 및 9300 디바이스의 Firepower Threat Defense에서 Radware DefensePro(vDP)의 서비스 체인을 지원합니다.

  참고: Radware DefensePro(vDP)와 Firepower Threat Defense는 FXOS 2.1.1.64 이상에서 지원되지만, FXOS 2.1.1.73과 같은 시점에 출시된 Radware vDP 버전 8.10.01.17-2가 필요합니다. 버전 호환성에 대한 자세한 내용은 *Cisco FXOS 호환성* (http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html)을 참조하십시오.

- 여러 문제점 해결(FXOS 2.1.1.73에서 해결된 버그, 23페이지 참조).

FXOS 2.1.1.64의 새로운 기능

Cisco Firepower eXtensible 운영 체제 2.1.1.64에서 다음 새로운 기능을 선보입니다.

- Firepower Chassis Manager 또는 FXOS CLI를 통해 Call Home URL을 제거하는 새로운 옵션.
- Firepower Chassis Manger를 사용하여 콘솔 인증을 구성할 수 있습니다.
- Firepower Chassis Manager를 사용하여 AAA 인증 폴백 방식을 보고 구성할 수 있습니다.
- FXOS에서 시스템에 설치된 CSP 파일의 무결성을 확인합니다.
- Firepower Threat Defense 6.2 지원.
- ASA 9.7(1) 지원.
- 모든 Firepower 4100 및 9300 디바이스의 Firepower Threat Defense에서 Radware DefensePro(vDP)의 서비스 체인을 지원합니다.
- Firepower 4100 Series Security Appliance에서의 1GB FTW 네트워크 모듈 지원.
- Firepower 9300 Security Appliance에서의 HVDC(high-voltage DC) 전원 공급 모듈 지원.
- Firepower Threat Defense 6.2 이상을 사용하는 섀시 간 클러스터링 지원.
- 사이트 간 클러스터링 개선.
- FXOS Chassis Manager를 사용하여 FIPs/Common Criteria 모드에서 FIPS(Federal Information Processing Standard) 140-2 및 Common Criteria 보안 인증에 대한 컴플라이언스를 지원할 수 있습니다.
- FXOS 2.1(1)은 새로운 기능 및 각종 향상된 기능을 통해 UC-APL(Unified Capabilities Approved Product List) 보안 인증에 대한 컴플라이언스를 지원합니다.
  - Firepower Chassis Manager를 사용하여 FIPS/CC 모드 활성화/비활성화
  - Firepower Chassis Manager를 통해 관리 ACL(ip-block) 구성
  - Firepower Chassis Manager를 통해 SSH 서버 - MAC 인증 구성
  - Firepower Chassis Manager를 통해 SSH 서버 - 암호화 알고리즘 구성
  - 로그인 알림
  - 주기적으로 CRL 목록 업데이트
  - 클라이언트 인증서 인증
- NTP 서버 인증을 활성화할 수 있습니다.
- FXOS는 세션 사용에 관계없이 Firepower Chassis Manager 세션을 종료하는 절대 시간 초과 값을 갖습니다. 절대 시간 초과의 기본값은 60분이며 FXOS CLI를 통해 변경할 수 있습니다. 자세한 내용은 FXOS CLI 컨피그레이션 가이드를 참조하십시오.
- 데이터 포트 - 채널 인라인 쌍에 대한 정보가 Firepower Threat Defense에서 FXOS로 전달됩니다.

- Firepower Chassis Manager를 사용하여 논리 디바이스의 일부가 아닌 애플리케이션 인스턴스를 삭제할 수 있습니다.
- 패킷 캡처 기능 향상:
  - IPv6 주소 기준 필터링.
  - 세션에 대한 스냅 길이 지정.
  - 1MB ~ 2GB의 세션 크기 지원. 이전 릴리스에서는 256MB ~ 2GB였습니다.
  - 모든 패킷 캡처 세션을 삭제하는 명령.
- QoS 향상:
  - FXOS에서 구성된 port-channel에 대한 LACP 제어 트래픽 우선 순위 지정.
  - 내부 제어 평면 트래픽에 우선 순위를 두도록 MIO CPU 포트 대기열 설정 수정.
- ASA 페일오버 쌍에 대한 라이선싱 변경. 액티브 유닛만 라이선스 엔타이틀먼트를 요청합니다. 이전에는 두 유닛 모두 라이선스 엔타이틀먼트를 요청했습니다.
- 여러 문제점 해결(Resolved Bugs in FXOS 2.1.1.64, 23페이지 참조).

소프트웨어 다운로드

다음 URL 중 하나에서 FXOS 및 지원되는 애플리케이션에 대한 소프트웨어 이미지를 다운로드할 수 있습니다.

- Firepower 9300 — https://software.cisco.com/download/type.html?mdfid=286287252
- Firepower 4100 — https://software.cisco.com/download/navigator.html?mdfid=286305164

특정 버전 또는 FXOS에서 지원되는 애플리케이션에 대해서는 다음 URL의 *Cisco FXOS 호환성* 가이드를 참조하십시오. http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

중요 참고 사항

- ASA 9.7부터 페일오버 쌍에 대한 스마트 라이선싱 컨피그레이션의 동작이 변경되었습니다. ASA 페일오버 쌍을 9.6 이하 버전에서 9.7 이상 버전으로 업그레이드하는 경우 다음 단계를 수행하여 디바이스의 엔타이틀먼트를 업그레이드해야 합니다(액티브 유닛은 디바이스 A, 스탠바이 유닛은 디바이스 B).

  a. 현재 스탠바이 유닛(디바이스 B)에 엔타이틀먼트가 구성된 경우 스탠바이 유닛에서 그 컨피그레이션을 제거하고 액티브 유닛(디바이스 A)에 동일한 엔타이틀먼트를 구성합니다. 상황 개수에서는 액티브 유닛과 스탠바이 유닛의 값을 합한 총 개수를 액티브 유닛에서 요청합니다.

  b. 스탠바이 유닛(디바이스 B)을 업그레이드한 다음 다시 페일오버 쌍에 스탠바이 유닛으로 합류시킵니다. 이제는 디바이스 B에 스마트 라이선스 컨피그레이션이 없습니다. 자세한 내용은 ASA 페일오버 쌍 업그레이드, 10페이지를 참조하십시오.

  c. 액티브 유닛(디바이스 A) 업그레이드. 업그레이드 과정에서 디바이스 A가 페일오버 쌍에서 벗어나고 디바이스 B가 액티브 유닛이 됩니다. 디바이스 A가 업그레이드되는 동안 디바이스 A에 구성되었던 모든 엔타이틀먼트가 디바이스 B에서 구성되어야 합니다.

  d. 디바이스 A는 업그레이드를 마치면 다시 페일오버 쌍에 스탠바이 유닛으로 합류합니다. 이제는 스탠바이 유닛이므로 모든 엔타이틀먼트를 해제하고 스마트 라이선스 컨피그레이션을 제거합니다.

     디바이스 B(액티브)에서 디바이스 A(스탠바이)로 컨피그레이션을 동기화하는 과정에서 디바이스 A는 디바이스 B로부터 스마트 라이선스 컨피그레이션을 받아 캐시에 저장합니다. 따라서 혹시 액티브 유닛이 되더라도 어떤 엔타이틀먼트를 요청해야 하는지 알고 있습니다.

- Firepower 100G Network Module과 Firepower 9300 Security Appliance를 함께 사용하려면 이 보안 어플라이언스에 펌웨어 패키지 1.0.10 이상이 설치되어 있어야 합니다. 펌웨어 패키지 버전을 확인하고 필요 시 펌웨어를 업그레이드하는 방법에 대해서는 *Cisco FXOS CLI 컨피그레이션 가이드 2.1(1)* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드 2.1(1)* (http://www.cisco.com/go/firepower9300-config)의 "펌웨어 업그레이드" 항목을 참조하십시오.
- FXOS 1.1(3)부터 port-channel의 동작이 변경되었습니다. FXOS 1.1(3) 이상 릴리스에서는 port-channel을 생성할 때 기본적으로 lacp cluster-detach로 구성되며 물리적 링크가 작동 중인 경우에도 상태가 다운된 것으로 표시됩니다. port-channel은 다음 상황에서 cluster-detach 모드가 됩니다.
  - port-channel의 port-type은 cluster 또는 mgmt 중 하나로 설정됩니다.
  - port-channel은 클러스터의 일부인 논리적 디바이스에 대한 데이터 포트로 추가되며 보안 모듈 하나 이상이 클러스터에 조인됩니다.

  port-channel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, port-channel은 cluster-detach 모드로 전환됩니다.

어댑터 부트로더 업그레이드

FXOS 2.1.1.83은 보안 어플라이언스의 보안 모듈 어댑터를 확인하는 테스트를 추가로 수행합니다. FXOS 2.1.1.83 설치 후 보안 어플라이언스에서 보안 모듈 어댑터의 펌웨어를 업데이트해야 한다는 다음 중대 오류 메시지가 나타날 수 있습니다.

```
Critical  F1715    2017-05-11T11:43:33.121    339561 Adapter 1 on Security Module 1
requires a critical firmware upgrade. Please see Adapter Bootloader Upgrade instructions
in the FXOS Release Notes posted with this release.
```

위와 같은 메시지가 표시될 경우 다음 절차에 따라 어댑터의 부트 이미지를 업데이트합니다.

1. Firepower Security Appliance의 FXOS CLI에 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).
2. 부트 이미지를 업데이트하고 있는 어댑터에 대한 어댑터 모드를 시작합니다.

   ```
   fxos-chassis# scope adapter 1/security_module_number/adapter_number
   ```

3. 가용 어댑터 이미지를 보고 fxos-m83-8p40-cruzboot.4.0.1.62.bin이 설치 가능함을 확인하려면 **show image** 명령을 사용합니다.

   ```
   fxos-chassis /chassis/server/adapter # show image
   Name                                       Type                 Version
   ------------------------------------------ -------------------- -------
   fxos-m83-8p40-cruzboot.4.0.1.62.bin        Adapter Boot         4.0(1.62)
   fxos-m83-8p40-vic.4.0.1.51.gbin            Adapter              4.0(1.51)
   ```

4. 어댑터 부트 이미지를 버전 4.0.1.62로 업데이트하려면 **update boot-loader** 명령을 사용합니다.

   ```
   fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
   Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
   adapter to become UNUSABLE!
   After upgrade has completed, blade will be power cycled automatically
   fxos-chassis /chassis/server/adapter* # commit-buffer
   ```

5. 업데이트 상태를 모니터링하려면 **show boot-update status** 명령을 사용합니다.

   ```
   fxos-chassis /chassis/server/adapter # show boot-update status
   State: Updating
   fxos-chassis /chassis/server/adapter # show boot-update status
   State: Ready
   ```

6. 업데이트가 성공했음을 확인하려면 **show version detail** 명령을 사용합니다.

   참고: 실제 **show version detail** 출력이 다음 예와 다를 수도 있습니다. 그러나 Bootloader-Update-Status가 “Ready”이고 Bootloader-Vers가 4.0(1.62)임을 확인하십시오.

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
    Running-Vers: 5.0(1.2)
    Package-Vers: 2.1(1.83)
    Update-Status: Ready
    Activate-Status: Ready
    Bootloader-Update-Status: Ready
    Startup-Vers: 5.0(1.2)
    Backup-Vers: 4.0(1.55)
    Bootloader-Vers: 4.0(1.62)
```

시스템 요구 사항

다음 브라우저를 사용하여 Firepower Chassis Manager에 액세스할 수 있습니다.

- Mozilla Firefox – 버전 42 이상
- Google Chrome – 버전 47 이상
- Microsoft Internet Explorer – 버전 11 이상

FXOS 2.1(1)에서 Mozilla Firefox 버전 42, Google Chrome 버전 47, Internet Explorer 버전 11을 사용하여 테스트했습니다. 이 브라우저의 향후 버전도 제대로 작동할 것으로 예상합니다. 그러나 브라우저 관련 문제가 있을 경우 검증된 버전 중 하나로 돌아가는 것이 좋습니다.

업그레이드 지침

Firepower 9300 또는 Firepower 4100 Series Security Appliance에서 FXOS 2.1(1) 빌드를 실행 중이라면 FXOS 2.1(1.83)로 업그레이드할 수 있습니다.

더 오래된 버전의 FXOS를 실행 중이라면 업그레이드 경로에서 해당 시스템을 FXOS 2.1(1.83)로 업그레이드하는 방법을 참조하십시오.

업그레이드 경로

이전 릴리스에서 이번 릴리스로 이전하는 데 필요한 업그레이드 경로에 대해 다음 표를 참조하십시오. 특정 릴리스로 업그레이드하는 것에 대해서는 해당 릴리스의 릴리스 노트 문서를 참조하십시오.

http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html

업그레이드 과정에서 이미 설치된 논리 디바이스에 대한 애플리케이션 버전의 업그레이드가 필요할 수도 있습니다. 각 FXOS 릴리스에서 지원되는 애플리케이션 버전에 각별히 주의하십시오. 지원되는 버전에 대한 자세한 내용은 *Cisco FXOS 호환성* 가이드(http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html)를 참조하십시오.

참고: FXOS 1.1(4)보다 오래된 버전의 FXOS를 실행하는 경우 *Cisco FXOS 릴리스 노트 1.1(4)*에서 시스템을 FXOS 1.1(4)로 업그레이드하는 방법을 참조하십시오.

현재 버전	업그레이드 경로					
FXOS 2.1(1.x)	→	FXOS 2.1(1.83)				
FXOS 2.0(1.x)	→	FXOS 2.1(1.64)	→	FXOS 2.1(1.83)		
FXOS 1.1(4.x)	→	FXOS 2.0(1.135)	→	FXOS 2.1(1.64)	→	FXOS 2.1(1.83)

설치 참고 사항

- FXOS 플랫폼 번들 소프트웨어 및 애플리케이션 CSP 이미지를 동시에 업그레이드할 경우 FXOS 플랫폼 번들 소프트웨어를 업그레이드할 때까지는 보안 어플라이언스에 애플리케이션 CSP 이미지를 업로드하지 마십시오.

업그레이드 지침

디바이스 컨피그레이션에 적용되는 업그레이드 지침을 참조하십시오.

- Firepower Threat Defense를 사용하는 경우 Firepower Security Appliance를 업그레이드하는 방법에 대해서는 업그레이드 이후 버전에 대한 Firepower System 릴리스 노트를 참조하십시오 (http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html).
- 독립형 ASA 논리 디바이스 또는 ASA 섀시 내 클러스터를 실행 중인 Firepower Security Appliance를 업그레이드하는 방법에 대해서는 독립형 ASA 논리 디바이스 또는 ASA 섀시 내 클러스터를 실행 중인 Firepower Security Appliance 업그레이드, 7페이지를 참조하십시오.
- ASA 페일오버 쌍으로 구성된 2대의 Firepower Security Appliance를 업그레이드하려면 현재 버전과 목표 버전에 적합한 절차를 수행합니다.
  - FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 방법에 대해서는 향상된 제로 다운타임 프로세스를 사용하여 ASA 페일오버 쌍 업그레이드, 8페이지를 참조하십시오.
  - FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.1(1.64)로 업그레이드하는 방법에 대해서는 ASA 페일오버 쌍 업그레이드, 10페이지를 참조하십시오.
- 섀시 간 클러스터로 구성된 Firepower Security Appliance를 업그레이드하려면 현재 버전과 목표 버전에 적합한 절차를 수행합니다.
  - FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 방법에 대해서는 향상된 제로 다운타임 프로세스를 사용하여 ASA 섀시 간 클러스터 업그레이드, 15페이지를 참조하십시오.
  - FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.0(1.64)로 업그레이드하는 방법에 대해서는 ASA 섀시 간 클러스터 업그레이드, 17페이지를 참조하십시오.

독립형 ASA 논리 디바이스 또는 ASA 섀시 내 클러스터를 실행 중인 Firepower Security Appliance 업그레이드

시스템을 2.1(1)로 업데이트하려면 다음 단계를 수행합니다.

1. FXOS 2.1.(1) 이미지를 논리 시스템에 다운로드합니다(소프트웨어 다운로드 참조).
2. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
3. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오.
4. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오.
5. ASA CSP 이미지를 사용하여 임의의 ASA 논리 디바이스(독립형 또는 섀시 내 클러스터)를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "논리 디바이스에 대한 이미지 버전 업데이트" 항목을 참조하십시오.

향상된 제로 다운타임 프로세스를 사용하여 ASA 페일오버 쌍 업그레이드

참고: 이 프로세스는 FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 경우에만 지원됩니다. FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.1(1.64)로 업그레이드하는 경우 ASA 페일오버 쌍 업그레이드, 10페이지를 참조하십시오.

1. FXOS 2.1.(1) 이미지를 논리 시스템에 다운로드합니다(소프트웨어 다운로드 참조).
2. ***스탠바이*** ASA 논리 디바이스를 포함하는 Firepower Security Appliance에서 Firepower eXtensible Operating System을 업그레이드합니다.
   a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
   b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오.
3. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다.
   a. 업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다.
   b. 업그레이드 프로세스가 끝나고 **scope ssa**에서 **show slot** 명령을 사용하여 슬롯이 "온라인" 상태가 되었음을 확인할 수 있습니다.
   c. 애플리케이션이 "온라인" 상태가 되었음을 확인하려면 **scope ssa** 에서 **show app-instance** 명령을 사용합니다.
4. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.
   a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

      자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
   b. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

      top (모드 계층 구조의 최상위 레벨로 범위 설정)
      scope ssa
      scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
      scope app-instance asa
      set startup-version *<version>*
      exit
   c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

      scope app-instance vdp
      set startup-version *<version>*
      exit
   d. 컨피그레이션을 커밋합니다.

      commit-buffer
   e. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-d 단계**에 따라 업그레이드합니다.
5. 업그레이드 프로세스가 끝나면 애플리케이션이 온라인 상태임을 확인합니다.

   scope ssa
   show app-instance

6. 방금 업그레이드한 유닛을 *액티브* 유닛으로 만들어 트래픽이 업그레이드된 유닛으로 이동하게 합니다.
   a. ***스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 ASA 콘솔로 연결합니다.
   b. 이 유닛을 액티브 유닛으로 만듭니다.
      failover active
   c. 컨피그레이션을 저장합니다.
      write memory
   d. 유닛이 *액티브* 유닛임을 확인합니다.
      show failover
7. ***새 스탠바이*** ASA 논리 디바이스를 포함하는 Firepower Security Appliance에서 Firepower eXtensible Operating System을 업그레이드합니다.
   a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
   b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오.
8. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다.
   a. 업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다.
   b. 업그레이드 프로세스가 끝나고 **scope ssa**에서 **show slot** 명령을 사용하여 슬롯이 "온라인" 상태가 되었음을 확인할 수 있습니다.
   c. 애플리케이션이 "온라인" 상태가 되었음을 확인하려면 **scope ssa** 에서 **show app-instance** 명령을 사용합니다.
9. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.
   a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

      자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
   b. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

      top (모드 계층 구조의 최상위 레벨로 범위 설정)
      scope ssa
      scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
      scope app-instance asa
      set startup-version *<version>*
      exit
   c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

      scope app-instance vdp
      set startup-version *<version>*
      exit
   d. 컨피그레이션을 커밋합니다.
      commit-buffer

e. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-d 단계**에 따라 업그레이드합니다.

10. 업그레이드 프로세스가 끝나면 애플리케이션이 온라인 상태임을 확인합니다.

    scope ssa
    show app-instance

11. 방금 업그레이드한 유닛을 업그레이드 이전처럼 *액티브* 유닛으로 만듭니다.

    a. ***새 스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 ASA 콘솔로 연결합니다.

    b. 이 유닛을 액티브 유닛으로 만듭니다.

    failover active

    c. 컨피그레이션을 저장합니다.

    write memory

    d. 유닛이 *액티브* 유닛임을 확인합니다.

    show failover

ASA 페일오버 쌍 업그레이드

참고: 이 프로세스는 FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.1(1.64)로 업그레이드하는 경우에만 지원됩니다. FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 경우 향상된 제로 다운타임 프로세스를 사용하여 ASA 페일오버 쌍 업그레이드, 8페이지를 참조하십시오.

1. FXOS 2.1.(1) 이미지를 논리 시스템에 다운로드합니다(소프트웨어 다운로드 참조).
2. ***스탠바이*** ASA 논리 디바이스의 애플리케이션을 비활성화합니다.

    a. ***스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 FXOS CLI로 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).

    b. ASA 애플리케이션을 끕니다.

    scope ssa
    scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
    scope app-instance asa
    비활성화
    exit

    c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 비활성화합니다. 그렇지 않으면 **d 단계**로 진행합니다.

    scope app-instance vdp
    비활성화
    exit

    d. 컨피그레이션을 커밋합니다.

    commit-buffer

    e. 애플리케이션이 오프라인 상태임을 확인합니다.

    show app-instance

    참고: ASA가 중지하고 보안 모듈이 리부팅한 후에 vDP가 중지할 수 있으므로 모든 애플리케이션이 "오프라인" 상태가 되는 데 2분 ~ 5분 가량 걸릴 수 있습니다. 중지 작업 중 하나라도 실패할 경우 **b-d단계**를 반복하십시오.

f. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-e 단계**에 따라 비활성화하고 확인합니다.

3. ***스탠바이*** ASA 논리 디바이스를 포함하는 Firepower Security Appliance에서 Firepower eXtensible Operating System을 업그레이드합니다.

   a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

   b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오.

4. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다.

   a. 업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다.

   b. 업그레이드 프로세스가 끝나고 **scope ssa**에서 **show slot** 명령을 사용하여 슬롯이 "온라인" 상태가 되었음을 확인할 수 있습니다.

5. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.

   a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

      자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

   b. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

      top (모드 계층 구조의 최상위 레벨로 범위 설정)
      scope ssa
      scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
      scope app-instance asa
      set startup-version <*version*>
      exit

   c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

      scope app-instance vdp
      set startup-version <*version*>
      exit

   d. 컨피그레이션을 커밋합니다.

      commit-buffer

   e. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-d 단계**에 따라 업그레이드합니다.

6. 업그레이드 프로세스가 끝나면 ***스탠바이*** ASA 논리 디바이스의 애플리케이션을 다시 활성화합니다.

   a. 모든 슬롯이 "온라인" 상태임을 확인하려면 **scope ssa**의 **show slot** 명령을 사용합니다.

   b. 애플리케이션에서 성공적으로 업그레이드를 완료했고 현재 "오프라인" 상태임을 확인하려면 **scope ssa**에서 **show app-instance** 명령을 사용합니다.

c. ASA 애플리케이션을 켭니다.

scope ssa
scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
scope app-instance asa
활성화
exit

d. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 활성화합니다. 그렇지 않으면 **e 단계**로 진행합니다.

scope app-instance vdp
활성화
exit

e. 컨피그레이션을 커밋합니다.

commit-buffer

f. 애플리케이션이 온라인 상태임을 확인합니다.

show app-instance

g. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **a-f 단계**에 따라 활성화하고 확인합니다.

7. 방금 업그레이드한 유닛을 *액티브* 유닛으로 만들어 트래픽이 업그레이드된 유닛으로 이동하게 합니다.

a. ***스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 ASA 콘솔로 연결합니다.

b. 페일오버를 활성화하고 액티브로 만듭니다.

failover

failover active

c. 컨피그레이션을 저장합니다.

write memory

d. 유닛이 *액티브* 유닛임을 확인합니다.

show failover

8. ***새 스탠바이*** ASA 논리 디바이스의 애플리케이션을 비활성화합니다.

a. ***새 스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 FXOS CLI로 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).

b. ASA 애플리케이션을 끕니다.

scope ssa
scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
scope app-instance asa
비활성화
exit

c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 비활성화합니다. 그렇지 않으면 **d 단계**로 진행합니다.

scope app-instance vdp
비활성화
exit

d. 컨피그레이션을 커밋합니다.

commit-buffer

e. 애플리케이션이 오프라인 상태임을 확인합니다.

show app-instance

참고: ASA가 중지하고 보안 모듈이 리부팅한 후에 vDP가 중지할 수 있으므로 모든 애플리케이션이 "오프라인" 상태가 되는 데 2분 ~ 5분 가량 걸릴 수 있습니다. 중지 작업 중 하나라도 실패할 경우 **b-d단계**를 반복하십시오.

f. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-e 단계**에 따라 비활성화하고 확인합니다.

9. ***새 스탠바이*** ASA 논리 디바이스를 포함하는 Firepower Security Appliance에서 Firepower eXtensible Operating System을 업그레이드합니다.

a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오.

10. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다.

a. 업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다.

b. 업그레이드 프로세스가 끝나고 **scope ssa**에서 **show slot** 명령을 사용하여 슬롯이 "온라인" 상태가 되었음을 확인할 수 있습니다.

11. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.

a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

b. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

top (모드 계층 구조의 최상위 레벨로 범위 설정)
scope ssa
scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
scope app-instance asa
set startup-version *<version>*
exit

c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

scope app-instance vdp
set startup-version *<version>*
exit

d. 컨피그레이션을 커밋합니다.

commit-buffer

e. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **b-d 단계**에 따라 업그레이드합니다.

12. 업그레이드 프로세스가 끝나면 ***새 스탠바이*** ASA 논리 디바이스의 애플리케이션을 다시 활성화합니다.
    a. 모든 슬롯이 "온라인" 상태임을 확인하려면 **scope ssa**의 **show slot** 명령을 사용합니다.
    b. 애플리케이션에서 성공적으로 업그레이드를 완료했고 현재 "오프라인" 상태임을 확인하려면 **scope ssa**에서 **show app-instance** 명령을 사용합니다.
    c. ASA 애플리케이션을 켭니다.

       scope ssa
       scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
       scope app-instance asa
       활성화
       exit

    d. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 활성화합니다. 그렇지 않으면 **e 단계**로 진행합니다.

       scope app-instance vdp
       활성화
       exit

    e. 컨피그레이션을 커밋합니다.

       commit-buffer

    f. 애플리케이션이 온라인 상태임을 확인합니다.

       show app-instance

    g. Firepower Security Appliance에 여러 페일오버 피어(Radware DefensePro 데코레이터가 있거나 없음)가 구성된 경우 **a-f 단계**에 따라 활성화하고 확인합니다.
13. 방금 업그레이드한 유닛을 업그레이드 이전처럼 *액티브* 유닛으로 만듭니다.
    a. ***새 스탠바이*** ASA 논리 디바이스를 포함한 Firepower Security Appliance의 ASA 콘솔로 연결합니다.
    b. 페일오버를 활성화하고 액티브로 만듭니다.

       failover
       failover active

    c. 컨피그레이션을 저장합니다.

       write memory

    d. 유닛이 *액티브* 유닛임을 확인합니다.

       show failover

향상된 제로 다운타임 프로세스를 사용하여 ASA 섀시 간 클러스터 업그레이드

참고: 이 프로세스는 FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 경우에만 지원됩니다. FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.1(1.64)로 업그레이드하는 경우 ASA 섀시 간 클러스터 업그레이드, 17페이지를 참조하십시오.

업그레이드 사전 체크리스트

1. 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).
2. 설치된 모든 보안 모듈이 온라인 상태임을 확인합니다.

   scope ssa
   show slot
3. 설치된 모든 보안 모듈에 올바른 버전의 FXOS 및 ASA가 설치되었음을 확인합니다.

   scope server 1/*x*
   show version
   scope ssa
   show logical-device
4. 섀시에 설치된 모든 보안 모듈의 클러스터 운영 상태가 “In-Cluster”임을 확인합니다.

   scope ssa
   show app-instance
5. 설치된 모든 보안 모듈이 클러스터의 일부로 표시됨을 확인합니다.

   connect module *x* **console**
   show cluster info
6. *기본* 유닛이 이 섀시에 없음을 확인합니다.

   scope ssa
   show app-instance

   클러스터 역할이 “마스터”로 설정된 ASA 인스턴스가 없어야 합니다.

절차

1. FXOS 2.1.(1) 이미지를 논리 시스템에 다운로드합니다(소프트웨어 다운로드 참조).
2. 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).
3. 섀시 #2에서 Firepower eXtensible Operating System 번들을 업그레이드합니다.
   a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).
   b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오(관련 설명서, 24페이지).

4. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다. 15분 ~ 20분 가량 걸립니다.
   a. 업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다. 모든 구성 요소가 “Upgrade-Status: Ready”로 표시되어야 합니다.
   b. 업그레이드 프로세스가 끝나면 설치된 모든 보안 모듈이 온라인 상태임을 확인합니다.

      scope ssa
      show slot

   c. 모든 ASA 애플리케이션이 현재 온라인 상태임을 확인합니다.

      scope ssa
      show app-instance

5. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.
   a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

      자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

   b. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

      top (모드 계층 구조의 최상위 레벨로 범위 설정)
      scope ssa
      scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
      scope app-instance asa
      set startup-version <*version*>
      exit

   c. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

      scope app-instance vdp
      set startup-version <*version*>
      exit

   d. 이 보안 어플라이언스에 설치된 논리 디바이스의 모든 슬롯에 대해 **b-c 단계**를 반복합니다.
   e. 컨피그레이션을 커밋합니다.

      commit-buffer

6. 업그레이드 프로세스가 끝나면 애플리케이션이 온라인 상태임을 확인합니다.

   scope ssa
   show app-instance

   섀시의 모든 ASA 및 vDP 애플리케이션에서 운영 상태가 "온라인"임을 확인합니다.

   섀시의 모든 ASA 및 vDP 애플리케이션에서 운영 상태가 "In-Cluster"임을 확인합니다.

   섀시의 모든 ASA에서 클러스터 역할이 "슬레이브"임을 확인합니다.

7. 섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

   connect module *x* **console**
   configure terminal
   cluster master

   섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정하면 섀시 #1은 더 이상 기본 유닛을 포함하지 않으므로 업그레이드할 수 있습니다.

8. 섀시 #1에 대해 업그레이드 사전 체크리스트 및 1단계 ~ 6단계를 반복합니다.
9. 클러스터에 추가로 포함된 섀시가 있을 경우 그 섀시에 대해 업그레이드 사전 체크리스트 및 1단계 ~ 6단계를 반복합니다.
10. 기본 역할을 섀시 #1로 돌려놓으려면 섀시 #1의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

    connect module *x* **console**
    configure terminal
    cluster master

ASA 섀시 간 클러스터 업그레이드

참고: 이 프로세스는 FXOS 2.0(1.37) ~ 2.0(1.86)에서 FXOS 2.1(1.64)로 업그레이드하는 경우에만 지원됩니다. FXOS 2.0(1.129) 이상에서 FXOS 2.1(1.64)로 또는 FXOS 2.1(1.64) 이상에서 FXOS 2.1(1.83)로 업그레이드하는 경우 향상된 제로 다운타임 프로세스를 사용하여 ASA 섀시 간 클러스터 업그레이드, 15페이지를 참조하십시오.

업그레이드 사전 체크리스트

1. 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).
2. 설치된 모든 보안 모듈이 온라인 상태임을 확인합니다.

   scope ssa
   show slot

3. 설치된 모든 보안 모듈에 올바른 버전의 FXOS 및 ASA가 설치되었음을 확인합니다.

   scope server 1/*x*
   show version
   scope ssa
   show logical-device

4. 섀시에 설치된 모든 보안 모듈의 클러스터 운영 상태가 “In-Cluster”임을 확인합니다.

   scope ssa
   show app-instance

5. 설치된 모든 보안 모듈이 클러스터의 일부로 표시됨을 확인합니다.

   connect module *x* **console**
   show cluster info

6. *기본* 유닛이 이 섀시에 없음을 확인합니다.

   scope ssa
   show app-instance

   클러스터 역할이 “마스터”로 설정된 ASA 인스턴스가 없어야 합니다.

절차

1. FXOS 2.1.(1) 이미지를 논리 시스템에 다운로드합니다(소프트웨어 다운로드 참조).
2. 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다. 자세한 내용은 *Cisco FXOS CLI 컨피그레이션 가이드* 또는 *Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드*의 "FXOS CLI 액세스" 항목을 참조하십시오(관련 설명서, 24페이지).

3. 섀시 #2의 모든 애플리케이션을 끕니다.
   a. ASA 애플리케이션을 끕니다.

      scope ssa
      scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
      scope app-instance asa
      비활성화
      exit

   b. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 비활성화합니다. 그렇지 않으면 **c 단계**로 진행합니다.

      scope app-instance vdp
      비활성화
      exit

   c. 이 보안 어플라이언스에 설치된 논리 디바이스의 모든 슬롯에 대해 **a-b 단계**를 반복합니다.

   d. 컨피그레이션을 커밋합니다.

      commit-buffer

   e. 애플리케이션이 오프라인 상태임을 확인합니다.

      top (모드 계층 구조의 최상위 레벨로 범위 설정)
      scope ssa
      show app-instance

   참고: 모든 애플리케이션이 "오프라인" 상태가 되려면 2분 ~ 5분 가량 걸릴 수 있습니다. 중지 작업 중 하나라도 실패할 경우 **a-d단계**를 반복하십시오.
4. 섀시 #2에서 Firepower eXtensible Operating System 번들을 업그레이드합니다.
   a. FXOS 2.1(1) 플랫폼 번들 이미지를 Firepower Security Appliance에 업로드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

   b. FXOS 2.1(1) 플랫폼 번들 이미지를 사용하여 Firepower Security Appliance를 업그레이드합니다. 자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower eXtensible Operating System 플랫폼 번들 업그레이드" 항목을 참조하십시오(관련 설명서, 24페이지).
5. 섀시가 리부팅하고 제대로 업그레이드할 때까지 기다립니다. 15분 ~ 20분 가량 걸립니다.

   업그레이드 프로세스를 모니터링하려면 **scope system**의 **show firmware monitor** 명령을 사용합니다. 모든 구성 요소가 “Upgrade-Status: Ready”로 표시되어야 합니다.
6. ASA 및 vDP 논리 디바이스 이미지를 업그레이드합니다.
   a. ASA CSP 이미지를 Firepower Security Appliance에 업로드합니다. Radware DefensePro(vDP)가 이 ASA 애플리케이션에 대한 데코레이터로 구성되었고 사용 가능한 업데이트가 있을 경우 vDP CSP 이미지도 업로드합니다.

      자세한 내용은 *Cisco Firepower Chassis Manager 컨피그레이션 가이드*에서 "Firepower 어플라이언스에 이미지 업로드" 항목을 참조하십시오(관련 설명서, 24페이지).

   b. 설치된 모든 보안 모듈이 온라인 상태임을 확인합니다.

      scope ssa
      show slot

   c. 모든 ASA 애플리케이션이 현재 오프라인 상태임을 확인합니다.

      scope ssa
      show app-instance

d. ASA CSP 이미지를 사용하여 논리 디바이스 이미지를 업그레이드합니다.

top (모드 계층 구조의 최상위 레벨로 범위 설정)
scope ssa
scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
scope app-instance asa
set startup-version <*version*>
exit

e. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 vDP 이미지를 업그레이드합니다.

scope app-instance vdp
set startup-version <*version*>
exit

f. 이 보안 어플라이언스에 설치된 논리 디바이스의 모든 슬롯에 대해 **d-e 단계**를 반복합니다.

g. 컨피그레이션을 커밋합니다.

commit-buffer

7. 업그레이드 프로세스가 끝나면 섀시 #2의 애플리케이션을 다시 활성화합니다.

a. 모든 슬롯이 "온라인" 상태임을 확인하려면 **scope ssa**의 **show slot** 명령을 사용합니다.

b. 모든 애플리케이션에서 성공적으로 업그레이드를 완료했고 현재 "오프라인" 상태임을 확인하려면 **scope ssa**에서 **show app-instance** 명령을 사용합니다.

c. ASA 애플리케이션을 켭니다.

scope ssa
scope slot *x*(여기서 *x*는 ASA 논리 디바이스가 구성된 슬롯 ID)
scope app-instance asa
활성화
exit

d. Radware DefensePro가 이 ASA 애플리케이션에 대한 데코레이터로 구성된 경우 활성화합니다. 그렇지 않으면 **e 단계**로 진행합니다.

scope app-instance vdp
활성화
exit

e. 이 보안 어플라이언스에 설치된 논리 디바이스의 모든 슬롯에 대해 **c-d 단계**를 반복합니다.

f. 컨피그레이션을 커밋합니다.

commit-buffer

성공적으로 업그레이드하고 다시 활성화하면 ASA 노드가 자동으로 다시 기존 클러스터에 합류합니다.

g. 애플리케이션이 온라인 상태임을 확인합니다.

show app-instance

섀시의 모든 ASA 및 vDP 애플리케이션에서 운영 상태가 "온라인"임을 확인합니다.

섀시의 모든 ASA 및 vDP 애플리케이션에서 운영 상태가 "In-Cluster"임을 확인합니다.

섀시의 모든 ASA에서 클러스터 역할이 "슬레이브"임을 확인합니다.

8. 섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

   connect module *x* **console**
   configure terminal
   cluster master

   섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정하면 섀시 #1은 더 이상 기본 유닛을 포함하지 않으므로 업그레이드할 수 있습니다.

9. 섀시 #1에 대해 업그레이드 사전 체크리스트 및 1단계 ~ 7단계를 반복합니다.
10. 클러스터에 추가로 포함된 섀시가 있을 경우 그 섀시에 대해 업그레이드 사전 체크리스트 및 1단계 ~ 7단계를 반복합니다.
11. 기본 역할을 섀시 #1로 돌려놓으려면 섀시 #1의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

    connect module *x* **console**
    configure terminal
    cluster master

오픈 버그 및 해결된 버그

이 릴리스에 대한 오픈 버그 및 해결된 버그는 Cisco 버그 검색 툴을 통해 액세스할 수 있습니다. 이 웹 기반 툴에서 Cisco 버그 추적 시스템에 액세스할 수 있습니다. 이 시스템에서는 이 제품 및 기타 Cisco 하드웨어/소프트웨어 제품의 버그 및 취약점에 대한 정보를 관리합니다.

참고: Cisco.com 계정이 있어야 Cisco 버그 검색 툴에 로그인하고 액세스할 수 있습니다. 계정이 없는 경우 계정을 등록하면 됩니다.

Cisco 버그 검색 툴에 대한 자세한 내용은 버그 검색 툴 도움말 및 FAQ를 참조하십시오.

오픈 버그

Firepower eXtensible 운영 체제 2.1(1)에 대한 심각도 3 이상의 오픈 버그가 다음 표에 나와 있습니다.

표 1 FXOS 2.1(1)에 영향을 주는 오픈 버그

식별자	설명
CSCus73654	ASA가 LD에 의한 관리 인터페이스 지정에 대해 관리 전용으로 표시하지 않음
CSCuu33739	포트-채널의 물리적 인터페이스 속도가 올바르지 않음
CSCuu50615	온박스 섀시 관리자: 온박스에 지원되지 않은 표준 시간대 표시
CSCuw31077	인터페이스에 적용된 필터를 검증해야 함
CSCuw81066	디스크 공간을 초과하는 세션을 활성화하는 경우 오류 메시지를 표시해야 함
CSCuw89854	5GB 이상의 세션을 생성할 경우 오류 메시지
CSCux37821	플랫폼 설정 순서 필드가 사용 가능한 가장 낮은 값만 표시
CSCux63101	메모리 어레이의 모든 메모리가 작동 가능 열에서 알 수 없음으로 표시
CSCux65728	vDP 및 APsolute Vision에서 기본 사용자 이름/비밀번호 제거
CSCux76704	논리 디바이스 저장 상자 아래에 풀다운 정보 없는 불가사의한 “>>” 상자 표시
CSCux77947	고속 데이터 전송 시 Pcap 파일 크기가 제대로 업데이트되지 않음
CSCux85255	세션 이름에 'port'가 있으면 패킷 캡처 세션 생성 실패
CSCux85969	QP: 존재하지 않을 때 PSU를 비어 있음으로 표시
CSCux98517	섀시 관리자에서 vDP에 대한 데이터 포트 데코레이션 취소가 허용되지 않아야 함
CSCuy21573	섀시 관리자: 업데이트 페이지에서 정렬 실패

표 1 FXOS 2.1(1)에 영향을 주는 오픈 버그

식별자	설명
CSCuy31784	필터가 사용될 경우 삭제 작업 후 이미지가 나열되지 않음
CSCuy34708	SSP MIO - MIO 부팅 과정에 MIO에서 커널 스핀 잠금 표시
CSCuy38842	플로우-오프로드, ASA 투명 LD, HSRP/VRRP 사용 시 ARP 문제
CSCuy58732	플로우-오프로드 사용 시 ASA + VDP 클러스터에서 데이터 트래픽의 레이턴시 증가
CSCuy73153	QP 4110: P2D 베타 유닛에서 잘못된 고정 포트 1-4
CSCuy98317	LD 이름에 -가 있을 경우 LD에서 intf 소프트 연결 해지 불가
CSCuz54858	FTW-클러스터: FXOS 업그레이드 시작 후 트래픽 연속성 부재
CSCuz59046	MIO 리부팅 과정에서 FTW가 우회 모드에서 대기 모드로 전환하는 데 2초 ~ 5초 소요
CSCuz62795	POST 인증 요청에서 잘못된 오류 메시지 표시
CSCuz69280	MIO-블레이드 통신 실패. 하트비트 업데이트 메시지를 보낼 수 없음
CSCuz81832	CM의 FTD 클러스터 내 컨피그레이션 과정에서 인터페이스 정보 탭이 지저분해짐
CSCuz93180	검증 실패 시 AAA LDAP 컨피그레이션에서 정보를 보존하지 않음
CSCva05729	aclmgr에서 MIO가 FXOS 2.0.1.24와 충돌
CSCva11473	업그레이드 이후 때때로 슬롯이 응답 없음 상태
CSCva46249	부트스트랩 설정 변경 후 1분 ~ 2분간 트래픽이 우회되지 않음
CSCva86402	전원을 켜는 과정에서 10G 및 40G SR FTW 모듈의 링크 파트너에서 링크 플랩
CSCva86452	전원을 끌 때 10G 및 40G SR FTW 카드와 연결된 스위치에서 링크 플랩
CSCvb52076	부팅 과정에서 Watford 1G-Copper FTW 모듈과의 링크 파트너에서 링크 플랩
CSCvb65011	EntityPhysical MIB가 섀시에 대한 Sup 일련 번호 포함
CSCvb87967	SdLduProvisionLDU 오류와 함께 로컬 디바이스 설치 실패
CSCvc03942	섀시 관리자에서 존재하지 않는 사용자 로그인 실패가 로깅되지 않음
CSCvc03494	Radware vDP를 APSolute Vision에 추가할 수 없음. 이를 해결하려면 디바이스 드라이버를 직접 다운로드하여 Vision에 설치해야 합니다.
CSCvc07229	SSH 호스트 키-문자열 입력이 ssh 사용자 키-문자열과 다름
CSCvc14775	FXOS 2.0.1.86 + ASA 9.6.2에서 FXOX 1.1.4.140으로 다운그레이드할 경우 앱-인스턴스가 응답하지 않음
CSCvc16980	CSP 이미지 무결성을 위해 FXOS 이미지의 검증 상태가 초기에는 "없음"으로 표시되어야 함
CSCvc19428	FCM: eventing 이벤트에 대해 앱-포트를 생성할 수 없음
CSCvc22039	BS/QP: snmpwalk 출력에서 불일치 발견
CSCvc37200	ICC FTD - EthPM이 SNM의 메시지를 기다리는 동안 시간이 초과되어 Po 인터페이스 꺼짐
CSCvc38763	온박스 관리자: FCM 및 LD 페이지에서 무한 루프
CSCvc41324	BS: ip-block 생성에 대해서는 감사 로그가 생성되지 않음
CSCvc44522	관리 컨트롤러 서버1/1의 로그 용량이 매우 부족하다는 경고 표시
CSCvc44733	때때로 특정 링크 파트너와 FPR 링크 플랩(err 비활성)
CSCvc52435	패킷 캡처: IPv6 패킷 캡처 필터 문제
CSCvc53082	DNS 및 호스트 이름 전달 시 FTD configure manager add에서 FTD appagent가 DONTRESOLVE 푸시
CSCvc53247	'show hardware-bypass-ports' 명령에서 FTW 상태가 잘못 표시됨
CSCvd05138	투명 모드의 공격 트래픽이 라우티드 모드보다 일찍 탐지됨
CSCvd21762	ASA HA: http CPS 트래픽 플로우에 대해 보조 스탠바이 유닛 연결 수 및 CPU가 계속 증가

FXOS 2.1.1.83에서 해결된 버그

다음 표는 Firepower eXtensible 운영 체제 2.1.1.83에서 해결된 결함을 보여줍니다.

표 2 FXOS 2.1.1.83에서 해결된 버그

식별자	설명
CSCuw92801	Cruz 링크 대기 중. 링크 플랩.
CSCvc58687	보안 잠금 해제 지원 추가
CSCvc72840	보안 잠금 해제에 대한 시스템 로그
CSCvc73959	ASA 앱-인스턴스 시작 실패, "CSP_INSTALL_Completed" 오류
CSCvc96198	Dist-S2S: 실제/강제 충돌 시 Transient_Core_Files에서 막혀 코어덤프 파일이 생성되지 않음
CSCvd05201	블레이드 업그레이드 번들 해제 알림 지연
CSCvd11605	연결된 SFP가 없을 때 Eth1/1 - 6 고정 포트의 QP/BS LED가 노란색으로 표시
CSCvd58911	대용량(5GB) 파일을 /bootflash에 복사할 때 섀시 리부팅
CSCvd66066	호스트 이름 설정 시 FXOS 동작 불일치
CSCvd90400	FPR4100 및 9300 FXOS 플랫폼의 메모리 누수 때문에 예기치 않게 리로드
CSCve14981	QP: appAG에 대한 최대 메모리 부족
CSCve28609	플랫폼 번들에 cruz-uboot 빌드
CSCve31871	FXOS: FTD 프롬프트에 블레이드가 있으면 모듈 기술 지원을 수집할 수 없음
CSCve32694	cruz uboot 업그레이드 및 일련 번호 오류
CSCve40673	cruz 코어 파일을 IO에 전달하는 것이 몇 시간 또는 며칠간 지연

FXOS 2.1.1.77에서 해결된 버그

다음 표는 Firepower eXtensible 운영 체제 2.1.1.77에서 해결된 결함을 보여줍니다.

표 3 FXOS 2.1.1.77에서 해결된 버그

식별자	설명
CSCuy37194	SNM 로그 파일에서 시간 잘못 표시
CSCvb83067	펌웨어 변경 사항이 하나뿐일 때 FXOS에서 펌웨어 업그레이드를 수행하지 않음
CSCvb91501	SFP 모듈 유형 스왑 시 SFP 체크섬 오류 발생
CSCvc33064	CISCO-FIREPOWER-MIB.MY가 트랩 정의를 포함하지 않음
CSCvc50397	VDP - START_FAILED, VNIC_Set_Verification_Error
CSCvc74558	플랫폼에서 cfg xml에 쓰는 방식을 개선해야 함
CSCvc74860	Lina에서 동기화되지 않은 오류 메시지가 나타난 후 SSP3RU 클러스터에 문제 발생
CSCvc77412	FXOS에서 show version 실행 시 오류 표시
CSCvc79927	ROMMON, FPGA, EPM FPGA 업그레이드 실패
CSCvc91000	블레이드에서 메모리, 디스크, CPU에 대한 카탈로그 종속성 해결
CSCvd00339	sstate 캐시 사용 시 ipmitool 설치가 실패할 수 있음
CSCvd13036	FXOS - 섀시 관리자 GUI를 통해 스마트 라이선싱 등록/등록 취소 불가
CSCvd13121	SAM 관련 기술 지원 불가
CSCvd20784	클라이언트 인증서 인증 시 섀시 관리자에서 잘못된 사용자 이름 표시
CSCvd24987	SNM 추적 로그가 show tech-support에 있어야 함

표 3 FXOS 2.1.1.77에서 해결된 버그

식별자	설명
CSCvd36898	FXOS가 제어 평면 및 데이터 평면 모두에 CPU 코어를 할당하는 것이 가능하며, 그러면 시스템이 불안정해질 수 있음
CSCvd43857	fxos 92.2.1.1953 + ASA 98.1.1.96에서 svc_sam_bladeAG_log 코어 발견
CSCvd48060	FPR 9300 Chassis Manager에서 메시지 전송: 경고: 메모리 누수 가능성 탐지
CSCvd51116	FXOS - workspace 폴더에서 부분 생성된 파일을 삭제할 수 없음
CSCvd56418	FP 9300: "show firmware monitor" 아래의 블레이드 상태가 아직도 업그레이드 중으로 표시됨
CSCvd63042	클러스터가 형성되었지만 클러스터 상태 및 역할이 "클러스터에 없음"으로 표시
CSCvd89895	링크 닫기/열기 후 간헐적으로 FP4100 FXOS 2.1.1.73 ecmp-groups가 "del" 상태
CSCvd97962	erase samdb 이후 IP-Block이 정리되지 않음
CSCve03445	2.0.1.144에서 2.1.1.76으로 업그레이드한 후 기본 ip-block이 제거됨

FXOS 2.1.1.73에서 해결된 버그

다음 표는 Firepower eXtensible 운영 체제 2.1.1.73에서 해결된 결함을 보여줍니다.

표 4 FXOS 2.1.1.73에서 해결된 버그

식별자	설명
CSCvc30488	SSP MIO CLI Copyright가 계속 2015로 표시
CSCvc59936	패킷 캡처 실행 및 LD 삭제 후 MIO appAG 충돌
CSCvc88408	FST에서 SSD 정보를 읽을 수 없음
CSCvc91208	카탈로그에 없는 DIMM에 대해 관리자가 생성한 오류 제거
CSCvc98489	2.0.1.136을 실행하는 섀시 관리자에서 9.6.1 ASA 앱을 찾을 수 없음
CSCvc98499	1.1.4.95에서 2.0.1.136으로 업그레이드한 후 ASA 앱-인스턴스가 온라인 상태가 되지 않음
CSCvc98978	BS SSD 작동 가능 여부가 해당 없음으로, 드라이브 상태, 전원 상태, 링크 속도가 알 수 없음으로 표시

Resolved Bugs in FXOS 2.1.1.64

다음 표는 이전 릴리스에서 공개하고 고객이 발견했으며 Firepower eXtensible 운영 체제 2.1.1.64에서 해결된 결함을 보여줍니다.

표 5 FXOS 2.1.1.64에서 해결된 버그

식별자	설명
CSCuw03704	FXOS SW가 잘못된 관리자 VID 표시
CSCuw37616	추가 모드에서 인터페이스를 삭제하거나 추가했는데 삭제된 인터페이스 파일이 있음
CSCuw65954	vDP: 변경 관리 부트스트랩 이후 vDP에서 mgmt-ip가 업데이트되지 않음
CSCux18974	SNMP 값이 잘린 상태이며 저작권을 업데이트해야 함
CSCux85255	세션 이름에 'port'가 있으면 패킷 캡처 세션 생성 실패
CSCux94525	펌웨어 업그레이드 과정에서 FXOS 업그레이드가 허용됨
CSCuy42650	로그인하지 않은 상태에서도 섀시 관리자 화면이 표시됨
CSCuz39085	포트 채널-관리 인터페이스 4 FTD에서 LD의 메모리 포트를 수정할 수 없음
CSCuz41682	예약이 있을 경우 CM export:msg에 필요한 On-Demand를 생성할 수 없음
CSCuz41747	온박스 관리자: scp/ftp/sftp를 비활성화하면 내보내기를 추가할 때 비밀번호 필요

표 5 FXOS 2.1.1.64에서 해결된 버그

식별자	설명
CSCuz60358	섀시 관리자 기본 설정에서 원격 사용자에 대한 액세스 거부
CSCuz87408	보안 모듈에서 하드웨어 및 서비스 상태 정렬 시 정보가 사라짐
CSCuz92172	세션 메모리 부족 시 오류 메시지가 올바르지 않음
CSCuz99352	인터페이스에서 어떤 열도 정렬할 수 없음
CSCva02605	SSP: 스위치 CDP 네이버 목록에서 포트 채널 멤버 표시
CSCva09907	애플리케이션 시작 실패 시 블레이드에서 FXOS 서비스가 중단되지 않아야 함
CSCva62672	FxOS:섀시 관리자가 등록 키에 특수 문자 허용
CSCva91923	FTW 포트에서 섀시 내 클러스터링 트래픽이 110초간 삭제
CSCva98245	9300/4100에서 ASA “show inventory” 명령이 더 구체적이어야 함
CSCvb16766	외부 인증을 사용하여 이미지를 업로드할 때 500 내부 서버 오류 발생
CSCvb33687	FxOS:FCM GUI의 보안 엔진 탭에서 전원이 꺼진 요소를 나타내기 위해 빨간색 버튼에 대한 툴팁 추가
CSCvc54102	노드 리부팅 후 마스터가 잘못된 체크섬으로 초대를 보냈기 때문에 노드가 클러스터 이탈

관련 설명서

Firepower 9300 Security Appliance 및 Firepower eXtensible 운영 체제에 대한 자세한 내용은 Cisco Firepower 9300 설명서 탐색을 참조하십시오.

설명서 받기 및 서비스 요청 제출

설명서 다운로드, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 *Cisco 제품 설명서의 새로운 사항*을 참조하십시오.

신규 및 수정된 Cisco 기술 콘텐츠를 데스크톱에서 곧바로 받으려면 Cisco 제품 설명서의 새로운 사항 RSS 피드를 구독하십시오. RSS 피드는 무료로 제공되는 서비스입니다.