시스템 관리

Firepower Chassis Manager 세션을 종료시키는 시스템 변경 사항

다음 시스템 변경 사항으로 인해 Firepower Chassis Manager에서 자동으로 로그아웃될 수 있습니다.

- 시스템 시간을 10분보다 길게 수정하는 경우
- Firepower Chassis Manager 또는 FXOS CLI를 사용하여 시스템을 리부팅하거나 종료하는 경우
- Firepower 4100/9300 섀시에서 FXOS 버전을 업그레이드하는 경우
- FIPS 또는 Common Criteria 모드를 활성화하거나 비활성화하는 경우

참고 위의 변경을 수행하는 경우와 더불어, 아무 작업도 수행하지 않는 상태로 일정 기간이 경과하는 경우에도 시스템에서 자동 로그아웃됩니다. 기본적으로는 10분 동안 작업을 하지 않으면 시스템에서 로그아웃됩니다. 이 시간 초과 설정을 구성하려면 세션 시간 초과 구성 섹션을 참조하십시오. 세션이 활성 상태이더라도 일정 기간이 지나면 사용자가 시스템에서 로그아웃되는 절대 시간 초과 설정을 구성할 수도 있습니다. 절대 시간 초과 설정을 구성하려면 절대 세션 시간 초과 구성 섹션을 참조하십시오.

관리 IP 주소 변경

시작하기 전에

Firepower 4100/9300 섀시의 관리 IP 주소를 FXOS CLI에서 변경할 수 있습니다.

참고 관리 IP 주소를 변경한 후, 새 주소를 사용하여 Firepower Chassis Manager 또는 FXOS CLI에 대한 모든 연결을 다시 설정해야 합니다.

프로시저

단계 **1** FXOS CLI에 연결합니다(액세스 - FXOS CLI 참고).

단계 **2** 다음과 같이 IPv4 관리 IP 주소를 구성합니다.

a) 패브릭 인터커넥트 a의 범위를 설정합니다.

Firepower-chassis# **scope fabric-interconnect a**

b) 다음 명령을 입력하여 현재 관리 IP 주소를 확인합니다.

Firepower-chassis /fabric-interconnect # **show**

c) 다음 명령을 입력하여 새로운 관리 IP 주소 및 게이트웨이를 구성합니다.

Firepower-chassis /fabric-interconnect # **set out-of-band ip** *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

d) 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /fabric-interconnect* # **commit-buffer**

단계 **3** 다음과 같이 IPv6 관리 IP 주소를 구성합니다.

a) 패브릭 인터커넥트 a의 범위를 설정합니다.

Firepower-chassis# **scope fabric-interconnect a**

b) 관리 IPv6 구성의 범위를 설정합니다.

Firepower-chassis /fabric-interconnect # **scope ipv6-config**

c) 다음 명령을 입력하여 현재 관리 IPv6 주소를 확인합니다.

Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 다음 명령을 입력하여 새로운 관리 IP 주소 및 게이트웨이를 구성합니다.

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

참고 IPv6 글로벌 유니캐스트 주소만 새시의 IPv6 관리 주소로 지원됩니다.

e) 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

예

다음 예에서는 IPv4 관리 인터페이스 및 게이트웨이를 구성합니다.

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

다음 예에서는 IPv6 관리 인터페이스 및 게이트웨이를 구성합니다.

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    2001::8998                         64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

애플리케이션 관리 IP 변경

Firepower 4100/9300 섀시에 연결된 애플리케이션의 관리 IP 주소를 FXOS CLI에서 변경할 수 있습니다. 그렇게 하려면 먼저 FXOS 플랫폼 레벨에서 IP 정보를 변경한 다음, 애플리케이션 레벨에서 IP 정보를 변경해야 합니다.

참고 애플리케이션 관리 IP를 변경하면 서비스가 중단됩니다.

프로시저

단계 **1** FXOS CLI에 연결합니다. (액세스 - FXOS CLI를 참조하십시오.)

단계 **2** 논리적 디바이스로 범위를 지정합니다.

scope ssa

scopelogical-device *logical_device_name*

단계 **3** 관리 부트스트랩으로 범위를 지정하고 새로운 관리 부트스트랩 파라미터를 구성합니다. 구축 간에는 다음과 같은 차이점이 있습니다.

ASA 논리적 디바이스의 독립형 구성:

a) 논리적 디바이스 관리 부트스트랩을 입력합니다.
scope mgmt-bootstrap *asa*

b) 슬롯에 대한 IP 모드를 입력합니다.
scope *ipv4_or_6 slot_number* default

c) (IPv4만 해당) 새 IP 주소를 설정합니다.
set ip *ipv4_address* **mask** *network_mask*

d) (IPv6만 해당) 새 IP 주소를 설정합니다.
set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) 게이트웨이 주소를 설정합니다.
set gateway *gateway_ip_address*

f) 구성을 커밋합니다.
commit-buffer

ASA 논리적 디바이스의 클러스터 구성:

a) 클러스터 관리 부트스트랩을 입력합니다.
scope cluster-bootstrap *asa*

b) (IPv4만 해당) 새 가상 IP를 설정합니다.

set virtual ipv4 *ip_address* **mask** *network_mask*

c) (IPv6만 해당) 새 가상 IP를 설정합니다.

set virtual ipv6 *ipv6_address* **prefix-length** *prefix_length_number*

d) 새 IP 풀을 설정합니다.

set ip pool *start_ip end_ip*

e) 게이트웨이 주소를 설정합니다.

set gateway *gateway_ip_address*

f) 구성을 커밋합니다.

commit-buffer

FTD의 독립 실행형 및 클러스터 구성:

a) 논리적 디바이스 관리 부트스트랩을 입력합니다.
scope mgmt-bootstrap *ftd*

b) 슬롯에 대한 IP 모드를 입력합니다.

scope*ipv4_or_6 slot_number* firepower

c) (IPv4만 해당) 새 IP 주소를 설정합니다.

set ip *ipv4_address* **mask** *network_mask*

d) (IPv6만 해당) 새 IP 주소를 설정합니다.

set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) 게이트웨이 주소를 설정합니다.

set gateway *gateway_ip_address*

f) 구성을 커밋합니다.

commit-buffer

참고 클러스터 구성의 경우 Firepower 4100/9300 섀시에 연결된 각 애플리케이션에 대해 새 IP 주소를 설정해야 합니다. 섀시 간 클러스터 또는 HA 구성의 경우, 두 섀시의 각 애플리케이션에 대해 이러한 단계를 반복해야 합니다.

단계 **4** 각 애플리케이션에 대한 관리 부트스트랩 정보를 지웁니다.

a) ssa 모드로 범위를 지정합니다.

scope ssa

b) slot로 범위를 지정합니다.

scope slot *slot_number*

c) 애플리케이션 인스턴스로 범위를 지정합니다.

scopeapp-instance *asa_or_ftd*

d) 관리 부트스트랩 정보를 지웁니다.

clear-mgmt-bootstrap

e) 구성을 커밋합니다.

commit-buffer

단계 **5** 애플리케이션을 비활성화합니다.

disable

commit-buffer

참고 클러스터 구성의 경우 Firepower 4100/9300 섀시에 연결된 각 애플리케이션에 대한 관리 부트스트랩 정보를 지우고 비활성화해야 합니다. 섀시 간 클러스터 또는 HA 구성의 경우, 두 섀시의 각 애플리케이션에 대해 이러한 단계를 반복해야 합니다.

단계 **6** 애플리케이션이 오프라인 상태이고 슬롯이 다시 온라인 상태가 되면 애플리케이션을 다시 활성화합니다.

a) ssa 모드로 다시 범위를 지정합니다.

scope ssa

b) slot로 범위를 지정합니다.

scope slot *slot_number*

c) 애플리케이션 인스턴스로 범위를 지정합니다.

scopeapp-instance *asa_or_ftd*

d) 애플리케이션을 활성화합니다.

enable

e) 구성을 커밋합니다.

commit-buffer

참고 클러스터형 구성의 경우 Firepower 4100/9300 섀시에 연결된 각 애플리케이션을 다시 활성화하려면 다음 단계를 반복해야 합니다. 섀시 간 클러스터 또는 HA 구성의 경우, 두 섀시의 각 애플리케이션에 대해 이러한 단계를 반복해야 합니다.

Firepower 4100/9300 섀시 이름 변경

Firepower 4100/9300 섀시에 사용된 이름을 FXOS CLI에서 변경할 수 있습니다.

프로시저

단계 1 FXOS CLI에 연결합니다(액세스 - FXOS CLI 참고).

단계 2 시스템 모드로 들어갑니다.

Firepower-chassis-A# **scope system**

단계 3 현재 이름을 확인합니다.

Firepower-chassis-A /system # **show**

단계 4 새 이름을 구성합니다.

Firepower-chassis-A /system # **set name** *device_name*

단계 5 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis-A /fabric-interconnect* # **commit-buffer**

예

다음 예는 디바이스 이름을 변경합니다.

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- --------------------
    New-name   Stand Alone 192.168.100.10    ::
New-name-A /system #
```

신뢰할 수 있는 ID 인증서 설치

초기 구성 이후 Firepower 4100/9300 섀시 웹 애플리케이션에서 사용하기 위한 자체 서명 SSL 인증서가 생성됩니다. 인증서가 자체 서명된 것이므로 클라이언트 브라우저에서 이를 자동으로 신뢰하지 않습니다. 새 클라이언트 브라우저는 Firepower 4100/9300 섀시 웹 인터페이스에 처음 액세스할 때, Firepower 4100/9300 섀시에 액세스하려면 먼저 인증서를 수락하도록 사용자에게 요구하는 SSL 경고를 표시합니다. FXOS CLI를 사용하여 CSR(Certificate Signing Request)을 생성하고 Firepower 4100/9300 섀시에서 사용할 결과 ID 인증서를 설치하려면 다음 절차를 사용할 수 있습니다. 이 ID 인증서를 사용하면 클라이언트 브라우저가 연결을 신뢰하며 경고 없이 웹 인터페이스를 표시합니다.

프로시저

단계 1 FXOS CLI에 연결합니다. (액세스 - FXOS CLI를 참조하십시오.)

단계 2 보안 모듈을 입력합니다.

scope security

단계 3 키 링을 생성합니다.

create keyring *keyring_name*

단계 4 개인 키의 모듈러스 크기를 설정합니다.

set modulus *size*

단계 5 구성을 커밋합니다.

commit-buffer

단계 6 CSR 필드를 구성합니다. 기본 옵션(예: subject-name)으로 인증서를 생성할 수도 있고, 인증서에 로케일 및 조직과 같은 정보를 포함하도록 허용하는 좀 더 고급 옵션을 선택적으로 사용할 수도 있습니다. CSR 필드를 구성할 때 인증서 비밀번호를 입력하라는 프롬프트가 표시됩니다.

create certreq subject-name *subject_name*

password

set country *country*

set state *state*

set locality *locality*

set org-name *organization_name*

setorg-unit-name *organization_unit_name*

set subject-name *subject_name*

단계 7 구성을 커밋합니다.

commit-buffer

단계 8 인증 증명에 제공할 CSR을 내보냅니다. 인증 기관은 CSR을 사용하여 ID 인증서를 생성합니다.

a) 전체 CSR을 표시합니다.

show certreq

b) "-----BEGIN CERTIFICATE REQUEST-----"로 시작하고(포함) "-----END CERTIFICATE REQUEST-----"로 끝나는(포함) 출력을 복사합니다.

예제:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
ETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
```

```
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA310ck6GjlNv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----END CERTIFICATE REQUEST-----
```

단계 **9** certreq 모드를 종료합니다.

exit

단계 **10** 키 링 모드를 종료합니다.

exit

단계 **11** 인증 기관의 등록 프로세스에 따라 인증 기관에 CSR 출력을 제공합니다. 요청에 성공하면 인증 기관은 CA의 개인 키를 사용하여 디지털 서명된 ID 인증서를 다시 전송합니다.

단계 **12** 참고 FXOS로 가져오려면 모든 ID 인증서는 Base64 형식이어야 합니다. 인증 기관에서 받은 ID 인증서 체인이 다른 형식인 경우 먼저 OpenSSL과 같은 SSL 툴로 변환해야 합니다.

ID 인증서 체인을 유지할 새 트러스트 포인트를 생성합니다.

create trustpoint *trustpoint_name*

단계 **13** 화면의 지침에 따라 11단계에서, 인증 기관에서 받은 ID 인증서 체인을 입력합니다.

참고 중간 인증서를 사용하는 인증 증명의 경우 루트 인증서와 중간 인증서를 결합해야 합니다. 텍스트 파일에서 맨 위에 루트 인증서를 붙여넣고, 그 뒤에 체인의 각 중간 인증서를 붙여넣습니다(모든 BEGIN CERTIFICATE 및 END CERTIFICATE 플래그 포함). 전체 텍스트 블록을 트러스트 포인트에 복사하여 붙여넣습니다.

set certchain

예제**:**

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
```

```
>ENDOFBUF
```

단계 **14** 구성을 커밋합니다.

commit-buffer

단계 **15** 트러스트 포인트 모드를 종료합니다.

exit

단계 **16** 키 링 모드로 들어갑니다.

scope keyring *keyring_name*

단계 **17** 13단계에서 생성한 트러스트 포인트를 CSR에 대해 생성한 키 링과 연결합니다.

set trustpoint *trustpoint_name*

단계 **18** 서명한 서버용 ID 인증서를 가져옵니다.

set cert

단계 **19** 인증 증명에서 제공한 ID 인증서의 내용을 붙여넣습니다.

예제:

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

단계 **20** 키 링 모드를 종료합니다.

exit

단계 **21** 보안 모드를 종료합니다.

exit

단계 **22** 시스템 모드로 들어갑니다.

scope system

단계 **23** 서비스 모드로 들어갑니다.

scope services

단계 **24** 새 인증서를 사용하도록 FXOS 웹 서비스를 구성합니다.

sethttps keyring *keyring_name*

단계 **25** 구성을 커밋합니다.

commit-buffer

단계 **26** HTTPS 서버와 연결된 키 링을 표시합니다. 이 절차의 3단계에서 생성한 키 링 이름을 반영해야 합니다. 화면 출력에 기본 키 링 이름이 표시되면 HTTPS 서버가 아직 새 인증서를 사용하도록 업데이트되지 않은 것입니다.

show https

예제**:**

```
fp4120 /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: firepower_cert
    Cipher suite mode: Medium Strength
   Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

단계 **27** 가져온 인증서의 내용을 표시하고 **Certificate Status** 값이 **Valid**로 표시되는지 확인합니다.

scope security

showkeyring *keyring_name***detail**

예제**:**

```
fp4120 /security #  scope security
fp4120 /security #  show keyring firepower_cert detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
    Certificate status: Valid
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
```

```
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:fp4120.test.local
            X509v3 Subject Key Identifier:
                FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
            X509v3 Authority Key Identifier:
                keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                  CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?cACertificate?base?objectClass=certificationAuthority
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
         2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
```

```
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

다음에 수행할 작업

신뢰할 수 있는 새 인증서가 표시되는지 확인하려면, 웹 브라우저의 주소 표시줄에 *https://<FQDN_or_IP>/*를 입력하여 Firepower Chassis Manager로 이동합니다.

참고 브라우저는 또한 주소 표시줄의 입력을 기준으로 인증서의 subject-name을 확인합니다. 인증서가 FQDN(Fully Qualified Domain Name)으로 발급된 경우 브라우저에서 해당 방식으로 액세스해야 합니다. IP 주소를 통해 액세스하는 경우, 신뢰할 수 있는 인증서가 사용되더라도 다른 SSL 오류가 표시됩니다(Common Name Invalid).

인증서 업데이트 자동 가져오기

Cisco 인증서 서버가 다른 루트 CA를 활용하도록 ID 인증서를 변경하면 ASA 디바이스를 실행하는 4100 또는 9300에서 스마트 라이선싱에 대한 연결이 끊어집니다. 라이선싱 연결은 애플리케이션의 Lina 대신 수퍼바이저에 의해 처리되므로 Smart Licensing 기능이 실패합니다. FXOS 기반 디바이스의 경우, FXOS 소프트웨어를 업그레이드하지 않고도 자동 가져오기 기능을 사용하여 문제를 해결할 수 있습니다.

자동 가져오기 기능은 기본적으로 비활성화됩니다. 다음 절차에 따라 FXOS CLI를 사용하여 자동 가져오기 기능을 활성화할 수 있습니다.

시작하기 전에

Cisco 인증서 서버에 연결하도록 DNS 서버를 구성해야 합니다.

프로시저

단계 **1** FXOS CLI에 연결합니다.

단계 **2** 보안 모듈을 입력합니다.

scope security

단계 **3** 자동 가져오기 기능을 활성화합니다.

enter tp-auto-import

예제**:**

```
FXOS# scope security
FXOS /security # enter tp-auto-import
 FXOS /security #
```

단계 **4** 구성을 커밋합니다.

commit-buffer

단계 **5** 자동 가져오기 상태 확인

show detail

예제**:**

자동 가져오기 성공:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

자동 가져오기 실패:

```
FXOS /security/tp-auto-import #
FXOS /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 22:00
Last Importing Status : Failure
TrustPoints auto Import function : Enabled
FXOS /security/tp-auto-import #
```

단계 **6** tp-auto-import 기능을 구성합니다. import-time-hour를 설정합니다.

set import-time-hour 시간 **import-time-min** 분

예제**:**

```
FXOS /security/tp-auto-import # set
  import-time-hour  Trustpoints auto import hour time
FXOS /security/tp-auto-import # set import-time-hour
  0-23  Import Time Hour
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min
  0-59  Import Time Min
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
<CR>
FXOS /security/tp-auto-import # set import-time-hour 7 import-time-min 20
```

```
FXOS /security/tp-auto-import* # commit-buffer
FXOS /security/tp-auto-import #
```

참고 자동 가져오기 소스 URL은 고정되어 있으며 가져오기 시간 세부사항을 일별 분으로 변경해야 합니다. 매일 예약된 시간에 가져오기가 수행됩니다. 시간과 분이 설정되지 않은 경우 인증서 가져오기는 활성화하는 동안 한 번만 발생합니다. 인증서는 secure-login 옵션을 통해서만 액세스할 수 있는 /opt/certstore 경로 아래의 상자에 번들로 다운로드됩니다. 번들(ios_core.p7b)과 함께 개별 인증서(AutoTP1~AutoTPn)가 자동으로 추출됩니다.

단계 **7** 자동 가져오기 구성이 완료되면 show detail 명령을 입력합니다.

show detail

예제**:**

```
FXOS  /security/tp-auto-import # show detail
Trustpoints auto import source URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
TrustPoints auto import scheduled time : 07:20
Last Importing Status : Success, Imported with 23 TrustPoint(s)
TrustPoints auto Import function : Enabled
```

참고 가져올 수 있는 최대 인증서는 30개입니다. 각 가져오기는 Cisco Certificate Server에 대한 연결 문제가 있는 경우 6번 반복된 다음 show 명령에서 마지막 가져오기 상태를 업데이트합니다.

단계 **8** (선택 사항) 자동 가져오기 기능을 비활성화하려면, delete auto-import 명령을 입력합니다.

delete tp-auto-import

예제**:**

```
FXOS /security #
FXOS /security # delete tp-auto-import
FXOS /security* # commit-buffer
FXOS /security # show detail
security mode:
    Password Strength Check: No
    Minimum Password Length: 8
    Is configuration export key set: No
    Current Task:
FXOS /security # scope tp-auto-import
Error: Managed object does not exist
FXOS /security #
FXOS /security # enter tp-auto-import
FXOS /security/tp-auto-import* # show detail
FXOS /security/tp-auto-import* #
```

참고 자동 가져오기 기능을 비활성화하면, 가져온 인증서는 빌드가 변경되지 않을 때까지 영구적으로 유지됩니다. 자동 가져오기 기능을 비활성화한 다음 빌드를 다운그레이드/업그레이드하면 인증서가 제거됩니다.

Pre-Login 배너

Pre-login 배너가 있으면 사용자가 Firepower Chassis Manager에 로그인할 때 시스템에 배너 텍스트가 표시됩니다. 사용자가 메시지 화면에서 **OK(**확인**)**를 클릭하면 사용자 이름과 비밀번호 프롬프트 창이 표시됩니다. Pre-login 배너가 구성되어 있지 않으면 사용자 이름과 비밀번호 프롬프트 창이 바로 표시됩니다.

사용자가 FXOS CLI에 로그인하면, 비밀번호 프롬프트가 나타나기 전에 배너 텍스트(구성한 경우)가 표시됩니다.

Pre-Login 배너 생성

프로시저

단계 **1** FXOS CLI에 연결합니다(액세스 - FXOS CLI 참고).

단계 **2** 보안 모드를 입력합니다.

Firepower-chassis# **scope security**

단계 **3** 배너 보안 모드로 들어갑니다.

Firepower-chassis /security # **scope banner**

단계 **4** 다음 명령을 입력하여 pre-login 배너를 만듭니다.

Firepower-chassis /security/banner # **create pre-login-banner**

단계 **5** 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인하기 전에 FXOS에서 사용자에게 표시해야 할 메시지를 지정합니다.

Firepower-chassis /security/banner/pre-login-banner* # **set message**

pre-login 배너 메시지 텍스트를 입력하기 위한 대화 상자가 열립니다.

단계 **6** 프롬프트에서 pre-login 배너 메시지를 입력합니다. 이 필드에는 어떤 표준 ASCII 문자도 사용할 수 있습니다. 여러 줄의 텍스트를 입력할 수 있으며 각 줄의 최대 문자 수는 192자입니다. 줄 사이에 **Enter**를 누릅니다.

입력 다음 줄에 **`ENDOFBUF`**를 입력하고 **Enter**를 눌러 완료합니다.

메시지 설정 대화 상자를 취소하려면 **`Ctrl`** 및 **`C`**를 누릅니다.

단계 **7** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

예

다음 예에서는 pre-login 배너를 생성합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

Pre-Login 배너 수정

프로시저

단계 **1** FXOS CLI에 연결합니다(액세스 - FXOS CLI 참고).

단계 **2** 보안 모드를 입력합니다.

Firepower-chassis# **scope security**

단계 **3** 배너 보안 모드로 들어갑니다.

Firepower-chassis /security # **scope banner**

단계 **4** pre-login-banner 배너 보안 모드로 들어갑니다.

Firepower-chassis /security/banner # **scope pre-login-banner**

단계 **5** 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인하기 전에 FXOS에서 사용자에게 표시해야 할 메시지를 지정합니다.

Firepower-chassis /security/banner/pre-login-banner # **set message**

pre-login 배너 메시지 텍스트를 입력하기 위한 대화 상자가 열립니다.

단계 **6** 프롬프트에서 pre-login 배너 메시지를 입력합니다. 이 필드에는 어떤 표준 ASCII 문자도 사용할 수 있습니다. 여러 줄의 텍스트를 입력할 수 있으며 각 줄의 최대 문자 수는 192자입니다. 줄 사이에 **Enter**를 누릅니다.

입력 다음 줄에 **ENDOFBUF**를 입력하고 **Enter**를 눌러 완료합니다.

메시지 설정 대화 상자를 취소하려면 **Ctrl** 및 **C**를 누릅니다.

단계 **7** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

예

다음 예에서는 pre-login 배너를 수정합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

Pre-Login 배너 삭제

프로시저

단계 **1** FXOS CLI에 연결합니다(액세스 - FXOS CLI 참고).

단계 **2** 보안 모드를 입력합니다.

Firepower-chassis# **scope security**

단계 **3** 배너 보안 모드로 들어갑니다.

Firepower-chassis /security # **scope banner**

단계 **4** 시스템에서 pre-login 배너를 삭제합니다.

Firepower-chassis /security/banner # **delete pre-login-banner**

단계 **5** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/banner* # **commit-buffer**

예

다음 예에서는 pre-login 배너를 삭제합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

Firepower 4100/9300 섀시 리부팅

프로시저

단계 **1** **Overview(**개요**)**를 선택하여 Overview(개요) 페이지를 엽니다.

단계 **2** Overview(개요) 페이지 오른쪽 위에서 Chassis Uptime(섀시 업타임) 옆에 있는 **Reboot(**리부팅**)**를 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 Firepower 4100/9300 섀시의 전원 끄기를 확인합니다.
시스템에 구성된 모든 논리적 디바이스가 정상적으로 셧다운된 후 각 보안 모듈/엔진의 전원이 꺼지고, 마지막으로 Firepower 4100/9300 섀시의 전원이 꺼진 후 재시작됩니다. 이 프로세스는 보통 15~20분 정도 걸립니다.

Firepower 4100/9300 섀시 전원 끄기

프로시저

단계 **1** **Overview(**개요**)**를 선택하여 Overview(개요) 페이지를 엽니다.

단계 **2** Overview(개요) 페이지 오른쪽 위에서 Chassis Uptime(섀시 업타임) 옆에 있는 **Shutdown(**셧다운**)**을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 Firepower 4100/9300 섀시의 전원 끄기를 확인합니다.
시스템에 구성된 모든 논리적 디바이스가 정상적으로 셧다운된 후 각 보안 모듈/엔진의 전원이 꺼지고, 마지막으로 Firepower 4100/9300 섀시의 전원이 꺼집니다.

공장 기본 구성 복원

FXOS CLI를 사용하여 Firepower 4100/9300 섀시를 공장 기본 구성으로 복원할 수 있습니다.

참고 이 프로세스는 모든 논리적 디바이스 구성을 포함하여 섀시의 모든 사용자 구성을 지웁니다. 이 절차를 완료한 후 시스템을 재구성해야 합니다(초기 구성 참조).

프로시저

단계 **1** (선택 사항) **erase configuration** 명령은 섀시에서 스마트 라이선스 구성을 제거하지 않습니다. 스마트 라이선스 구성을 제거하려는 경우에도 다음 단계를 수행합니다.

scope license

deregister

Firepower 4100/9300 섀시를 등록 취소하면 계정에서 디바이스가 제거됩니다. 디바이스의 모든 라이선스 엔타이틀먼트 및 인증서가 제거됩니다.

단계 **2** 로컬 관리 셸에 연결합니다.

connect local-mgmt

단계 **3** Firepower 4100/9300 섀시에서 모든 사용자 구성을 지우고 섀시를 원래 공장 기본 구성으로 복원하려면 다음 명령을 입력합니다.

erase configuration

시스템에서 모든 사용자 구성을 지울지 확인하는 메시지를 표시합니다.

단계 **4** 명령 프롬프트에 **yes**를 입력하여 구성을 지운다는 것을 확인합니다.
모든 사용자 구성이 Firepower 4100/9300 섀시에서 지워진 후 시스템이 재부팅됩니다.

시스템 구성 요소를 안전하게 지우기

FXOS CLI를 사용하여 어플라이언스의 구성 요소를 지우고 안전하게 지울 수 있습니다.

erase configuration 명령은 공장 기본 구성 복원, 19 페이지에 설명된 대로 섀시에서 모든 사용자 구성 정보를 제거하고 원래 공장 기본 구성으로 복원합니다.

secure erase 명령은 지정된 어플라이언스 구성 요소를 안전하게 지웁니다. 즉, 데이터만 삭제되는 것이 아니라 물리적 스토리지가 "삭제"됩니다(완전히 지워짐). 이는 하드웨어 스토리지 구성 요소가 잔여 데이터 또는 스텁을 유지하지 않으므로 어플라이언스를 전송하거나 반품할 때 중요합니다.

참고 보안 지우기 중에 디바이스가 재부팅되고, SSH 연결이 종료됩니다. 따라서 직렬 콘솔 포트 연결을 통해 보안 지우기를 수행하는 것이 좋습니다.

프로시저

단계 **1** 로컬 관리 셸에 연결합니다.

connect local-mgmt

단계 **2** 다음 **erase configuration** 명령 중 하나를 입력하여 지정된 어플라이언스 구성 요소를 안전하게 지웁니다.

a) **erase configuration chassis**

모든 데이터와 이미지가 손실되며 복구할 수 없다는 경고 메시지가 표시되고 계속 진행할 것인지 확인하는 메시지가 표시됩니다. **y**를 입력하면, 전체 섀시가 안전하게 지워집니다. 보안 모듈이 먼저 지워지고 수퍼바이저가 지워집니다.

디바이스의 모든 데이터와 소프트웨어가 지워지므로 ROMMON(ROM 모니터)에서만 디바이스 복구를 수행할 수 있습니다.

b) **erase configuration security_module** *module_id*

모듈의 모든 데이터와 이미지가 손실되어 복구할 수 없다는 경고 메시지가 표시되고, 계속 진행할 것인지 확인하는 메시지가 표시됩니다. **y**를 입력하면 모듈이 지워집니다.

참고 **decommission-secure** 명령은 기본적으로 이 명령과 동일한 결과를 생성합니다.

보안 모듈은 삭제된 후 승인될 때까지 중단된 상태로 유지됩니다(해제되는 모듈과 유사).

c) **erase configuration supervisor**

모든 데이터와 이미지가 손실되며 복구할 수 없다는 경고 메시지가 표시되고, 계속 진행할 것인지 확인하는 메시지가 표시됩니다. **y**를 입력하면 수퍼바이저가 안전하게 지워집니다.

수퍼바이저의 모든 데이터와 소프트웨어가 지워지므로 ROMMON(ROM 모니터)에서만 디바이스 복구를 수행할 수 있습니다.