升級Firepower裝置上的ASA HA配對

目錄

簡介

本檔案介紹在firepower硬體裝置上安裝的高可用性(HA)對調適型安全裝置(ASA)的升級程式。

必要條件

需求

思科建議您瞭解以下主題：

- ASA管理
- ASA故障轉移

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 2個運行代碼2.0.1-86的FP4150
- ASA 9.6.2.1（升級到9.6.2.3）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

配置HA（主用/備用或主用/主用）時，在Firepower裝置（FPR4100、FPR9300等）上安裝的

ASA模組的升級過程在Firepower可擴展操作系統(FXOS)配置指南中進行了介紹。以下是相關部分：

Updating the Image Version for a Logical Device

Before You Begin

Download the application image you want to use for the logical device from Cisco.com (see Downloading Images from Cisco.com) and then upload that image to the FXOS chassis (see Uploading an Image to the Firepower Security Appliance).

If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.

✎ **Note**   You cannot directly upgrade a Firepower Threat Defense logical device. To upgrade a Firepower Threat Defense logical device, you must delete the existing device and then create a new one using the updated image.
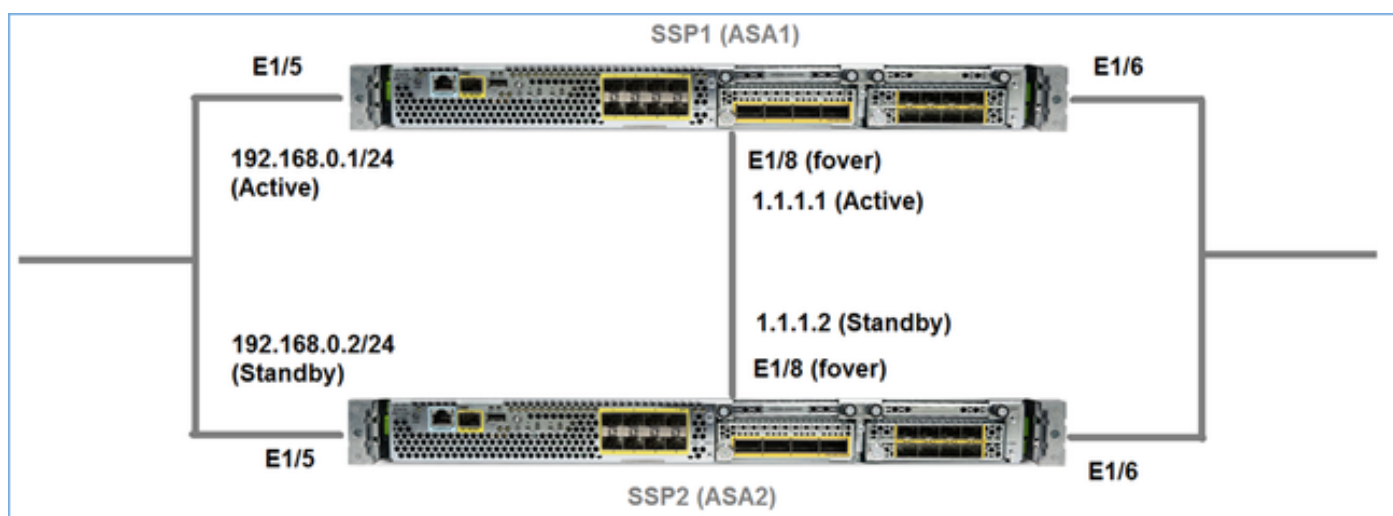
Procedure

Step 1   Choose **Logical Devices** to open the Logical Devices page. The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

Step 2   Click **Update Version** for the logical device that you want to update to open the **Update Image Version** dialog box.

Step 3   For the **New Version**, choose the software version to which you want to update.

Step 4   Click **OK**.

本文的目標是對HA環境中的升級過程提供更為詳細的概述。

附註：本文檔假定目標ASA版本與現有的FXOS版本相容，因此在此情況下不需要升級FXOS捆綁包。請始終檢查FXOS相容性矩陣，確認目標ASA版本是否與FXOS映像相容。如果沒有，則按照FXOS發行說明中的說明先升級FXOS映像。

設定

網路圖表

在Firepower機箱管理器(FCM)UI中看到ASA1：

ASA2:

任務1.從思科軟體下載頁面下載ASA映像

導覽至Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls(NGFW)，然後選擇硬體平台（例如4100、9000等），如下圖所示。

任務2.將ASA映像上傳到Firepower機箱管理器

將ASA映像上傳到Firepower機箱。可從Firepower機箱管理器(FCM)UI或FXOS命令列介面(CLI)執行此操作。

方法1.從FCM UI上傳ASA映像。

導航到System > Updates。選擇Upload Image，指定檔名並選擇Upload:
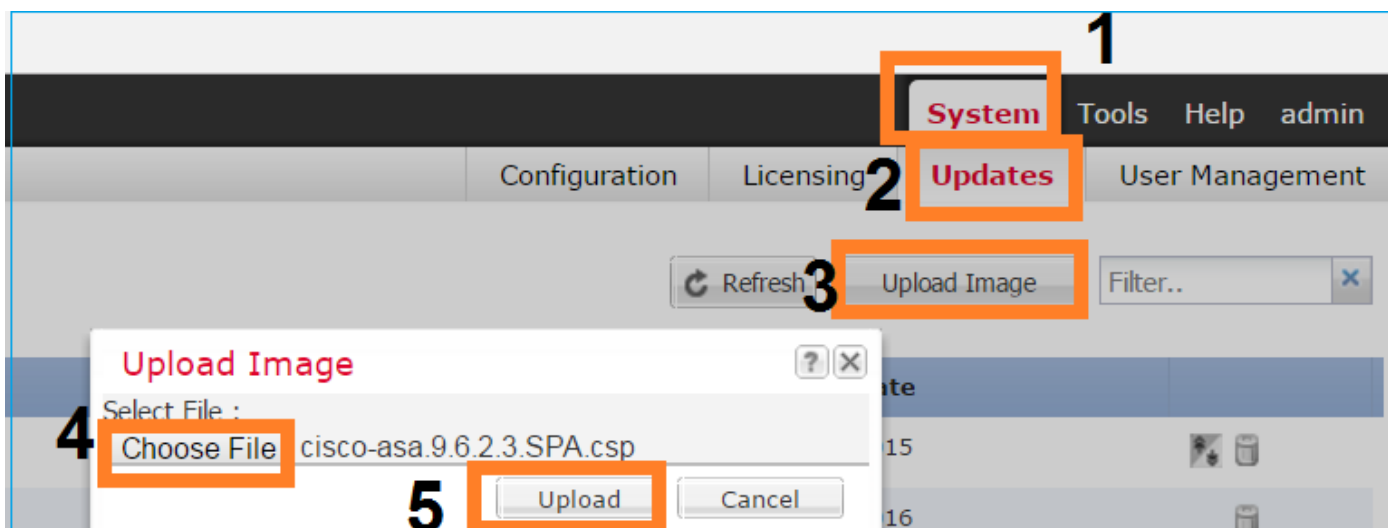
方法2.從FXOS CLI上傳ASA映像。

您可以從FTP、SCP、SFTP或TFTP伺服器上傳映像。要驗證機箱管理介面和遠端伺服器之間的連線，請執行以下操作：

```
FPR4100# connect local-mgmt
FPR4100(local-mgmt)# ping 10.48.40.70
PING 10.48.40.70 (10.48.40.70) from 10.62.148.88 eth0: 56(84) bytes of data.
64 bytes from 10.48.40.70: icmp_seq=1 ttl=61 time=34.4 ms
64 bytes from 10.48.40.70: icmp_seq=2 ttl=61 time=34.3 ms
64 bytes from 10.48.40.70: icmp_seq=3 ttl=61 time=34.3 ms
```

若要傳輸ASA映像，請導航到此範圍並運行download image命令：

```
FPR4100# scope ssa
FPR4100 /ssa # scope app-software
FPR4100 /ssa/app-software # download image ftp://ftp_username@ 10.48.40.70/cisco-
asa.9.6.2.3.SPA.csp
Password:
```

若要監控映像傳輸進度，請執行show download-task detail命令：

```
FPR4100 /ssa/app-software # show download-task detail

Downloads for Application Software:
    File Name: cisco-asa.9.6.2.3.SPA.csp
    Protocol: Ftp
    Server: 10.48.40.70
    Port: 0
    Userid: anonymous
    Path:
    Downloaded Image Size (KB): 94214
    Time stamp: 2016-12-08T10:21:56.775
    State: Downloading
    Transfer Rate (KB/s): 450.784698
    Current Task: downloading image cisco-asa.9.6.2.3.SPA.csp from 10.48.40.70(FSM-
STAGE:sam:dme:ApplicationDownloaderDownload:Local)
```

您也可以使用以下命令驗證傳輸是否成功：

```
FPR4100 /ssa/app-software # show download-task
```

```
Downloads for Application Software:
    File Name                       Protocol   Server          Port      Userid       State
    ------------------------------- ---------- --------------- --------- ------------ -----
    cisco-asa.9.6.2.2.SPA.csp       Ftp        10.48.40.70               0 anonymous  Downloaded
```

有關其他詳細資訊：

```
FPR4100 /ssa/app-software # show download-task fsm status expand

File Name: cisco-asa.9.6.2.3.SPA.csp

    FSM Status:

        Affected Object: sys/app-catalogue/dnld-cisco-asa.9.6.2.3.SPA.csp/fsm
        Current FSM: Download
        Status: Success
        Completion Time: 2016-12-08T10:26:52.142
        Progress (%): 100

        FSM Stage:

        Order   Stage Name                               Status        Try
        ------  ---------------------------------------  ------------  ---
        1       DownloadLocal                            Success       1
        2       DownloadUnpackLocal                      Success       1
```

ASA映像顯示在機箱儲存庫中：

```
FPR4100 /ssa/app-software # exit
FPR4100 /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.6.2.1    N/A         cisco      Native      Application No
    asa        9.6.2.3    N/A         cisco      Native      Application No
```

任務3.升級第一個ASA裝置

首先升級備用ASA裝置，如下圖所示：
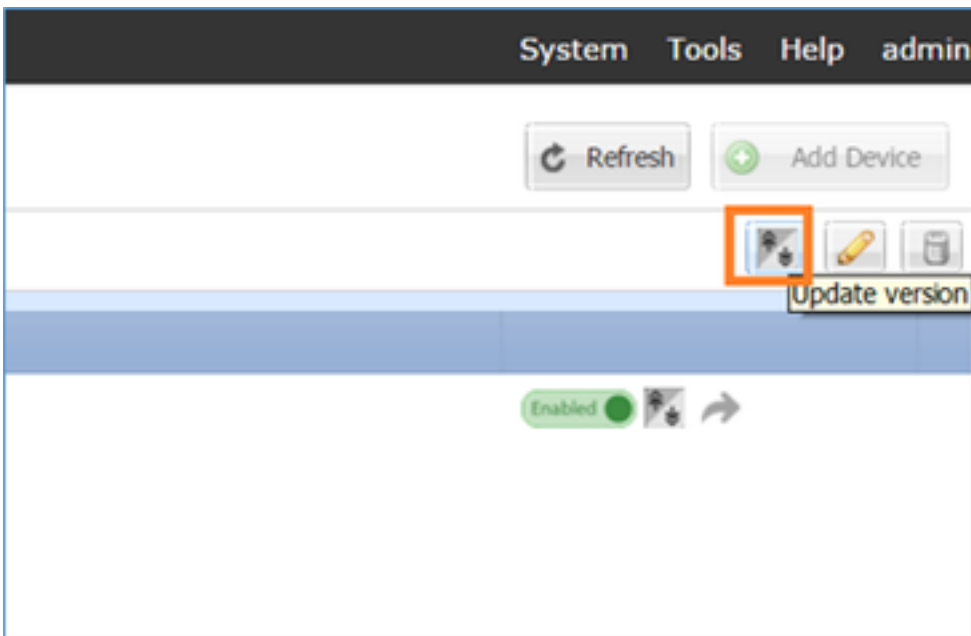
指定新映像並選擇**確定**以開始升級：
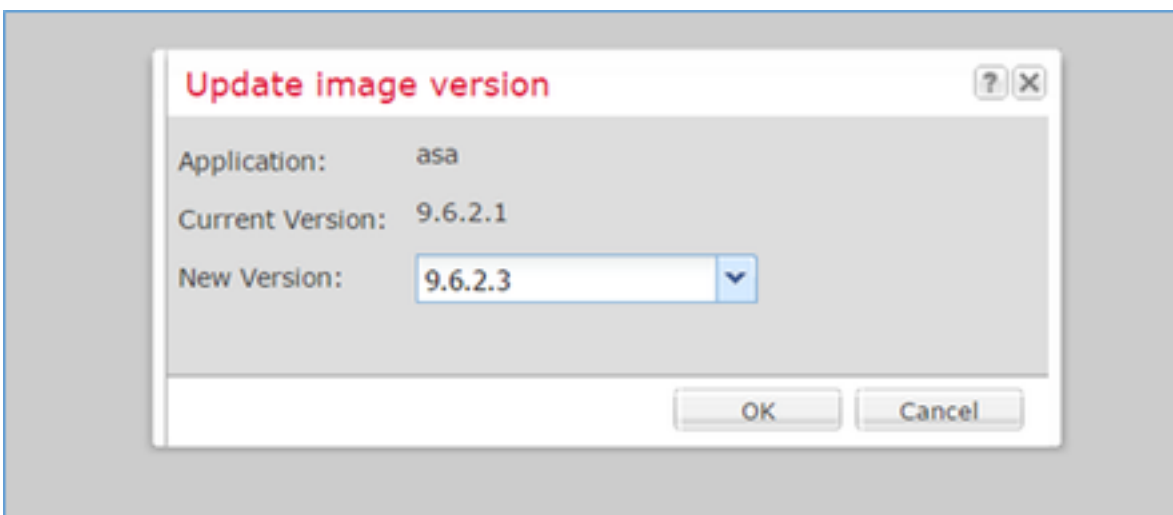
驗證

從FCM GUI升級ASA的進度：
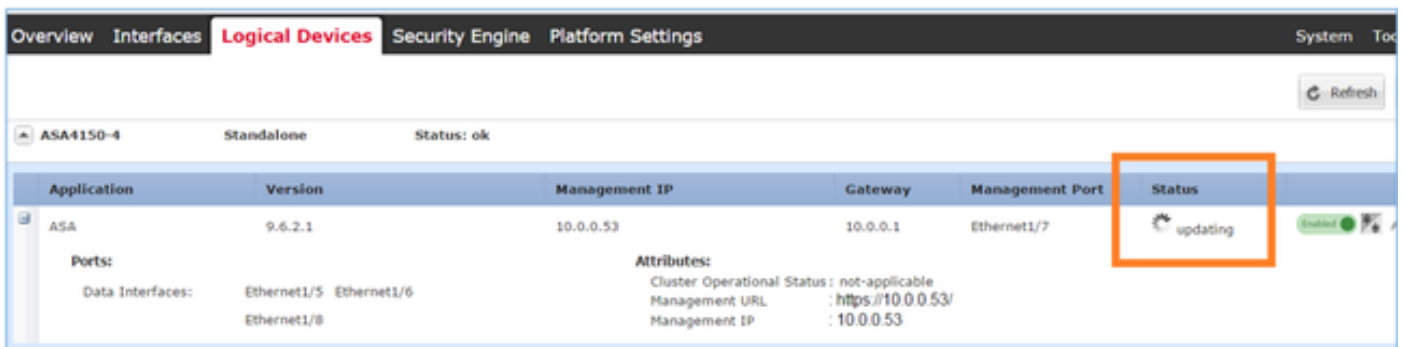
1-2分鐘後，FCM UI顯示：
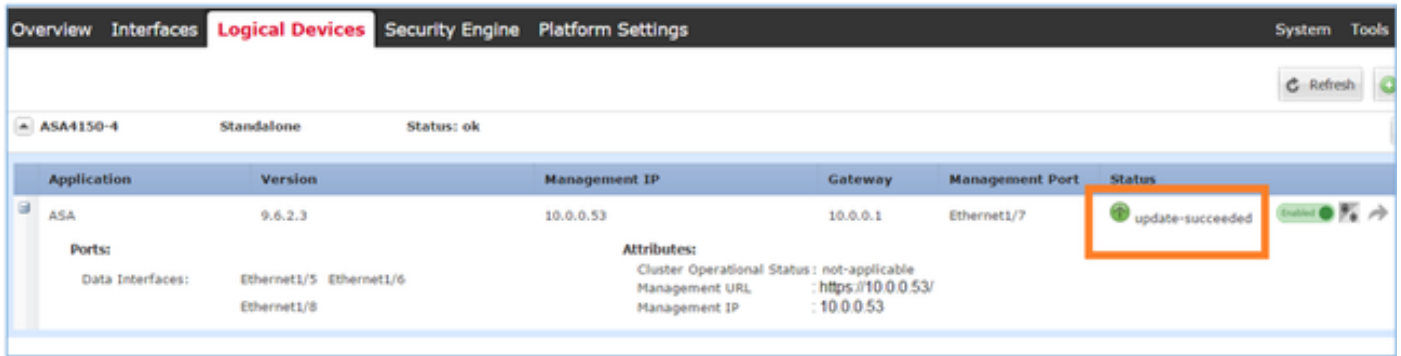
ASA模組重新載入：
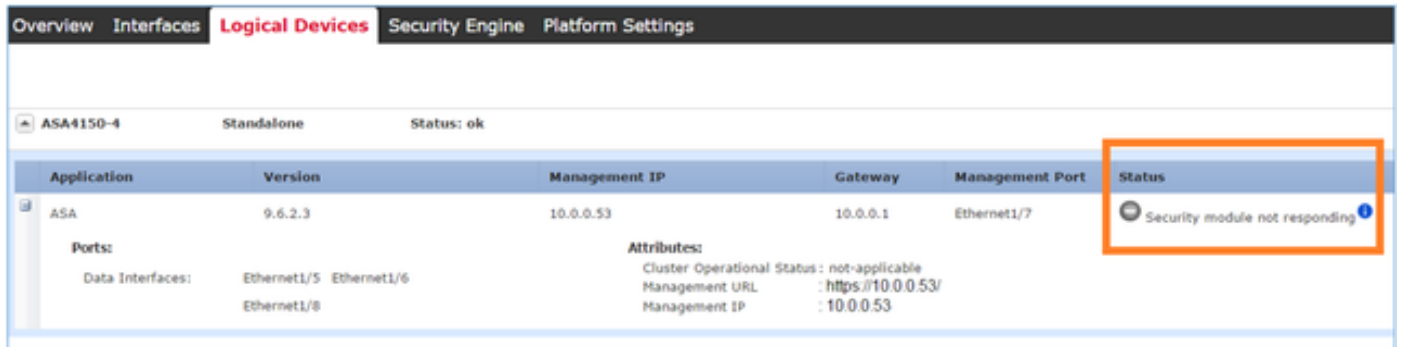
從Firepower機箱CLI升級ASA的過程。

CLI顯示邏輯裝置(ASA)重新啟動。從以下輸出中的模組引導CLI執行整個升級過程：

```
asa/sec/stby(config)#
[screen is terminating]
Disconnected from asa console!
Firepower-module1>
INIT: SwitchingStopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd (pid 5738)
.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid 5742)
acpid: exiting

acpid.
Stopping system message bus: dbus.
Stopping ntpd: stopped process in pidfile '/var/run/ntp.pid' (pid 6186)
done
Stopping crond: OK
Deconfiguring network interfaces... done.
Sending all processes the TERM signal...
SIGKILL_ALL will be delayed for 1 + 5 secs
Sending all processes the KILL signal...
Deactivating swap...
Unmounting local filesystems...
Rebooting... [ 1679.605561] Restarting system.

 Cisco Systems, Inc.
 Configuring and testing memory..

 Cisco Systems, Inc.
 Configuring and testing memory..
 Configuring platform hardware...
Bios Version : FXOSSM1.1.2.1.3.031420161207
Platform ID  : FXOSSM1
Processor(s) Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
```

```
Total Memory  = 256 GB Effective Memory = 256 GB
Memory Operating Speed 2400 Mh

Please wait, preparing to boot..
....................................................................................
.........
UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x0005000B). Revision 1.02
Mapping table
      fs0: Alias(s):HD17a65535a1:;blk1:
           PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(1,MBR,0x000EC692,0x800,0xEE6800)
     blk0: Alias(s):
           PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)
     blk2: Alias(s):
           PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(2,MBR,0x000EC692,0xEE7000,0x3BA000)
     blk3: Alias(s):

PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(3,MBR,0x000EC692,0x12A1000,0x950000)
     blk4: Alias(s):

PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(4,MBR,0x000EC692,0x1BF1000,0x2CD20800)
     blk5: Alias(s):

PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(4,MBR,0x000EC692,0x1BF1000,0x2CD20800)/HD(1,M
BR,0x00000000,0x1BF1800,0x5D22000)
     blk6: Alias(s):

PciRoot(0x0)/Pci(0x1F,0x2)/Sata(0x0,0xFFFF,0x0)/HD(4,MBR,0x000EC692,0x1BF1000,0x2CD20800)/HD(2,M
BR,0x00000000,0x7914000,0x26FFD800)
To launch ROMMON.

CpuFrequency = 2200002 KHz
Cisco FXOSSM1 Blade Rommon 1.2.1.3, Mar 14 2016 12:11:29
Platform: SSPXRU

INFO: enic_identify: Enabling Cruz driver...
INFO: enic_identify: Cruz driver enabled.
INFO: init_spi_interface: HSFS_BERASE_4K.
INFO: enic_init: bar[0].vaddr 0xc6e00000.
INFO: enic_init: bar[2].vaddr 0xc6e10000.
INFO: enic_init: eNic port MTU is 1500.
INFO: enic_init: eNic bsize 1500 ring size 512.
INFO: enic_init: Waiting for Cruz link...
INFO: enic_init: Cruz link detected.
INFO: nb_eth_app_init: MAC address for interface 0: 00 15 a5 01 01 00
INFO: nb_eth_app_init: IP address 127.128.1.254

Start communicating with MIO in blade slot 1...
INFO: Allocated 1000 bytes of memory for cmd at 0x78a7d018.
INFO: Allocated 1000 bytes of memory for status at 0x76d34918.
INFO: Allocated 196608 bytes of memory for key file at 0x76d03018.
INFO: Status code 1: 'rommon initialize is completed'.

INFO: tftp_open: '/rommon/status_1.txt'@127.128.254.1 via 127.128.254.1
!
INFO: nb_tftp_upload: 31 bytes sent.
tftpget 0x78a7d018 1000
INFO: tftp_open: '/rommon/command_1.txt'@127.128.254.1 via 127.128.254.1
Received 154 bytes
WARNING: retrieve_mio_cmd_info: Invalid checksum 0x0.
tftpget 0x76d03018 196608
INFO: tftp_open: 'rommon/key_1.bin'@127.128.254.1 via 127.128.254.1
!
Received 131072 bytes
INFO: Status code 8: 'rommon succeeds to retrieve key file'.
```

```
INFO: tftp_open: '/rommon/status_1.txt'@127.128.254.1 via 127.128.254.1
!
INFO: nb_tftp_upload: 31 bytes sent.
INFO: Primary keys in flash are up-to-date.
INFO: Backup keys in flash are up-to-date.
continue check local image
the image file path: installables/chassis/fxos-lfbff-k8.9.6.2.2.SPA
the image file name only: fxos-lfbff-k8.9.6.2.2.SPA
local_image_file: fs0:fxos-lfbff-k8.9.6.2.2.SPA
INFO: File 'fs0:fxos-lfbff-k8.9.6.2.2.SPA' has 104831328 bytes.
local_image_file_size 104831328
Found image fs0:fxos-lfbff-k8.9.6.2.2.SPA in local storage, boot local image.
set pboot_image fxos-lfbff-k8.9.6.2.2.SPA
INFO: File 'fs0:fxos-lfbff-k8.9.6.2.2.SPA' has 104831328 bytes.
INFO: 'fs0:fxos-lfbff-k8.9.6.2.2.SPA' has 104831328 bytes
INFO: Booting LFBFF image...
INFO: Status code 7: 'rommon about to verify image signature from local disk'.
INFO: tftp_open: '/rommon/status_1.txt'@127.128.254.1 via 127.128.254.1
!
INFO: nb_tftp_upload: 31 bytes sent.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.2.2.SPA ciscodmasz=786432 cisconrsvsz=2359296
hugepagesz=1g hugepages=24 ssp_mode=0
No Partitions for HDD2.. Creating partition..
mount: special device /dev/sdb1 does not exist
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.2.2.SPA ciscodmasz=786432 cisconrsvsz=2359296
hugepagesz=1g hugepages=24 ssp_mode=0
Create libvirt group
Start libvirtd Service
 * Starting virtualization library daemon: libvirtd
no /usr/bin/dnsmasq found; none killed
2016-12-07 12:47:24.090+0000: 4373: info : libvirt version: 1.1.2
2016-12-07 12:47:24.090+0000: 4373: warning : virGetHostname:625 : getadd[ ok ]failed for
'ciscoasa': Name or service not known
Disable the default virtual networks
Network default destroyed

Done with libvirt initialization
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.2.2.SPA ciscodmasz=786432 cisconrsvsz=2359296
hugepagesz=1g hugepages=24 ssp_mode=0
+++++++++++++++ BOOT CLI FILES COPIED ++++++++++++++++++++++++++
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.2.2.SPA ciscodmasz=786432 cisconrsvsz=2359296
hugepagesz=1g hugepages=24 ssp_mode=0
Turbo Boost is UNSUPPORTED on this platform.
Configuration Xml found is /opt/cisco/csp/applications/configs/cspCfg_cisco-
asa.9.6.2.3__asa_001_JAD201200C64A93395.xml
INIT: Entering runlevel: 3
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic=1
ide_generic.probe_mask=0x1 ide1=noprobe pci=nocrs processor.max_cstate=1 iommu=pt
platform=sspxru boot_img=disk0:/fxos-lfbff-k8.9.6.2.2.SPA ciscodmasz=786432 cisconrsvsz=2359296
hugepagesz=1g hugepages=24 ssp_mode=0
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
```

```
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up

acpid: 1 rule loaded

acpid: waiting for events: event logging is off

Starting ntpd: done
Starting crond: OK
            Cisco Security Services Platform
                 Type ? for list of commands
Firepower-module1>
Firepower-module1>show services status
Services currently running:
Feature   | Instance ID    |    State    |        Up Since
------------------------------------------------------------
asa       | 001_JAD201200C64A93395 |    RUNNING  |  :00:00:20
Firepower-module1>
```

整個過程大約需要5分鐘。

您還可以從機箱CLI使用show app-instance命令驗證ASA應用程式是否已聯機運行:

```
FPR4100# scope ssa
FPR4100 /ssa # show app-instance
Application Name      Slot ID    Admin State    Operational State  Running Version Startup
Version Cluster Oper State
-------------------- ---------- --------------- ------------------ --------------- -------------
-- ------------------
asa                   1          Enabled        Online             9.6.2.3          9.6.2.3
Not Applicabl
```

ASA模組相互發現:

```
asa/sec/actNoFailover>
*************WARNING****WARNING****WARNING****************************** Mate version 9.6(2)1
is not identical with ours 9.6(2)3
*************WARNING****WARNING****WARNING*******************************
.
        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

asa/sec/stby>
```

驗證

```
FPR4100# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect asa
asa> enable
Password:
asa/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: fover Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 1041 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.6(2)3, Mate 9.6(2)1
Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U
Last Failover at: 12:48:23 UTC Dec 7 2016
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)3) status (Up Sys)
                  Interface INSIDE (192.168.0.2): Normal (Not-Monitored)
                  Interface OUTSIDE (192.168.1.2): Normal (Monitored)
                  Interface management (0.0.0.0): Normal (Waiting)
        Other host: Primary - Active
                Active time: 10320 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)1) status (Up Sys)
                  Interface INSIDE (192.168.0.1): Normal (Not-Monitored)
                  Interface OUTSIDE (192.168.1.1): Normal (Monitored)
                  Interface management (10.0.0.50): Normal (Waiting)
...
```

要確認ASA裝置之間的正確故障轉移操作，請運行以下命令：

- show conn count
- show xlate count
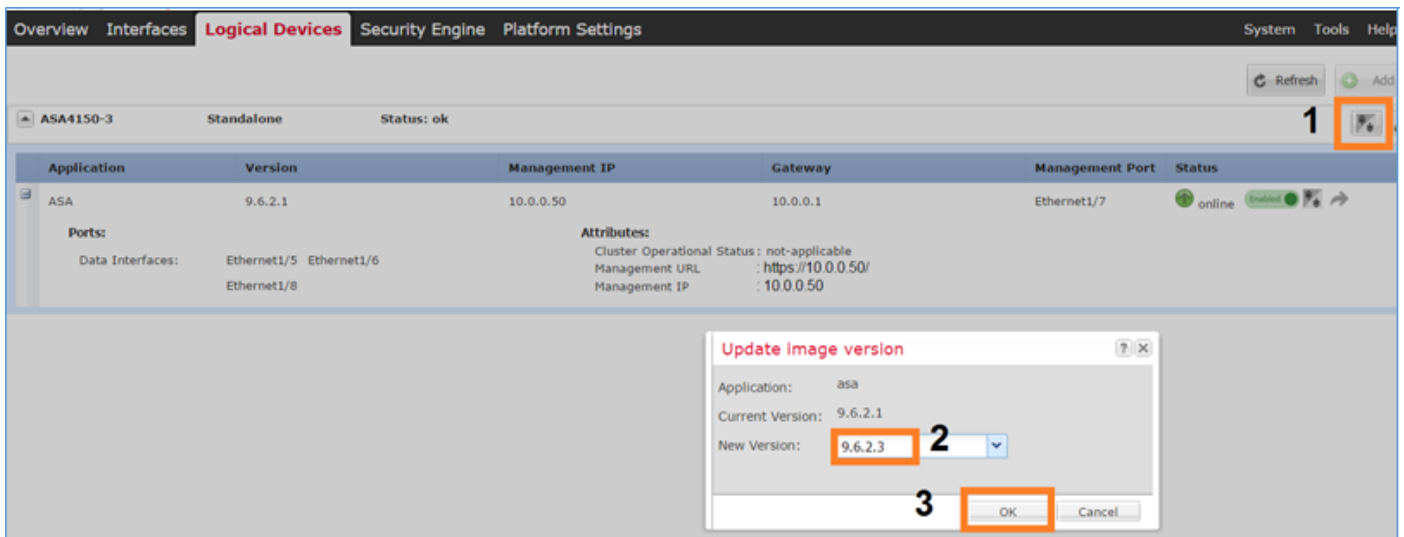- show crypto ipsec sa

任務4.升級第二台ASA裝置

切換故障轉移對等項並升級主ASA:

```
asa/sec/stby# failover active

        Switching to Active
asa/sec/act#
```

指定新映像並開始升級：

5分鐘後，升級完成。

驗證

從機箱CLI驗證ASA應用已聯機:

```
FPR4100# scope ssa
FPR4100 /ssa # show app-instance
Application Name    Slot ID    Admin State    Operational State  Running Version Startup
Version Cluster Oper State
------------------- ---------- -------------- ------------------ --------------- -------------
-- -----------------
asa                 1          Enabled        Online             9.6.2.3         9.6.2.3
Not Applicable
```

從ASA模組驗證故障切換操作：

```
asa/pri/stby# show failover
Failover On
Failover unit Primary
Failover LAN Interface: fover Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 1041 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.6(2)3, Mate 9.6(2)3
Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW
Last Failover at: 14:35:37 UTC Dec 7 2016
        This host: Primary - Standby Ready
                Active time: 0 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)3) status (Up Sys)
                  Interface INSIDE (192.168.0.2): Normal (Not-Monitored)
                  Interface OUTSIDE (192.168.1.2): Normal (Waiting)
                  Interface management (0.0.0.0): Normal (Waiting)
        Other host: Secondary - Active
                Active time: 656 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)3) status (Up Sys)
                  Interface INSIDE (192.168.0.1): Failed (Not-Monitored)
```

```
            Interface OUTSIDE (192.168.1.1): Normal (Waiting)
            Interface management (10.0.0.50): Normal (Waiting)

Stateful Failover Logical Update Statistics
      Link : fover Ethernet1/8 (up)
      Stateful Obj    xmit         xerr        rcv         rerr
      General         7            0           8           0
...
```

切換回故障切換以具有主/主用、輔助/備用：

```
asa/pri/stby# failover active

      Switching to Active
asa/pri/act#
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [FXOS配置指南](#)
- [FXOS-ASA相容性指南](#)
- [《 FXOS發佈說明》](#)
- [技術支援與文件 - Cisco Systems](#)