Troubleshooting

Packet Capture

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your Firepower 4100/9300 chassis. You can use the Packet Capture tool to log traffic that is going through specific interfaces on your Firepower 4100/9300 chassis.

You can create multiple packet capture sessions, and each session can capture traffic on multiple interfaces. For each interface included in a packet capture session, a separate packet capture (PCAP) file will be created.

Backplane Port Mappings

The Firepower 4100/9300 chassis uses the following mappings for internal backplane ports:

Security Module	Port Mapping	Description
Security Module 1/Security Engine	Ethernet1/9	Internal-Data0/0
Security Module 1/Security Engine	Ethernet1/10	Internal-Data0/1
Security Module 2	Ethernet1/11	Internal-Data0/0
Security Module 2	Ethernet1/12	Internal-Data0/1
Security Module 3	Ethernet1/13	Internal-Data0/0
Security Module 3	Ethernet1/14	Internal-Data0/1

Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Can capture only up to 100 Mbps.
- Packet capture sessions can be created even when there is not enough storage space available to run the packet capture session. You should verify that you have enough storage space available before you start a packet capture session.
- Does not support multiple active packet capturing sessions.
- Captures only at the ingress stage of the internal switch.
- Filters are not effective on packets that cannot be understood by the internal switch (for example Security Group Tag and Network Service Header packets).
- You can only capture packets for one subinterface per session, even if you have multiple subinterfaces on one or more parents.
- You cannot capture packets for an EtherChannel as a whole or for subinterfaces of an EtherChannel. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel. If you allocate a subinterface, but not the parent interface, then you cannot capture packets on member interfaces.
- You cannot copy or export a PCAP file while the capture session is still active.
- When you delete a packet capture session, all packet capture files associated with that session are also deleted.

Creating or Editing a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a packet capture session, click the **Capture Session** button.
- To edit an existing packet capture session, click the **Edit** button for that session.

The left side of the window lets you select a specific application instance and then shows a representation of that instance. This representation is used to select the interfaces on which you would like to capture packets. The right side of the window contains fields for defining the packet capture session.

Step 3 **Select an Instance** from the drop-down menu.

Step 4 Click the interfaces on which you want to capture traffic. Selected interfaces show a check mark.

Step 5 For subinterfaces, click the icon to the left of the parent interface to view subinterfaces in the **Subinterface selection** column. Click one subinterface in the column; you can only capture packets for one subinterface per capture session, even if you have multiple subinterfaces on one or more parents.

In the case of multiple subinterfaces, the icon will be labled **Subinterfaces(n)**; for a single subinterface, it will be labeled with the subinterface ID. If the parent interface is also allocated to the instance, you can either choose the parent interface or a subinterface; you cannot choose both. If the parent is not allocated, it will be grayed out. Subinterfaces for EtherChannels are not supported.

Step 6 To capture traffic from the logical device going out over the backplane ports:

a) Click the box representing the application instance.

The **Capture On**, **Application Port**, and **Application Capture Direction** fields are made available on the right side of the **Configure Packet Capture Session** window.

b) Select the backplane port you wish to capture traffic on or select **All Backplane Ports** from the **Capture On** drop-down list.

Step 7 Enter a name for the packet capture session in the **Session Name** field.

Step 8 Specify the buffer size to use for this packet capture session by selecting one of the pre-defined values from the **Buffer Size** list, or by selecting **Custom in MB** and then entering the desired buffer size. The specified buffer size must be between 1 and 2048 MB.

Step 9 Specify the length of the packet that you want to capture in the **Snap Length** field. Valid values are from 64 to 9006 bytes. The default snap length is 1518 bytes.

Step 10 Specify whether you want to overwrite existing PCAP files or append data to the PCAP files when this packet capture session is executed.

Step 11 To capture traffic between the application instance and a specific interface:

a) Click the box representing the logical device.
b) From the **Capture On** drop-down list, choose the application type (for example, **asa**).
c) Select the **Application Port** that you would like to capture traffic coming from or going to.
d) To capture only the traffic going from the logical device toward the specified interface, click the **Egress Packets** option next to **Application Capture Direction**.
e) To capture traffic coming from or going to the specified interface, click the **All Packets** option next to **Application Capture Direction**.

Step 12 To filter the traffic being captured:

a) Click the **Apply Filter** option for the **Capture Filter** field.

You are given a set of fields for configuring the filter.

b) If you need to create the filter, click **Create Filter**.

You see the **Create Packet Filter** dialog box. For more information, see Configuring Filters for Packet Capture, on page 4.

c) Select the filter you want to use from the **Apply** drop-down list.
d) Select the interface to which you want to apply the filter from the **To** drop-down list.
e) To apply additional filters, click **Apply Another Filter** and then repeat the steps above to apply the additional filter.

Step 13 Do one of the following:

- To save this packet capture session and run it now, click the **Save and Run** button. This option is only available if no other packet capture sessions are currently running.

- To save this packet capture session so that it can be ran at a later time, click the **Save** button.

You see the **Capture Session** tab with your session listed along with any other sessions that have been created. If you selected **Save and Run**, your packet capture session will be capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

Configuring Filters for Packet Capture

You can create filters to limit the traffic that is included in a packet capture session. You can select which interfaces should use a specific filter while creating a packet capture session.

Note If you modify or delete a filter that is applied to a packet capture session that is currently running, the changes will not take affect until you disable that session and then reenable it.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a filter, click the **Add Filter** button.
- To edit an existing filter, click the **Edit** button for that fitler.

You see the **Create or Edit Packet Filter** dialog box.

Step 3 Enter a name for the packet capture filter in the **Filter Name** field.

Step 4 To filter on a specific protocol, select it from the **Protocol** list, or select**Custom** and then enter the desired protocol. The custom protocol must be an IANA defined protocol in decimal format (0-255).

Step 5 To filter on a specific EtherType, select it from the **EtherType** list, or select**Custom** and then enter the desired EtherType. The custom EhterType must be an IANA defined EtherType in decimal format (for example, IPv4 = 2048, IPv6 = 34525, ARP = 2054, and SGT = 35081).

Step 6 To filter traffic based on an Inner VLAN (VLAN ID while ingressing the port) or Outer VLAN (VLAN ID added by the Firepower 4100/9300 chassis), enter the VLAN ID in the specified field.

Step 7 To filter traffic from a specific source or destination, enter the IP address and port or enter the MAC address in the specified source or destination fields.

Note You can filter using IPv4 or IPv6 addresses, but you cannot filter on both in the same packet capture session.

Step 8 Click **Save** to save the filter,

You see the **Filter List** tab with your filter listed along with any other filters that have been created.

Starting and Stopping a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To start a packet capture session, click the **Enable Session** button for that session and then click **Yes** to confirm.

Note You cannot start a packet capture session while another session is running.

The PCAP files for the interfaces included in the session will start collecting traffic. If the session is configured to overwrite session data, the existing PCAP data will be erased. If not, data will be appended to the existing file (if any).

While the packet capture session is running, the file size for the individual PCAP files will increase as traffic is captured. Once the Buffer Size limit is reached, the system will start dropping packets and you will see the Drop Count field increase.

Step 3 To stop a packet capture session, click the **Disable Session** button for that session and then click **Yes** to confirm.

After the session has been disabled, you can then download the PCAP files (see Downloading a Packet Capture File, on page 5).

Downloading a Packet Capture File

You can download the Packet Capture (PCAP) files from a session to your local computer so that they can be analyzed using a network packet analyzer.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To download the PCAP file for a specific interface from a packet capture session, click the **Download** button that corresponds to that interface.

Note You cannot download a PCAP file while a packet capture session is running.

Depending on your browser, the specified PCAP file is either automatically downloaded to your default download location or you are prompted to save the file.

Deleting Packet Capture Sessions

You can delete an individual packet capture session if it is not currently running or you can delete all inactive packet capture sessions.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To delete a specific packet capture session, click the **Delete** button that corresponds to that session.

Step 3 To delete all inactive packet capture sessions, click the **Delete All Sessions** button above the list of packet capture sessions.

Testing Network Connectivity

Before you begin

To test basic network connectivity by pinging another device on the network with its host name or IPv4 address, use the **ping** command. To ping another device on the network with its host name or IPv6 address, use the **ping6** command.

To trace the route to another device on the network with its host name or IPv6 address, use the **traceroute** command. To trace the route to another device on the network with its host name or IPv6 address, use the **traceroute6** command.

- The **ping** and **ping6** commands are available in `local-mgmt` mode.
- The **ping** command is also available in `module` mode.
- The **traceroute** and **traceroute6** commands are available in `local-mgmt` mode.
- The **traceroute** command is also available in `module` mode.

Procedure

Step 1 Connect to `local-mgmt` or `module` mode by entering one of the following commands:

- **connect local-mgmt**
- **connect module** *module-ID* {**console** | **telnet**}

Example:

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

Step 2 To test basic network connectivity by pinging another device on the network with its host name or IPv4 address:

ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

Example:

This example shows how to connect to ping another device on the network twelve times:

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

Step 3 To trace the route to another device on the network using its host name or IPv4 address:

traceroute {*hostname* | *IPv4_address*}

Example:

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1  198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

FP9300-A(local-mgmt)#
```

Step 4 (Optional) Enter **exit** to exit `local-mgmt` mode and return to the top-level mode.

Determine Port Channel Status

You can follow these steps to determine the status of currently defined port channels.

Procedure

Step 1 Enter `/eth-uplink/fabric` mode by entering the following commands:

- **scope eth-uplink**
- **scope fabric** {**a** | **b**}

Example:

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

Step 2 Enter the **show port-channel** command to display a list current port channels with the administrative state and operational state for each.

Example:

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    --------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members
    11              Port-channel11   Data               Enabl
ed     Failed           No operational members
    12              Port-channel12   Data               Disab
led    Admin Down       Administratively down
    48              Port-channel48   Cluster            Enabl
ed     Up

FP9300-A /eth-uplink/fabric #
```

Step 3 Enter `/port-channel` mode to display individual port-channel and port information by entering the following command:

- **scope port-channel** *ID*

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.
```

```
    <--- remaining lines removed for brevity --->

FP9300-A(fxos)#
```

Step 4 Enter the **show** command to display status information for the specified port channel.

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    --------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

Step 5 Enter the **show member-port** command to display status information for the port channel's member port(s).

Example:

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
    Port Name       Membership         Oper State       State Reas
on
    --------------- ------------------ ---------------- ----------
--
    Ethernet2/3     Suspended          Failed           Suspended
    Ethernet2/4     Suspended          Failed           Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

A port channel does not come up until you assign it to a logical device. If the port channel is removed from the logical device, or the logical device is deleted, the port channel reverts to a Suspended state.

Step 6 To view additional port channel and LACP information, exit `/eth-uplink/fabric/port-channel` mode and enter `fxos` mode by entering the following commands:

- **top**
- **connect fxos**

Example:

Step 7 Enter the **show port-channel summary** command to display summary information for the current port channels.

Example:

```
FP9300-A(fxos)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
------------------------------------------------------------
```

```
------------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------
------------------
10    Po10(SD)    Eth      LACP      Eth2/3(s)    Eth2/4(s)

11    Po11(SD)    Eth      LACP      Eth2/1(s)    Eth2/2(s)

12    Po12(SD)    Eth      LACP      Eth1/4(D)    Eth1/5(D)

48    Po48(SU)    Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

Additional **show port-channel** and **show lacp** commands are available in `fxos` mode. You can use these commands to display a variety of port channel and LACP information such as capacity, traffic, counters, and usage.

What to do next

See Add an EtherChannel (Port Channel) for information about creating port channels.

Recovering from a Software Failure

Before you begin

In the event of software failure that prevents the system from booting successfully, you can use the following procedure to boot a new version of software. To complete this process you need to TFTP boot a kickstart image, download new system and manager images, and then boot using the new images.

The recovery images for a specific FXOS version can be obtained from Cisco.com at one of the following locations:

- Firepower 9300—https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 Series—https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

The recovery images include three separate files. For example, below are the current recovery images for FXOS 2.1.1.64.

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

Procedure

Step 1 Access ROMMON:

a) Connect to the console port.

b) Reboot the system.

The system will start loading and during the process display a countdown timer.

c) Press the **Escape** key during the countdown to enter ROMMON mode.

Example:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

Step 2 TFTP boot a kickstart image:

a) Verify that the management IP address, management netmask, and gateway IP address are set correctly. You can see their values using the **set** command. You can test the connectivity to the TFTP server using the **ping** command.

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) Copy the kickstart image to a TFTP directory that is accessible from your Firepower 4100/9300 chassis.

Note The kickstart image version number will not match the bundle version number. Information showing the mapping between your FXOS version and the kickstart image can be found on the Cisco.com software download page.

c) Boot the image from ROMMON using the boot command:

```
boot tftp://<IP address>/<path to image>
```

Note You can also boot the kickstart from ROMMON using a USB media device inserted into the USB slot on the front panel of the Firepower 4100/9300 chassis. If the USB device is inserted while the system is running, you will need to reboot the system before it will recognize the USB device.

The system will display a series of #'s indicating that the image is being received and will then load the kickstart image.

Example:

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

############################################################################
############################################################################
############################################################################

File reception completed.
```

Step 3 Download the recovery system and manager images that match the kickstart image you just loaded to the Firepower 4100/9300 chassis:

a) To download the recovery system and manager images you will need to set the management IP address and gateway. You cannot download these images via USB.

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
```

```
switch(boot)(config)# exit
```

b) Copy the recovery system and manager images from the remote server to the bootflash:

switch(boot)# **copy** *URL* **bootflash:**

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*
- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname/path/image_name*

Example:

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) After the images have been successfully copied to the Firepower 4100/9300 chassis, make a symlink to the manager image from nuova-sim-mgmt-nsg.0.1.0.001.bin. This link tells the load mechanism which manager image to load. The symlink name should always be nuova-sim-mgmt-nsg.0.1.0.001.bin regardless of what image you are trying to load.

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Example:

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
```

```
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

Step 4 Load the system image that you just downloaded:

```
switch(boot)# load bootflash:<system-image>
```

Example:

```
switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful
...
System is coming up ... Please wait ...


Cisco FPR Series Security Appliance
FP9300-A login:
```

Step 5 After the recovery images have loaded, enter the following commands to prevent the system from trying to load the prior images:

Note This step should be performed immediately after loading the recovery images.

```
FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer
```

Step 6 Download and install the Platform Bundle image that you want to use on your Firepower 4100/9300 chassis. For more information, see Image Management.

Example:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2           0                  Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
```

```
FP9300-A /firmware #
```

Recovering from a Corrupted File System

Before you begin

If the Supervisor's onboard flash becomes corrupted and the system is no longer able to start successfully, you can use the following procedure to recover the system. To complete this process you need to TFTP boot a kickstart image, reformat the flash, download new system and manager images, and then boot using the new images.

Note This procedure includes reformatting the system flash. As a result, you will need to completely reconfigure your system after it has been recovered.

The recovery images for a specific FXOS version can be obtained from Cisco.com at one of the following locations:

- Firepower 9300—https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 Series—https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

The recovery images include three separate files. For example, below are the recovery images for FXOS 2.1.1.64.

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

Procedure

Step 1 Access ROMMON:

a) Connect to the console port.

b) Reboot the system.

The system will start loading and during the process display a countdown timer.

c) Press the **Escape** key during the countdown to enter ROMMON mode.

Example:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
```

```
Compiled Sun 01/01/1999 23:59:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

Step 2 TFTP boot a kickstart image:

a) Verify that the management IP address, management netmask, and gateway IP address are set correctly. You can see their values using the **set** command. You can test the connectivity to the TFTP server using the **ping** command.

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) Copy the kickstart image to a TFTP directory that is accessible from your Firepower 4100/9300 chassis.

Note The kickstart image version number will not match the bundle version number. Information showing the mapping between your FXOS version and the kickstart image can be found on the Cisco.com software download page.

c) Boot the image from ROMMON using the boot command:

```
boot tftp://<IP address>/<path to image>
```

Note You can also boot the kickstart from ROMMON using a USB media device inserted into the USB slot on the front panel of the Firepower 4100/9300 chassis. If the USB device is inserted while the system is running, you will need to reboot the system before it will recognize the USB device.

The system will display a series of #'s indicating that the image is being received and will then load the kickstart image.

Example:

```
rommon 1 > set
    ADDRESS=
```

```
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

############################################################################
############################################################################
############################################################################

File reception completed.
```

Step 3 After the kickstart image has loaded, reformat the flash using the **init system** command.

The **init system** command erases the contents of the flash including all software images downloaded to the system and all configurations on the system. The command takes approximately 20-30 minutes to complete.

Example:

```
switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.

Do you want to continue? (y/n)  [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting SAM partition:
```

```
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Sysdebug  partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
```

Step 4 Download the recovery images to the Firepower 4100/9300 chassis:

a) To download the recovery images you will need to set the management IP address and gateway. You cannot download these images via USB.

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

b) Copy all three recovery images from the remote server to the bootflash:

switch(boot)# **copy** *URL* **bootflash:**

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*
- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname/path/image_name*

Example:

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) After the images have been successfully copied to the Firepower 4100/9300 chassis, make a symlink to the manager image from nuova-sim-mgmt-nsg.0.1.0.001.bin. This link tells the load mechanism which manager image to load. The symlink name should always be nuova-sim-mgmt-nsg.0.1.0.001.bin regardless of what image you are trying to load.

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Example:

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

Step 5 Reload the switch:

```
switch(boot)# reload
```

Example:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.

!!  Rommon image verified successfully  !!


Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016  by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
```

```
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >
```

Step 6 Boot from the kickstart and system images:

```
rommon 1 > boot <kickstart-image> <system-image>
```

Note You will likely see license manager failure messages while the system image is loading. These messages can be safely ignored.

Example:

```
rommon 1 > dir
Directory of: bootflash:\

  01/01/12  12:33a <DIR>          4,096  .
  01/01/12  12:33a <DIR>          4,096  ..
  01/01/12  12:16a <DIR>         16,384  lost+found
  01/01/12  12:27a           34,333,696  fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  01/01/12  12:29a          330,646,465  fxos-k9-manager.4.1.1.69.SPA
  01/01/12  12:31a          250,643,172  fxos-k9-system.5.0.3.N2.4.11.69.SPA
  01/01/12  12:34a          330,646,465  nuova-sim-mgmt-nsg.0.1.0.001.bin
          4 File(s) 946,269,798 bytes
          3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
  !!   Kickstart Image verified successfully   !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[    0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan  1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful
```

```
...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

           ---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.


  You have chosen to setup a new Security Appliance. Continue? (y/n):
```

Step 7 After the images have loaded, the system will prompt you to enter initial configuration settings. For more information, see Initial Configuration Using Console Port.

Step 8 Download the Platform Bundle image that you want to use on your Firepower 4100/9300 chassis. For more information, see Image Management.

Example:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2            0                 Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

Step 9 Install the Platform Bundle image you downloaded in the previous step:

a) Enter auto-install mode:

Firepower-chassis /firmware # **scope auto-install**

b) Install the FXOS platform bundle:

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.1(1.73).

c) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

d) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

e) To monitor the upgrade process:

- Enter **scope firmware**.
- Enter **scope auto-install**.
- Enter **show fsm status expand**.

Step 10 If the Platform Bundle image that you installed corresponds with the images you used for recovering your system, you must manually activate the kickstart and system images so that they will be used when loading the system in the future. Automatic activation does not occur when installing a Platform Bundle that has same images as the recovery images that were used.

a) Set the scope for fabric-interconnect a:

```
FP9300-A# scope fabric-interconnect a
```

b) Use the **show version** command to view the running kernel version and the running system version. You will use these strings to activate the images.

```
FP9300-A /fabric-interconnect # show version
```

Note If the Startup-Kern-Vers and Startup-Sys-Vers are already set and match the Running-Kern-Vers and Running-Sys-Vers, you do not need to activate the images and can proceed to Step 11.

c) Enter the following command to activate the images:

```
FP9300-A /fabric-interconnect # activate firmware
  kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

Note The server status might change to "Disk Failed." You do not need to worry about this message and can continue with this procedure.

d) Use the **show version** command to verify that the startup versions have been set correctly and to monitor the activation status for the images.

Important Do not proceed to the next step until the status changes from "Activating" to "Ready."

```
FP9300-A /fabric-interconnect # show version
```

Example:

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers:
```

```
    Startup-Sys-Vers:
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
  5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Activating
    Act-Sys-Status: Activating
    Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

Step 11 Reboot the system:

Example:

```
FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #
```

The system will power down each security module/engine before finally powering down and then restarting the Firepower 4100/9300 chassis. This process takes approximately 5-10 minutes.

Step 12 Monitor the system status. The server status should go from "Discovery" to "Config" and then finally to "Ok".

Example:

```
FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Discovery             In Progress
1/2     Equipped                           Discovery             In Progress
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Config                Complete
1/2     Equipped                           Config                Complete
1/3     Empty

FP9300-A# show server status
```

```
Server  Slot Status                      Overall Status        Discovery
------- -------------------------------- --------------------- ---------
1/1     Equipped                         Ok                    Complete
1/2     Equipped                         Ok                    Complete
1/3     Empty
```

When the Overall Status is "Ok" your system has been recovered. You must still reconfigure your security appliance (including license configuration) and re-create any logical devices. For more information:

- Firepower 9300 Quick Start Guides—http://www.cisco.com/go/firepower9300-quick
- Firepower 9300 Configuration Guides—http://www.cisco.com/go/firepower9300-config
- Firepower 4100 Series Quick Start Guides—http://www.cisco.com/go/firepower4100-quick
- Firepower 4100 Series Configuration Guides—http://www.cisco.com/go/firepower4100-config

Restoring the Factory Default Configuration when the Admin Password is Unknown

This procedure returns your Firepower 4100/9300 chassis system to its default configuration settings, including the admin password. Use this procedure to reset the configurations on your device when the admin password is not known.

Note This procedure requires console access to the Firepower 4100/9300 chassis.

Procedure

Step 1 Connect your PC to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. For more information on the console cable, see Cisco Firepower 9300 Hardware Installation Guide .

Step 2 Power on the device. When you see the following prompt, press ESC to stop the boot.

Example:

```
!!  Rommon image verified successfully  !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015  by Cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: 00:00:00:00:00:00
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
 bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
rommon 1 >
```

Step 3 Make a note of the kickstart and system image names:

Example:

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

Step 4 Load the kickstart image:

rommon 1 > **boot** *kickstart_image*

Example:

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
 !! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab~302: No such file or directory (use -n flag to override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

Step 5 Enter the config terminal mode:

switch(boot) # **config terminal**

Example:

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 6 Reset the password and confirm the change:

switch(boot) (config) # **admin-password erase**

Note This step erases all configurations and returns your system to its default configuration settings.

Example:

```
switch(boot)(config)# admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n)  [n] y
```

Step 7 Exit the config terminal mode:

switch(boot) (config) # **exit**

Step 8 Load the system image noted in step 3 of this procedure and configure your system from scratch using the Initial Configuration Using Console Port task flow.

switch(boot) # **load** *system_image*

Example:

```
switch(boot)# load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

Disaster Recovery of a Firepower Threat Defense Cluster Member

Use this procedure to bring a Firepower 4100/9300 cluster member with Firepower Threat Defense back online and into a cluster after a disaster recovery scenario. Note that if the Firepower Threat Defense application versions associated with the clustered units are out of sync, you will have to follow the steps outlined in Updating the Image Version for a Logical Device to bring them up to the same version.

Before you begin

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server or your local computer. For more information, see About Configuration Import/Export.

Procedure

Step 1 Once the slave unit is up, restore the backup. For instructions on how to import the configuration, see Importing a Configuration File. The application installation starts.

Step 2 Accept the License Agreement.

Step 3 If necessary, set the application startup version so that the versions on each unit in the cluster match. For instructions on how to set the application startup version, see Updating the Image Version for a Logical Device.

Step 4 Once you have changed the application startup version, reinitialize the security module so that the Firepower Threat Defense running version matches the startup version.

a) Navigate to the Security Modules/Security Engine page.
b) Click on the **Reinitialize Security Engine** button.
c) Click Yes to confirm the change. The security module is reformatted and the application is reinstalled with the startup version.

The application comes online and joins the cluster.

Step 5 Verify that the application Startup Version and Running Version are the same.

a) In the FXOS CLI, enter Security Services mode:

firepower **scope ssa**

b) Show the application instance:

firepower /ssa # **show app-instance**

Example:

```
firepower /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile
 Name Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
------------ --------------- ------------
ftd        1          Enabled     Online           6.2.3.1624      6.2.3.1624
         In Cluster      Slave
```

Step 6 In the Firepower Management Center, delete the slave member. See "Delete a Slave Member" in the Firepower Management Center configuration guide.

Step 7 Re-add the recovered Firepower 9300/4100 slave unit to the Firepower Management Center. See "Replace a Cluster Member" in the Firepower Management Center configuration guide.