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 backplane or uplink interface is an internal interface that connects the security module (SM) to the internal switch. In case of 2 backplane interfaces per module, the internal switch and the applications on the modules perform traffic load-balancing over the 2 blackplane interfaces.The Firepower 4100/9300 chassis uses the following mappings for internal backplane ports:

Platform	Number of supported security modules	Backplane/uplink interfaces	Mapped application interfaces
Firepower 4100 (except Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	Internal-Data0/0
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10	Internal-Data0/0 Internal-Data0/1
		SM2: Ethernet1/11 Ethernet1/12	Internal-Data0/0 Internal-Data0/1
		SM3: Ethernet1/13 Ethernet1/14	Internal-Data0/0 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.
- For packet capture sessions on a single-wide 4x100Gbps or 2x100Gbps network module (part numbers FPR-NM-4X100G and FPR-NM-2X100G respectively), if the module `adminstate` is set to `off`, the capture session is automatically disabled with an "Oper State Reason: Unknown Error." You will have to restart the capture session after the module `adminstate` is set to `on` again.

  With all other network modules, packet capture sessions continue across module `adminstate` changes.
- 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 Enter packet capture mode:

Firepower-chassis # **scope packet-capture**

Step 2 Create a filter; see Configuring Filters for Packet Capture, on page 6.

You can apply filters to any of the interfaces included in a packet capture session.

Step 3 To create or edit a packet capture session:

Firepower-chassis /packet-capture # **enter session** *session_name*

Step 4 Specify the buffer size to use for this packet capture session:

Firepower-chassis /packet-capture/session* # **set session-memory-usage** *session_size_in_megabytes*

The specified buffer size must be between 1 and 2048 MB.

Step 5 Specify the length of the packet that you want to capture for this packet capture session:

Firepower-chassis /packet-capture/session* # **set session-pcap-snaplength** *session_snap_length_in_bytes*

The specified snap length must be between 64 and 9006 bytes. If you do not configure the session snap length, the default capture length is 1518 bytes.

Step 6 Specify the physical source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session. You cannot capture packets for an EtherChannel as a whole. 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 EtherChannel, then you cannot capture packets on member interfaces.

Note To remove a port from the packet capture session, use **delete** instead of **create** in the commands listed below.

a) Specify the physical port.

Firepower-chassis /packet-capture/session* # **create** {**phy-port | phy-aggr-port**} *port_id*

Example:

```
Firepower-chassis /packet-capture/session* # create phy-port Ethernet1/1
```

```
Firepower-chassis /packet-capture/session/phy-port* #
```

b) Capture packets on a subinterface.

Firepower-chassis /packet-capture/session/phy-port* # **set subinterface** *id*

You can only capture packets for one subinterface per capture session, even if you have multiple subinterfaces on one or more parents. Subinterfaces for EtherChannels are not supported. If the parent interface is also allocated to the instance, you can either choose the parent interface or a subinterface; you cannot choose both.

Example:

```
Firepower-chassis /packet-capture/session/phy-port* # set subinterface 100
Firepower-chassis /packet-capture/session/phy-port* #
```

c) For container instances, specify the container instance name.

Firepower-chassis /packet-capture/session/phy-port* # **set app-identifier** *instance_name*

Example:

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/phy-port* #
```

d) Specify the application type.

Firepower-chassis /packet-capture/session/phy-port* # **set app** *name*

Example:

```
Firepower-chassis /packet-capture/session/phy-port* # set app ftd
Firepower-chassis /packet-capture/session/phy-port* #
```

e) (Optional) Apply the desired filter.

Firepower-chassis /packet-capture/session/phy-port* # **set** {**source-filter**} *filtername*

Note To remove a filter from a port, use **set source-filter ""**.

f) Repeat the steps above as needed to add all desired ports.

Step 7 Specify the application source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session.

Note To remove a port from the packet capture session, use **delete** instead of **create** in the commands listed below.

a) Specify the application port.

Firepower-chassis /packet-capture/session* # **create app_port** *module_slot link_name interface_name app_name*

Syntax Description

module_slot	Security module in which the application is installed.

link_name	Any user descriptive name referring to the interface, for example, link1, inside_port1, etc.
interface_name	Interface attached to the application where packets need to be captured from, for example, Ethernet1/1, Ethernet2/2
app_name	Application installed on the module - ftd, asa

b) For container instances, specify the container instance name.

Firepower-chassis /packet-capture/session/app-port* # **set app-identifier** *instance_name*

Example:

```
Firepower-chassis /packet-capture/session/app-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/app-port* #
```

Syntax Description

instance_name	Name of the application instance for which packet capture is required, i.e., native or container

c) (Optional) Apply the desired filter.

Firepower-chassis /packet-capture/session/phy-port* # **set** {**source-filter**} *filtername*

Syntax Description

filtername	The filter name from the 'create filter' command under packet-capture scope

Note To remove a filter from a port, use **set source-filter ""**.

d) Repeat the steps above as needed to add all desired application ports.

Step 8 If you want to start the packet capture session now:

Firepower-chassis /packet-capture/session* # **enable**

Newly created packet-capture sessions are disabled by default. Explicit enabling of a session activates the packet capture session when the changes are committed. If another session is already active, enabling a session will generate an error. You must disable the already active packet-capture session before you can enable this session.

Step 9 Commit the transaction to the system configuration:

Firepower-chassis /packet-capture/session* # **commit-buffer**

If you enabled the packet capture session, the system will begin capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create session asa1inside
Firepower-chassis packet-capture/session # set session-memory-usage 256
Firepower-chassis packet-capture/session* # create phy-port Ethernet3/1
Firepower-chassis packet-capture/session* # create phy-aggr-port Ethernet2/1/1
```

```
Firepower-chassis packet-capture/session* # create app-port 1 link1 Ethernet 1/1 asa
Firepower-chassis packet-capture/session* # exit
Firepower-chassis packet-capture* # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcIP 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcPort 80
Firepower-chassis packet-capture/filter* # set destIP 10.10.10.10
Firepower-chassis packet-capture/filter* # set destPort 5050
Firepower-chassis packet-capture/filter* # exit
Firepower-chassis packet-capture/session* # scope phy-port Ethernet3/1
Firepower-chassis packet-capture/session/phy-port* # set src-filter interface1vlan100
Firepower-chassis packet-capture/session/phy-port* # exit
Firepower-chassis packet-capture/session* # scope app-port 1 link1 Ethernet1/1 asa
Firepower-chassis packet-capture/session/app-port* # set src-filter interface1vlan100
Firepower-chassis packet-capture/session/app-port* # exit
Firepower-chassis packet-capture/session* # enable
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/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 Enter packet capture mode:

Firepower-chassis # **scope packet-capture**

Step 2 To create a new packet capture filter:

Firepower-chassis /packet-capture # **create filter** *filter_name*

To edit an existing packet capture filter:

Firepower-chassis /packet-capture # **enter filter** *filter_name*

To delete an existing packet capture filter:

Firepower-chassis /packet-capture # **delete filter** *filter_name*

Step 3 Specify the filter details by setting one or more filter properties:

Firepower-chassis /packet-capture/filter* # **set** <*filterprop filterprop_value*

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

Table 1: Supported Filter Properties

ivlan	Inner VLAN ID (vlan of packet while ingressing port)
ovlan	Outer VLAN ID (vlan added by the Firepower 4100/9300 chassis)
srcip	Source IP Address (IPv4)
destip	Destination IP Address (IPv4)
srcipv6	Source IP Address (IPv6)
destipv6	Destination IP Address (IPv6)
srcport	Source Port Number
destport	Destination Port Number
protocol	IP Protocol [IANA defined Protocol values in decimal format]
ethertype	Ethernet Protocol type [IANA defined Ethernet Protocol type value in decimal format. For eg: IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081]
srcmac	Source Mac Address
destmac	Destination Mac Address

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcip 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcport 80
Firepower-chassis packet-capture/filter* # set destip 10.10.10.10
Firepower-chassis packet-capture/filter* # set destport 5050
Firepower-chassis packet-capture/filter* # commit-buffer
```

Starting and Stopping a Packet Capture Session

Procedure

Step 1 Enter packet capture mode:

Firepower-chassis # **scope packet-capture**

Step 2 Enter the scope for the packet capture session that you want to start or stop:

Firepower-chassis /packet-capture # **enter session** *session_name*

Step 3 To start a packet capture session:

Firepower-chassis /packet-capture/session* # **enable** [append | overwrite]

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

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 4 To stop a packet capture session:

Firepower-chassis /packet-capture/session* # **disable**

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /packet-capture/session* # **commit-buffer**

If you enabled the packet capture session, 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).

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # scope session asa1inside
Firepower-chassis packet-capture/session # enable append
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

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.

PCAP files are stored into the `workspace://packet-capture` directory and use the following naming conventions:

`workspace://packet-capture/session-<id>/<session-name>-<interface-name>.pcap`

Procedure

To copy a PCAP file from the Firepower 4100/9300 chassis:

Note You should stop the packet capture session before you download the PCAP files from that session.

a) Connect to local management:

Firepower-chassis # **connect localmgmt**

b) Copy the PCAP files:

copy *pcap_file copy_destination*

Example

```
Firepower-chassis# connect localmgmt
# copy workspace:/packet-capture/session-1/test-ethernet-1-1-0.pcap
scp://user@10.10.10.1:/workspace/
```

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 Enter packet capture mode:

Firepower-chassis # **scope packet-capture**

Step 2 To delete a specific packet capture session:

Firepower-chassis /packet-capture # **delete session** *session_name*

Step 3 To delete all inactive packet capture sessions:

Firepower-chassis /packet-capture # **delete-all-sessions**

Step 4 Commit the transaction to the system configuration:

Firepower-chassis /packet-capture* # **commit-buffer**

Example

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # delete session asa1inside
Firepower-chassis packet-capture* # commit-buffer
Firepower-chassis packet-capture #
```

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 IPv4 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.

Troubleshooting Management Interface Status

During initialization and configuration, if you suspect the management interface has not come up for some reason (for example, you cannot access the Chassis Manager), use the **show mgmt-port** command in the `local-mgmt` shell to determine the status of the management interface.

Note Do not use the **show interface brief** command in the `fxos` shell as it currently displays incorrect information.

Procedure

Step 1 Connect to `local-mgmt` mode by entering the following command:

- **connect local-mgmt**

Example:

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

Step 2 Use the **show mgmt-port** command to determine the status of the management interface.

Example:

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1648941394 (1.5 GiB)  TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#
```

You also can use the **show mgmt-ip-debug** command; however, it produces an extensive listing of interface-configuration information.

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 23:59:59.99 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:

Note Installation process typically takes between 15 and 20 minutes.

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 FXOS 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**.

Example:

```
TB10 /firmware/auto-install # show fsm status expand
    FSM Status:
        Affected Object: sys/fw-system/fsm
        Current FSM: Deploy
        Status: In Progress
        Completion Time:
        Progress (%): 98

        FSM Stage:
        Order  Stage Name                                Status       Try
        ------ ----------------------------------------- ------------ ---
        1      DeployWaitForDeploy                       Success      0
        2      DeployResolveDistributableNames           Skip         0
        3      DeployResolveDistributable                Skip         0
        4      DeployResolveImages                       Skip         0
        5      DeployValidatePlatformPack                Success      1
        6      DeployDebundlePort                        Success      0
        7      DeployPollDebundlePort                    Success      1
        8      DeployActivateUCSM                        Success      0
        9      DeployPollActivateOfUCSM                  Success      0
        10     DeployActivateMgmtExt                     Skip         0
        11     DeployPollActivateOfMgmtExt               Skip         0
        12     DeployUpdateIOM                           Skip         0
        13     DeployPollUpdateOfIOM                     Skip         0
        14     DeployActivateIOM                         Skip         0
        15     DeployPollActivateOfIOM                   Skip         0
        16     DeployActivateRemoteFI                    Skip         0
        17     DeployPollActivateOfRemoteFI              Skip         0
        18     DeployWaitForUserAck                      Skip         0
        19     DeployActivateLocalFI                     Success      0
        20     DeployPollActivateOfLocalFI               In Progress  1
```

Note Do not proceed to the next step until the status of the stages changes from "In Progress" to "Skip" or "Success."

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. This procedure erases any installed logical devices as well.

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 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
```

Generating Troubleshooting Log Files

You can generate log files to help with troubleshooting or to send to Cisco TAC if requested.

Procedure

Step 1 Connect to local management mode:

Firepower# connect local-mgmt

Step 2 (Optional) Enter the following command:

Firepower(local-mgmt)# show tech-support ?

The command output shows the components for which you can generate a troubleshooting file.

Example:

```
chassis  Chassis
fprm     Firepower Platform Management
module   Security Module
```

Step 3 Run the following command to generate a troubleshooting file:

Firepower(local-mgmt)# show tech-support <component keyword>

Make sure that you provide the required keyword for the component for which you want to generate a troubleshooting file. For example, the **module** keyword generates a troubleshooting file for the Security Module.

Make sure that you provide the required keyword for the component for which you want to generate a troubleshooting file. For example, the **fprm** keyword generates a troubleshooting file for the Platform Management.

Table 2: Components with Command Examples

Component	Command Example
Chassis	**Firepower (local-mgmt)# show tech-support chassis 1**
Firepower platform management	The **fprm** option was deprecated in version 2.8(1) and can no longer be used.
Security module	**Firepower (local-mgmt)# show tech-support module 1**

Example:

```
Firepower(local-mgmt)# show tech-support chassis 1 detail
```

```
The show tech support file will be located at
/workspace/techsupport/20191105041703_firepower-9300_BC1_all.tar

Initiating tech-support information task on FABRIC A ...

Initiating tech-support information task on Chassis 1 Fabric Extender 1 ...
Initiating tech-support information task on Chassis 1 CIMC 1 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/1 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/1 ...
Initiating tech-support information task on Chassis 1 CIMC 2 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/2 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/2 ...
Completed initiating tech-support subsystem tasks (Total: 8)
Waiting (Timeout: 900 Elapsed: 30) for completion of subsystem tasks (1/8).
Waiting (Timeout: 900 Elapsed: 50) for completion of subsystem tasks (2/8).
Waiting (Timeout: 900 Elapsed: 70) for completion of subsystem tasks (5/8).
Waiting (Timeout: 900 Elapsed: 90) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 110) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 130) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 150) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 170) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 190) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 210) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 230) for completion of subsystem tasks (7/8).
--More--
The detailed tech-support information is located at workspace:///techsupport/201--More--
91105041703_firepower-9300_BC1_all.tar
```

Similarly, you can also generate troubleshooting files from security module.

After a troubleshooting file generates, you can find the file in the workspace.

Step 4 Run the following command to confirm whether the file is generated:

dir workspace:/techsupport

Example:

```
1  34426880 Mar 05 13:10:05 2019 20190305130133_firepower-9300_FPRM.tar
1  56995840 Aug 27 05:30:37 2019 20190827052331_firepower-9300_FPRM.tar
1  56842240 Aug 27 12:42:42 2019 20190827123535_firepower-9300_FPRM.tar
1  87623680 Sep 17 06:27:57 2019 20190917062046_firepower-9300_FPRM.tar
1  87756800 Sep 17 10:22:38 2019 20190917101527_firepower-9300_FPRM.tar
1 152627200 Nov 05 04:30:10 2019 20191105041703_firepower-9300_BC1_all.tar

Usage for workspace://
3999125504 bytes total
476835840 bytes used
3317436416 bytes free
```

Note If you successfully generate files using all three parameters (fprm, chassis, and module), you should see them in the **/techsupport** directory.

Step 5 Run the following command.

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> ?

The output shows the supported protocols to allow copying the troubleshooting files from FXOS to your local computer. You can use any of the supported protocols.

Example:

```
Firepower(local-mgmt)# copy workspace:/techsupport/
20191105041703_firepower-9300_BC1_all.tar ?
  ftp:        Dest File URI
```

```
http:       Dest File URI
https:      Dest File URI
scp:        Dest File URI
sftp:       Dest File URI
tftp:       Dest File URI
usbdrive:   Dest File URI
volatile:   Dest File URI
workspace:  Dest File URI
```

Before copying a file from FXOS to your computer, make sure that the following prerequisites are met:

- The firewall on your local computer accepts incoming connection over any necessary ports. For example, if you copy a file over Secure Shell, your computer must allow connections from any related ports, such as port 22.
- Your computer must be running the Secure Copy (SCP) service or any of the supported protocols to allow copying a file. You can find various SSH or SCP server software on the internet. However, Cisco does not provide support for installing and configuring any particular SCP server.

Step 6 Run the following command to copy the files.

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> <supported file transfer protocol>://<username>@<destination IP address>

Example:

```
firepower-9300(local-mgmt)# copy workspace:/techsupport/
20191105041703_firepower-9300_BC1_all.tar scp:/xyz@192.0.2.1
```

FXOS Enic Devcmd Failure Logs

Devcmd is a mechanism of communication between lina and Cruz firmware. You can see this error logs on the TS files within the LINA **show tech** console logs:

Log synatx: *Enic: Devmcd <**devcmd #**> failed with error code <**error #**>*

```
Message #184 : Enic: Devcmd 107 failed with error code 1
Message #185 : Enic: Devcmd 9 failed with error code 1
Message #233 : Enic: Devcmd 9 failed with error code 2
```

You can use the below tables to identify the devcmd and error strings found in the logs.

devcmd #	devcmd string
1	CMD_MCPU_FW_INFO_OLD
1	CMD_MCPU_FW_INFO
2	CMD_DEV_SPEC
3	CMD_STATS_CLEAR
4	CMD_STATS_DUMP
7	CMD_PACKET_FILTER
7	CMD_PACKET_FILTER_ALL

8	CMD_HANG_NOTIFY
9	CMD_MAC_ADDR/CMD_GET_MAC_ADDR
12	CMD_ADDR_ADD
13	CMD_ADDR_DEL
14	CMD_VLAN_ADD
15	CMD_VLAN_DEL
16	CMD_NIC_CFG
17	CMD_RSS_KEY
18	CMD_RSS_CPU
19	CMD_SOFT_RESET
20	CMD_SOFT_RESET_STATUS
21	CMD_NOTIFY
22	CMD_UNDI
23	CMD_OPEN
24	CMD_OPEN_STATUS
25	CMD_CLOSE
26	CMD_INIT_v1
27	CMD_INIT_PROV_INFO
28	CMD_ENABLE
28	CMD_ENABLE_WAIT
29	CMD_DISABLE
30	CMD_STATS_DUMP_ALL
31	CMD_INIT_STATUS
32	CMD_INT13
33	CMD_LOGICAL_UPLINK
34	CMD_DEINIT
35	CMD_INIT
36	CMD_CAPABILITY
37	CMD_PERBI
38	CMD_IAR
39	CMD_HANG_RESET
40	CMD_HANG_RESET_STATUS
41	CMD_IG_VLAN_REWRITE_MODE

42	CMD_PROXY_BY_BDF
43	CMD_PROXY_BY_INDEX
44	CMD_CONFIG_INFO_GET
45	CMD_INT13_ALL
46	CMD_SET_DEFAULT_VLAN
47	CMD_INIT_PROV_INFO2
48	CMD_ENABLE2
49	CMD_STATUS
50	CMD_INTR_COAL_CONVERT
51	CMD_ISCSI_DUMP_REQ
52	CMD_ISCSI_DUMP_STATUS
53	CMD_MIGRATE_SUBVNIC
54	CMD_SUBVNIC_NOTIFY
55	CMD_SET_MAC_ADDR
56	CMD_PROV_INFO_UPDATE
57	CMD_INITIALIZE_DEVCMD2
58	CMD_ADD_FILTER
59	CMD_DEL_FILTER
61-74	Queue Pair/RDMA/Overlay Offload
106	CMD_SET_FT_CFG
107	CMD_GET_FT_CFG
108	CMD_SET_FT_CTRL
109	CMD_GET_FT_CTRL
110	CMD_CFG_FQ
111	CMD_GET_SHLIF_STATS
112	CMD_CLEAR_SHLIF_STATS
113	CMD_UPDATE_RWMEM_BASE
114	CMD_SET_FT_CFG_CMP

Error Code #	Error String
1	ERR_EINVAL
2	ERR_EFAULT
3	ERR_EPERM
4	ERR_EBUSY

5	ERR_ECMDUNKNOWN
6	ERR_EBADSTATE
7	ERR_ENOMEM
8	ERR_ETIMEDOUT
9	ERR_ELINKDOWN
10	ERR_EMAXRES
11	ERR_ENOTSUPPORTED
12	ERR_EINPROGRESS

Enabling Module Core Dumps

Enabling core dumps on a module can help with troubleshooting in the event of a system crash, or to send to Cisco TAC if requested.

Procedure

Step 1 Connect to the desired module; for example:

Firepower# connect module 1 console

Step 2 (Optional) Enter the following command to view current core dump status:

Firepower-module1> show coredump detail

The command output shows current core dump status information, including whether core dump compression is enabled.

Example:

```
Firepower-module1>show coredump detail
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

Note This command is available only when running ASA Logical device on appliance and not when running Firepower Threat Defense Logical device on appliance.

Step 3 Use the **config coredump** command to enable or disable core dumps, and to enable or disable core dump compression during a crash.

- Use **config coredump enable** to enable creation of a core dump during a crash.
- Use **config coredump disable** to disable core dump creation during a crash.
- Use **config coredump compress enable** to enable compression of core dumps.
- Use **config coredump compress disable** to disable core dump compression.

Example:

```
Firepower-module1>config coredump enable
Coredump enabled successfully.
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure.  Are you sure? (y/n):
y
Firepower-module1>
```

Note Core dump files consume disk space, and if space is running low and compression is not enabled, a core dump file may not be saved even if core dumps are enabled.

Finding the Serial Number of the Firepower 4100/9300 Chassis

You can find details about the Firepower 4100/9300 Chassis and its serial number. Note that serial number of Firepower 4100/9300 Chassis is different than serial numbers of the logical devices.

Procedure

Step 1 Enter the chassis scope:

scope chassis

Example:

```
Firepower# scope chassis
Firepower /chassis #
```

Step 2 View inventory details:

show inventory

Example:

```
Firepower /chassis # show inventory
```

The output shows the serial number and other details.

```
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-C9300-AC    Cisco Systems Inc JMX1950196H 0
```

Rebuild RAID Virtual Drive

RAID (Redundant Array of Independent Disks) is an array, or group, of multiple independent physical drives that provide high performance and fault tolerance. A drive group is a group of physical drives. These drives are managed in partitions known as virtual drives.

RAID drive groups improve data storage reliability and fault tolerance compared to single-drive storage systems. Data loss resulting from a drive failure can be prevented by reconstructing missing data from the remaining drives. RAID improves I/O performance and increases storage subsystem reliability.

If one of your RAID drives has failed or is offline, then the RAID virtual drive is considered to be in a degraded state. Use this procedure to verify whether a RAID virtual drive is in a degraded state, and temporaritly set the local disk configuration protection policy to no to rebuild it if necessary.

Note When you set the local disk configuration protection policy to no, all data on the disk is destroyed.

Procedure

Step 1 Check the RAID drive status.

a. Enter chassis mode:

scope chassis

b. Enter server mode:

scope server 1

c. Enter the raid controller:

scope raid-controller 1 sas

d. View the virtual drive:

show virtual-drive

If the RAID virtual drive is degraded, the operability displays as **Degraded**. For example:

```
Virtual Drive:
    ID: 0
    Block Size: 512
    Blocks: 3123046400
    Size (MB): 1524925
    Operability: Degraded
Presence: Equipped
```

Step 2 Set the local disk configuration policy protection to no to rebuild the RAID drive. Note - all data on the disk will be destroyed after you complete this step.

a. Enter the organization scope:

scope org

b. Enter the local disk configuration policy scope:

scope local-disk-config-policy ssp-default

c. Set protect to no:

set protect no

d. Commit the configuration:

commit-buffer

Step 3 Wait for the RAID drive to rebuild. Check the RAID rebuild status:

scope chassis 1

show server

When the RAID drive has rebuilt successfully, the slot's overall status displays as **Ok**. For example:

Example:

```
Server:
    Slot    Overall Status        Service Profile
    ------- --------------------- ---------------
          1 Ok                    ssp-sprof-1
```

Step 4 Once the RAID drive has rebuilt successfully, set the local disk configuration policy protection back to yes.

a. Enter the organization scope:

scope org

b. Enter the local disk configuration policy scope:

scope local-disk-config-policy ssp-default

c. Set protect to no:

set protect yes

d. Commit the configuration:

commit-buffer

Identify Issues with the SSD

Use the following procedure to collect information and identify possible issues with the SSD installed on your device. One example symptom of an SSD issue is the Data Management Engine (DME) process failing to start.

Note When you insert a new SSD, only the basic information (Type, Model, SN, etc.) gets populated under inventory after the Blade BIOS detection. Only upon the SSP-OS upgrade completion, the Local Disk data gets populated under inventory. If the SSP-OS upgrade is still under "Updating state", the inventory shows no entry for the Local Disk and no fault messages regarding conection of the SSD.

If the output of the below logging files indicate a problem with the SSD, contact TAC (see https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html).

Procedure

Step 1 Connect to the FXOS command shell:

connect fxos

Step 2 Display the nvram logging file:

show logging nvram

Example error output:

```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
block - inode=14, block=6
```

Step 3 Display the logging file:

show logging logfile

Example error output:

```
   2020 Oct 21 21:11:25  (none) kernel: [28118744.718445] EXT3-fs error (device sda4):
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```