Troubleshoot Firmware

- Recovering Fabric Interconnect During Upgrade, on page 1
- Recovering IO Modules During Firmware Upgrade, on page 8

Recovering Fabric Interconnect During Upgrade

If one or both fabric interconnects fail during failover or firmware upgrade, you can recover them by using one of the following approaches:

- Recover a fabric interconnect when you do not have a working image on the fabric interconnect
- Recover a fabric interconnect when you have a working image on the fabric interconnect
- Recover an unresponsive fabric interconnect during upgrade or failover
- Recover fabric interconnects from a failed FSM during upgrade with Auto Install

Recovering Fabric Interconnects When You Do Not Have Working Images on the Fabric Interconnect or the Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt, and you do not have working images on the fabric interconnect.

Procedure

Step 1 Reboot the switch, and in the console, press **Ctrl+L** as it boots to get the loader prompt.

Note
You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Example:

```
loader>
```

Step 2 Required: Configure the interface to receive the kickstart image through TFTP.

a) Enter the local IP address and subnet mask for the system at the loader> prompt, and press **Enter**.

Example:

```
loader> set ip 10.104.105.136 255.255.255.0
```

b) Specify the IP address of the default gateway.

Example:

```
loader> set gw 10.104.105.1
```

c) Boot the kickstart image file from the required server.

Example:

```
loader> boot
tftp://10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Note
You do not need to do this step if you already have a kickstart image in the bootflash.

Step 3 Enter the **init system** command at the switch(boot)# prompt.

This will reformat the fabric interconnect.

Example:

```
switch(boot)# init system
```

Step 4 Configure the management interface.

a) Change to configuration mode and configure the IP address of the mgmt0 interface.

Example:

```
switch(boot)# config t
switch(boot)(config)# interface mgmt0
```

b) Enter the **ip address** command to configure the local IP address and the subnet mask for the system.

Example:

```
switch(boot)(config-if)# ip address 10.104.105.136 255.255.255.0
```

c) Enter the **no shutdown** command to enable the mgmt0 interface on the system.

Example:

```
switch(boot)(config-if)# no shutdown
```

d) Enter the **ip default-gateway** command to configure the IP address of the default gateway.

Example:

```
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.104.105.1
```

e) Enter **exit** to exit to EXEC mode.

Example:

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

Step 5 Copy the kickstart, system, and Cisco UCS Manager management images from the TFTP server to the bootflash.

Example:

```
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-manager-k9.3.0.2d56.bin bootflash://
```

Step 6 Create separate directories for installables and installables/switch in the bootflash.

Example:

```
switch(boot)# mkdir bootflash:installables
switch(boot)# mkdir bootflash:installables/switch
```

Step 7 Copy the kickstart, system, and Cisco UCS Manager images to the installables/switch directory.

Example:

```
switch(boot)# copy ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-6300-k9-system.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-manager-k9.3.02d56.bin bootflash:installables/switch/
```

Step 8 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy bootflash:installables/switch/ucs-manager-k9.3.02d56.bin
nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 9 Reload the switch.

Example:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

Step 10 Boot from the kickstart image.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

Step 11 Load the system image.

The **Basic System Configuration Dialog** wizard appears after the system image is completely loaded. Use this wizard to configure the fabric interconnect.

Example:

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Uncompressing system image: bootflash:/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin

...

---- 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.

...

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

Step 12 Log in to Cisco UCS Manager and download the firmware.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<infra bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<b-series bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<c-series bundle name>
Password:
UCS-A /firmware # show download-task
Download task:
    File Name Protocol Server          Userid          State
    --------- -------- --------------- --------------- -----
    ucs-k9-bundle-b-series.3.0.2.B.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-c-series.3.0.2.C.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-infra.3.0.2.A.bin
              Scp      10.104.105.22   abcdefgh        Downloading
UCS-A /firmware #
```

Step 13 After the firmware download is complete, activate the fabric interconnect firmware and Cisco UCS Manager firmware.

This step updates Cisco UCS Manager and the fabric interconnects to the version you want, and then reboots them.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect* # activate firmware kernel-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
```

```
UCS-A /fabric-interconnect* # activate firmware system-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect # exit

UCS-A# scope system
UCS-A /system # show image

Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.3.02d56.bin                  System              3.0(2d)
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system #
```

Recovering Fabric Interconnect During Upgrade When You have Working Images on the Bootflash

You can perform these steps when both or any fabric interconnect goes down during firmware upgrade, gets rebooted, and is stuck at the loader prompt.

Before you begin

You must have working images on the bootflash to perform these steps.

Procedure

Step 1 Reboot the switch, and in the console, press Ctrl+L as it boots to get the loader prompt.

Note
You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Example:

```
loader>
```

Step 2 Run the **dir** command.

The list of available kernel, system, and Cisco UCS Manager images in the bootflash appears.

Example:

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6400-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6400-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
```

Step 3 Boot the kernel firmware version from the bootflash.

Note
Any kernel image available here will be a working image from which you can boot.

Example:

```
loader> boot ucs-6400-k9-kickstart.5.0.2.N1.3.02d56.bin
```

Step 4 Ensure that the management image is linked to nuova-sim-mgmt-nsg.0.1.0.001.bin.

nuova-sim-mgmt-nsg.0.1.0.001.bin is the name that the reserved system image uses, and it makes the management image Cisco UCS Manager-compliant.

Example:

```
switch(boot)# copy ucs-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.0.001.bin
```

Step 5 Load the system image.

Example:

```
switch(boot)# load ucs-6400-k9-system.5.0.2.N1.3.02d56.bin
```

Step 6 Log in to Cisco UCS Manager and update your fabric interconnect and Cisco UCS Manager software to the version that you want.

Recovering Unresponsive Fabric Interconnects During Upgrade or Failover

During upgrade or failover, avoid performing the following tasks because they introduce additional risk:

- Pmon stop/start
- FI reboots – power cycle or CLI
- HA failover

Procedure

Step 1 If the **httpd_cimc.sh** process is lost, as documented in CSCup70756, you lose access to the KVM. Continue with the failover or contact Cisco Technical Assistance.

Step 2 If you lose access to the KVM on the primary side, continue with the failover to resolve the issue.

Step 3 If KVM is needed or is down on the subordinate side, start only that service using the debug plugin. Contact TAC to run the debug image.

Step 4 If the /dev/null issue is encountered, as documented in CSCuo50049, fix the rights to 666 with the debug-plugin at both steps if required. Contact Cisco Technical Assistance to run debug commands.

Step 5 If both CSCup70756 and CSCuo50049 are encountered, it can cause VIP loss. If the VIP is lost, do the following:

a. Access the primary physical address through the GUI and use the GUI to verify all IO Module backplane ports recovered.

b. If the GUI is down, verify IO Module backplane ports with the NXOS **show fex detail** command.

c. Perform the workaround and verify that the cluster state is UP on both fabric interconnects.

d. If the cluster state is UP on both fabric interconnects, continue the upgrade by reacknowledging the primary fabric interconnect reboot using the SSH CLI syntax:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

Recovering Fabric Interconnects From a Failed FSM During Upgrade With Auto Install

You can perform these steps when all the following occur:

- You are upgrading or downgrading firmware using Auto Install between Cisco UCS Manager Release 3.1(2) and Release 3.1(3) while a service pack is installed on the fabric interconnects.
- Both or any fabric interconnect goes down because of an FSM failure or multiple retries in the DeployPollActivate stage of the FSM

Procedure

Step 1 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) Remove the service pack from the subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Step 2 Upgrade the infrastructure firmware using the force option through Auto Install.

Example:

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 3.1(3a)A force
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes
Triggering Install-Infra with:
Infrastructure Pack Version: 3.1(3a)A
```

Step 3 Acknowledge the reboot of the primary fabric interconnect.

Example:

```
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

Step 4 When the FSM fails, or when multiple retries are observed in the DeployPollActivate stage of the FSM on the current subordinate fabric interconnect, do the following:

a) Clear the startup version of the default infrastructure pack and the service pack.

Example:

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) Remove the service pack from the current subordinate fabric interconnect.

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

Both fabric interconnects will now reflect Release 3.1(3) firmware and the default service pack for Running and Startup versions.

Recovering IO Modules During Firmware Upgrade

You can recover an IO Module during firmware upgrade by resetting it from a peer IO Module. After it is reset, it can derive the configuration from the fabric interconnect.

Resetting an I/O Module from a Peer I/O Module

Sometimes, I/O module upgrades can result in failures or I/O modules can become unreachable from Cisco UCS Manager due to memory leaks. You can reboot an I/O module that is unreachable through its peer I/O module.

Resetting the I/O module restores the I/O module to factory default settings, deletes all cache files and temporary files, but retains the size-limited OBFL file.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Choose the peer I/O module of the I/O module that you want to reset.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the Actions area, click **Reset Peer IO Module**.