Completing the Prerequisites for Upgrading the Firmware

This chapter includes the following sections:

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS domain must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Before you upgrade or downgrade firmware in a Cisco UCS domain, complete the following prerequisites:

- Review the Release Notes.
- Review the relevant Hardware and Software Interoperability Matrix to ensure the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade.
- Back up the configuration into an All Configuration backup file.

- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that the data path is up and running. For more information, see the Verifying that the Data Path is Ready section in the appropriate Firmware Management Guide.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that the Cisco UCS domain does not include any critical or major faults. If such faults exist, you must resolve them before you upgrade the system. A critical or major fault may cause the upgrade to fail.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.
- If you want to integrate a rack-mount server into the Cisco UCS domain, follow the instructions in the appropriate C-Series Rack-Mount Server Integration Guide for installing and integrating a rack-mount server in a system managed by Cisco UCS Manager.

Creating an All Configuration Backup File

This procedure assumes that you do not have an existing backup operation for an All Configuration backup file.

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**	Creates an enabled All Configuration backup operation that runs as soon as you enter the **commit-buffer** command. The **all-configuration** option backs up the server, fabric, and system related configuration. Specify the URL for the backup file using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path*
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

The following example uses SCP to create an All Configuration backup file on the host named host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
enabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Faults Generated Due to Reboot During the Upgrade of a Fabric Interconnect

During firmware upgrade, to ensure proper functioning of all services on the fabric interconnect, it is essential to ensure that port configurations and services that go down when the fabric interconnect reboots are re-established after the fabric interconnect comes back up.

Cisco UCS Manager displays any service that is not re-established after the last reboot of a fabric interconnect. Cisco UCS Manager creates a baseline of the outstanding faults before a fabric interconnect is to be rebooted. After the fabric interconnect reboots and comes up, you can view the new faults generated since the last baseline to identify the services that went down because of the fabric reboot.

When a specific interval of time has passed after Cisco UCS Manager created a baseline of the outstanding faults, baselining is cleared and all faults show up as new faults. This interval is called baseline expiration interval. Modifying Baseline Expiration Interval for Faults, on page 3 provides detailed information about modifying a baseline expiration interval in Cisco UCS Manager.

Cisco recommends that you resolve service-impacting faults before you continue with the fabric interconnect reboot or evacuation.

Modifying Baseline Expiration Interval for Faults

You can modify a baseline expiration interval in Cisco UCS Manager.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **scope fault policy**	Enters monitoring fault policy mode.
Step 3	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.
Step 4	UCS-A /monitoring/fault-policy # **set baseline-expiration-interval** {*days hours minutes seconds*}	Modifies the baseline expiration interval. The default baseline expiration interval is 24 hours. **Note** After the baseline-expiration-interval expires, all faults are shown as new faults.

	Command or Action	Purpose
Step 5	UCS-A /monitoring/fault-policy* # **commit**	Commits the transaction.
Step 6	UCS-A /monitoring/fault-policy # **show**	Displays the details of the fault policy.

This example shows how to modify the baseline expiration interval for faults:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- -------------------------------- -----------------------
------------------------------------------
    Retain       00:00:20:00    00:01:00:00                      10
10:00:00:12

UCS-A /monitoring/fault-policy # set baseline-expiration-interval 0 2 24 0
UCS-A /monitoring/fault-policy* # commit
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- -------------------------------- -----------------------
------------------------------------------
    Retain       10:00:00:00    01:01:01:01                      10
00:02:24:00
UCS-A /monitoring/fault-policy #
```

Viewing Faults Generated During the Upgrade of a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope monitoring**	Enters monitoring mode.
Step 2	UCS-A /monitoring # **show new-faults**	Shows the faults generated after baselining and because of the reboot of the fabric interconnect during upgrade.
Step 3	UCS-A /monitoring # **show baseline-faults**	Shows the faults baselined before the reboot of the fabric interconnect during upgrade.

This example shows how to view faults generated at various stages of the upgrade process:

Faults before reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
```

```
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Faults after reboot of the primary fabric interconnect:

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

To view faults generated because of reboot of the primary fabric interconnect:

```
UCS-A /monitoring # show new-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server 1
/ 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state is
down
```

To view faults before reboot of the primary fabric interconnect:

```
UCS-A# show baseline-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ------------------------ -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1 link
state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state is
down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2 link
state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state is
down
```

Verifying the Operability of a Fabric Interconnect

If your Cisco UCS domain is running in a high availability cluster configuration, you must verify the operability of both fabric interconnects.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect #**show**	Displays information about the fabric interconnect. Verify that the operability of the fabric interconnects is in the Operable state. If the operability is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Manager B-Series Troubleshooting Guide*.

The following example displays that the operability for both fabric interconnects is in the Operable state:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show cluster state**	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster. Verify that both fabric interconnects (A and B) are in the Up state and HA is in the Ready state. If the fabric interconnects are not in the Up state or HA is not

	Command or Action	Purpose
		in the Ready state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*. Also note which fabric interconnect has the primary role and which has the subordinate role; you will need to know this information to upgrade the firmware on the fabric interconnects.

The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Verifying the Status of an I/O Module

If your Cisco UCS is running in a high availability cluster configuration, you must verify the status for both I/O modules in all chassis.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-id*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope iom** *iom-id*	Enters chassis I/O module mode for the selected I/O module.
Step 3	UCS-A # **show**	Shows the status of the specified I/O module on the specified chassis. Verify that the overall status of the I/O module is in the Operable state. If the overall status is not in the Operable state, run a **show tech-support** command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the **show tech-support** command, see the *Cisco UCS Troubleshooting Guide*.

The following example displays that the overall status for both I/O modules on chassis 1 is in the Operable state:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
```

```
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             2 Right B         Operable
```

Verifying the Status of a Server

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server in the specified chassis.
Step 2	UCS-A /chassis/server # **show status detail**	Shows the status detail of the server. Verify that the overall status of the server is Ok, Unavailable, or any value that does not indicate a failure. If the overall status is in a state that indicates a failure, such as Discovery Failed, the endpoints on that server cannot be upgraded.

The following example displays that the overall status for server 7 on chassis 1 is in the Ok state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

Verifying the Status of Adapters on Servers in a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id / server-id*	Enters chassis server mode for the specified server in the specified chassis
Step 2	UCS-A /chassis/server # **show adapter status**	Displays the status of the adapter. Verify that the overall status of the adapter is in the Operable state. If the overall status of the adapter is in any state other than Operable, you cannot upgrade it. However, you can proceed with the upgrade for the other adapters in the Cisco UCS domain.

The following example displays that the overall status for the adapter in server 7 on chassis 1 is in the Operable state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
Server 1/1:
    Overall Status
    --------------
    Operable
```

Obtaining Cisco UCS PowerTool and Running the Duplicate IQN Script

If a Cisco UCS domain is configured for iSCSI boot, before you upgrade from Cisco UCS, Release 2.0(1) to Cisco UCS, Release 2.0(2) or higher, you must ensure that all iSCSI vNICs used across multiple service profile have unique initiator names.

You can use a script that runs in the Cisco UCS PowerTool to determine whether a Cisco UCS configuration for iSCSI boot includes duplicate IQNs.

Procedure

Step 1 To download Cisco UCS PowerTool, do the following:

a) In your web browser, navigate to the following website: http://developer.cisco.com/web/unifiedcomputing/microsoft
b) Scroll down to the **Cisco UCS PowerTool (PowerShell Toolkit) Beta Download** area.
c) Download the `CiscoUcs-PowerTool-0.9.6.0.zip` file.
d) Unzip the file and follow the prompts to install Cisco UCS PowerTool.
You can install Cisco UCS PowerTool on any Windows computer. You do not need to install it on a computer used to access Cisco UCS Manager.

Step 2 To launch Cisco UCS PowerTool, enter the following at a command line:
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUc sPS.ps1

Example:

The following example shows what happens when you launch Cisco UCS PowerTool:

```
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowe
rshell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUc
sPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

Step 3 In Cisco UCS PowerTool, do the following:

a) Connect to Cisco UCS Manager, as follows:
PS C:\> **Connect-Ucs** *IP_address*

b) Enter your username and password when prompted for your credential as shown in the following example:

```
cmdlet Connect-Ucs at command pipeline position 1
Supply values for the following parameters:
Credential
```

Cisco UCS PowerTool outputs the following to your screen after you log in.

```
Cookie                : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains               :
LastUpdateTime        : 3/9/2012 6:20:42 AM
Name                  : 209.165.201.15
NoSsl                 : False
NumPendingConfigs     : 0
NumWatchers           : 0
Port                  : 443
Priv                  : {admin, read-only}
RefreshPeriod         : 600
SessionId             : web_49846_A
TransactionInProgress : False
Ucs                   : ucs-4
Uri                   : https://209.165.201.15
UserName              : admin
VirtualIpv4Address    : 209.165.201.15
Version               : 2.0(2i)3.0(1a)
WatchThreadStatus     : None
```

Step 4 In the Cisco UCS PowerTool, run the following script to validate your iSCSI boot configuration and check for duplicate IQNs :
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj }**

Cisco UCS PowerTool outputs the results to your screen, as follows:

```
Count InitiatorName              Dn
----- -------------              --
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
```

```
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...
```

Step 5 (Optional) If you have .NET Frame work 3.5 Service Pack 1 installed, you can use the following script to view the output in the GUI:
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj } | ogv**

Step 6 Disconnect from Cisco UCS Manager, as follows:
PS C:\>**Disconnect-Ucs**

What to Do Next

If duplicate IQNs exist across multiple service profiles in the Cisco UCS domain, reconfigure the iSCSI vNICs with unique IQNs in Cisco UCS Manager before you upgrade to Cisco UCS, Release 2.1 or greater.

If you do not ensure that all iSCSI vNICs are unique across all service profiles in a Cisco UCS domain before you upgrade, Cisco UCS Manager raises a fault on the iSCSI vNICs to warn you that duplicate IQNs are present. Also, if you do not ensure that there are no duplicate IQN names within a service profile (for example, the same name used for both iSCSI vNICs), Cisco UCS reconfigures the service profile to have a single IQN. For information on how to clear this fault and reconfigure the duplicate IQNs, see the Cisco UCS B-Series Troubleshooting Guide.