Troubleshooting Issues with Cisco UCS B-Series Operation

This chapter includes the following sections:

Troubleshooting Cisco UCS Manager Initial Configuration

Verify Console Setup

You can verify that both fabric interconnect configurations are complete by logging into the fabric interconnect via SSH and verifying the cluster status through CLI. For this procedure, you can watch Cisco UCS Manager Initial Setup part 3.

Use the following commands to verify the cluster state:

Command	Purpose	Sample Output

show cluster state	Displays the operational state and leadership role for both fabric interconnects in a high availability cluster.	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`

show cluster extended-state	Displays extended details about the cluster state and typically used when troubleshooting issues.	The following example shows how to view the extended state of a cluster:
		`UCSC# show cluster`
		`extended-state`
		`0x2e95deacbd0f11e2-0x8ff35147e84f3de2Start`
		` time: Thu May 16 06:54:22`
		`2013Last election time: Thu`
		`May 16 16:29:28 2015System`
		`Management`
		`Viewing the Cluster State`
		`A: UP, PRIMARY`
		`B: UP, SUBORDINATE`
		
		`A: memb state UP, lead state`
		`PRIMARY, mgmt services state:`
		` UP`
		`B: memb state UP, lead state`
		`SUBORDINATE,`
		`mgmt services state: UP`
		`heartbeat state PRIMARY_OK`
		`HA READY`
		`Detailed state of the device`
		`selected for HA quorum data:`
		`Device 1007, serial:`
		`a66b4c20-8692-11df-bd63-1b72ef3ac801,`
		` state: active`
		`Device 1010, serial:`
		`00e3e6d0-8693-11df-9e10-0f4428357744,`
		` state: active`
		`Device 1012, serial:`
		`1d8922c8-8693-11df-9133-89fa154e3fa1,`
		` state: active`

Troubleshooting Boot Issues

Reboot Warning Does Not Display

Problem—The system fails to produce a reboot warning that lists any dependencies.

Possible Cause—This problem can be caused by changes to a vNIC template or a vHBA template. Reboot warnings occur when the back-end returns a list of dependencies. When you update the template type for a vNIC or vHBA template and make changes to any boot-related properties without applying changes between steps, the back-end systems are not triggered to return a list of dependencies.

Procedure

Step 1 Launch the Cisco UCS Manager GUI.

Step 2 In the vNIC template or vHBA template included in the service profile, do the following:

a) Change the template type from **Initial Template** to **Updating Template**.
b) Click **Save Changes**.

Step 3 Make any additional changes to the reboot-related values and click **Save Changes**.

A reboot warning and the list of dependencies are displayed.

Server Does Not Boot from OS Installed on eUSB

Problem—The eUSB embedded inside the Cisco UCS server includes an operating system. However, the server does not boot from that operating system.

Possible Cause—This problem can occur when, after associating the server with the service profile, the eUSB is not at the top of the actual boot order for the server.

Procedure

Step 1 Launch the Cisco UCS Manager GUI.

Step 2 On **Servers**, do the following to verify the boot policy configuration:

a) Navigate to the service profile associated with the server.
b) In the **Work** pane, click the **Boot Order** tab
c) Ensure that **Local Disk** is configured as the first device in the boot policy.

Step 3 On **Equipment**, do the following to verify the actual boot order for the server:

a) Navigate to the server.
b) On the **General** tab, expand the **Boot Order Details** area and verify that the eUSB is listed as the first device on the **Actual Boot Order** tab.

   For example, the first device should be **VM eUSB DISK**.

Step 4 If the eUSB is not the first device in the actual boot order, do the following:

a) On the **General** tab for the server, click the following links in the **Actions** area:

- Click **KVM Console** to launch the KVM console.
- Click **Boot Server** to boot the server.

b) In the KVM console, while the server is booting, press `F2` to enter the BIOS setup.

c) In the BIOS utility, click on the **Boot Options** tab.

d) Click **Hard Disk Order**.

e) Configure **Boot Option #1** to the eUSB.

For example, set this option to `VM eUSB DISK`.

f) Press `F10` to save and exit.

Server Does Not Boot After RAID1 Cluster Migration

Problem—The server does not boot from the operating system after a RAID1 cluster migration. The RAID LUN remains in “inactive” state during and after service profile association. As a result, the server cannot boot.

Possible Cause—This problem can occur if the local disk configuration policy in the service profile on the server is configured with **Any Configuration** mode rather than RAID1.

Procedure

Step 1 In Cisco UCS Manager GUI, click **Servers**.

Step 2 Navigate to the service profile associated with the server and click the **Storage** tab.

Step 3 Do one of the following:

- Change the local disk configuration policy included in the service profile to the same policy included in the service profile associated with the server prior to the migration, as follows:
  - In the **Actions** area, click **Change Local Disk Configuration Policy**.
  - From the **Select the Local Disk Configuration Policy** drop-down list, choose the appropriate policy.
  - Click **OK**.
- Change the mode property in the local disk configuration policy included in the service profile, as follows:
  - In the **Local Disk Configuration Policy** area of the **Storage** tab, click the link in the **Local Disk Policy Instance** field.
  - In the **Mode** field, ensure that the **Raid 1 Mirrored** option is chosen.
  - Click **Save Changes**.

Troubleshooting KVM Issues

BadFieldException When Launching the KVM Viewer

Problem—The BadFieldException error appears when the KVM viewer is launched.

Possible Cause—This problem can occur because the Java Web Start disables the cache by default when it is used with an application that uses native libraries.

Procedure

Step 1 Choose **Start** > **Control Panel** > **Java**.

Step 2 Click on the **General** tab.

Step 3 In the **Temporary Internet Files** area, click **Settings**.

Step 4 Click the **Keep temporary files on my computer** check box.

Step 5 Click **OK**.

KVM Console Failure

Problem—The KVM console fails to launch and the JRE displays the following message:

```
Unable to launch the application.
```

Possible Cause—This problem can be caused if several KVM consoles are launched simultaneously.

Procedure

Step 1 If possible, close all of the open KVM consoles.

Step 2 Relaunch the KVM consoles one at a time.

KVM Fails to Open

Problem—The first time you attempt to open the KVM on a server, the KVM fails to launch.

Possible Cause—This problem can be caused by a JRE version incompatibility.

Procedure

Step 1 Upgrade to JRE 1.6_11.

Step 2 Reboot the server.

Step 3 Launch the KVM console.

Troubleshooting VM issues

No Ports Available for Distributed Virtual Switch

Problem—The following error displays:

```
Currently connected network interface x uses Distributed Virtual Switch (uusid:y) which is

accessed on the host via a switch that has no free ports.
```

Possible Cause—This problem can be caused by one of the following issues:

- After powering off or migrating a VM from one host to another, the vSphere server fails to recompute the numPortsAvailable property in the hostProxySwitch object.
- The cumulative number of vNICs for the VMs powered on an ESX host matches or exceeds the number of dynamic nVINCs configured in the server's service profile.
- After migrating a VM from one data-store to another data-store on the same server, the server incorrectly detects an increase in the number of DVS ports being used by all of the VMs powered on the host.

Procedure

Step 1 Identify what you were doing when the error displayed.

Step 2 If the error resulted from powering off a VM, or from migrating a VM from one host to another, do the following:

a) Migrate a second VM from the ESX host to another system.

b) When a second port is made available, do one of the following:

- Power on a VM.
- Migrate a VM back to the ESX host.

Step 3 If the error resulted from migrating a VM instance from one data-store to another data-store on the same server, do the following:

a) Shut down all of the VMs on the ESX host.

b) Retry the migration.

Troubleshooting Cisco UCS Manager Issues

DME Process Timed Out

Problem—When you run Cisco UCS Manager CLI commands, Cisco UCS Manager CLI displays the following message:

```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

Possible Cause—This problem occurs when the DME process on the primary fabric interconnect is either unresponsive or has crashed, and is not in the running state. Other symptoms that appear when the DME is down are:

- Cisco UCS Manager GUI becomes unresponsive
- Connectivity to Virtual IP goes down

Procedure

Step 1 Gather information on the sequence of events, such as upgrade of Cisco UCS Manager and configuration changes, that lead the system to this state.

Step 2 Connect to each fabric interconnect by using its individual IP address, and verify the cluster status, process and core dumps by using the following commands:

a) UCS-A# **connect local-mgmt**

Enters local management mode for the cluster.

b) UCS-A (local-mgmt) # **show cluster extended-state**

Displays the state of fabric interconnects in the cluster and whether the cluster is HA ready.

c) UCS-A(local-mgmt)# **show pmon state**

Displays the state of all processes within Cisco UCS Manager.

d) UCS-A(local-mgmt)# **ls workspace:/cores**

Displays a list of all core dumps in workspace.

Step 3 Identify the primary fabric interconnect, and whether HA election is incomplete.

Step 4 Review NXOS logs for fabric interconnect hardware issues by using the following commands:

a) UCS-A# **connect nxos {a | b}**

Enters NX-OS mode for the fabric interconnect.

b) UCS-A(nxos)# **show logg**

Displays details about log files.

Step 5 Collect technical support information for Cisco UCS Manager from local-mgmt CLI by using the following commands:

a) UCS-A# **connect local-mgmt**

Enters local management mode for the cluster.

b) UCS-A(local-mgmt)# **show tech-support ucsm detail**

Displays technical support information for Cisco UCS Manager.

What to do next

Contact TAC with these logs and information to further investigate the failure.

Event Sequencing Fatal Error

Problem—After coming back from sleep mode, the Cisco UCS Manager GUI displays the following message:

```
Fatal error: event sequencing is skewed.
```

Possible Cause—This problem can be caused if the Cisco UCS Manager GUI was running when the computer went to sleep. Since the JRE does not have a sleep detection mechanism, the system is unable to retrack all of the messages received before it went into sleep mode. After multiple retries, this event sequencing error is logged.

Note Always shut down Cisco UCS Manager GUI before putting your computer to sleep.

Procedure

In Cisco UCS Manager GUI, if a **Connection Error** dialog box is displayed, click one of the following:

- Click **Re-login** to log back in to the Cisco UCS Manager GUI.
- Click **Exit** to exit the Cisco UCS Manager GUI.

Troubleshooting Fabric Interconnect Issues

Recovering a Fabric Interconnect from the Boot Loader Prompt

If the fabric interconnect fails to start, you may have one of the following issues:

- The kickstart image is corrupted or non-functional for other reasons
- The file system on the bootflash memory is corrupted

If either of these issues exist, you might need to use the boot loader prompt to recover the fabric interconnect.

Procedure

Contact Cisco Technical Assistance Center to obtain the firmware recovery images and information about how to recover the fabric interconnect from the boot loader prompt.

Resolving Fabric Interconnect Cluster ID Mismatch

Problem—When you set up two fabric interconnects to support a high availability cluster and connect the L1 ports and L2 ports, a fabric interconnect cluster ID mismatch can occur. This type of mismatch means that the cluster fails and Cisco UCS Manager cannot be initialized.

Procedure

Step 1 In Cisco UCS Manager CLI, connect to fabric interconnect B and execute **erase configuration**.

All configuration on the fabric interconnect is erased.

Step 2 Reboot fabric interconnect B.

After rebooting, fabric interconnect B detects the presence of fabric interconnect A and downloads the cluster ID from fabric interconnect A. You need to configure the subordinate fabric interconnect for the cluster configuration.

Step 3 When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

Note The fabric interconnect should detect the peer fabric interconnect in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that the peer fabric interconnect has been enabled for a cluster configuration.

Step 4 Enter **y** to add the subordinate fabric interconnect to the cluster.

Step 5 Enter the admin password of the peer fabric interconnect.

Step 6 Enter the IP address for the management port on the subordinate fabric interconnect.

Step 7 Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

Troubleshooting Server Disk Drive Detection and Monitoring

Support for Local Storage Monitoring

The type of monitoring supported depends upon the Cisco UCS server.

Supported Cisco UCS Servers for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the following servers:

- Cisco UCS B200 M3 blade server
- Cisco UCS B420 M3 blade server
- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server
- Cisco UCS C460 M2 rack server
- Cisco UCS C420 M3 rack server
- Cisco UCS C260 M2 rack server
- Cisco UCS C240 M3 rack server
- Cisco UCS C220 M3 rack server
- Cisco UCS C24 M3 rack server
- Cisco UCS C22 M3 rack server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4 rack server
- Cisco UCS C460 M4 rack server

Note Not all servers support all local storage components. For Cisco UCS rack servers, the onboard SATA RAID 0/1 controller integrated on motherboard is not supported.

Supported Cisco UCS Servers for Legacy Disk Drive Monitoring

Only legacy disk drive monitoring is supported through Cisco UCS Manager for the following servers:

- Cisco UCS B200 M1/M2 blade server
- Cisco UCS B250 M1/M2 blade server

Note In order for Cisco UCS Manager to monitor the disk drives, the 1064E storage controller must have a firmware level contained in a UCS bundle with a package version of 2.0(1) or higher.

Prerequisites for Local Storage Monitoring

These prerequisites must be met for local storage monitoring or legacy disk drive monitoring to provide useful status information:

- The drive must be inserted in the server drive bay.
- The server must be powered on.
- The server must have completed discovery.
- The results of the BIOS POST complete must be TRUE.

Viewing the Status of a Disk Drive

Viewing the Status of Local Storage Components in the Cisco UCS Manager GUI

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to view the status of your local storage components.

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

Step 5 Click the **Storage** subtab to view the status of your RAID controllers and any FlexFlash controllers.

Step 6 Click the down arrows to expand the **Local Disk Configuration Policy**, **Actual Disk Configurations**, **Disks**, and **Firmware** bars and view additional status information.

Interpreting the Status of a Monitored Disk Drive

Cisco UCS Manager displays the following properties for each monitored disk drive:

- Operability—The operational state of the drive.
- Presence—The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state.

You need to look at both properties to determine the status of the monitored disk drive. The following table shows the likely interpretations of the combined property values.

Operability Status	Presence Status	Interpretation
Operable	Equipped	No fault condition. The disk drive is in the server and can be used.

Operability Status	Presence Status	Interpretation
Inoperable	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The disk drive is unusable due to a hardware issue such as bad blocks. • There is a problem with the IPMI link to the storage controller.
N/A	Missing	Fault condition. The server drive bay does not contain a disk drive.
N/A	Equipped	Fault condition. The disk drive is in the server, but one of the following could be causing an operability problem: • The server is powered off. • The storage controller firmware is the wrong version and does not support disk drive monitoring. • The server does not support disk drive monitoring.

Note The **Operability** field might show the incorrect status for several reasons, such as if the disk is part of a broken RAID set or if the BIOS power-on self-test (POST) has not completed.

HDD Metrics Not Updated in Cisco UCS Manager GUI

Problem—After hot-swapping, removing, or adding a hard drive, the updated hard disk drive (HDD) metrics do not appear in the Cisco UCS Manager GUI.

Possible Cause—This problem can be caused because Cisco UCS Manager gathers HDD metrics only during a system boot. If a hard drive is added or removed after a system boot, the Cisco UCS Manager GUI does not update the HDD metrics.

Procedure

Reboot the server.

Disk Drive Fault Detection Tests Fail

Problem—The fault LED is illuminated or blinking on the server disk drive, but Cisco UCS Manager does not indicate a disk drive failure.

Possible Cause—The disk drive fault detection tests failed due to one or more of the following conditions:

- The disk drive did not fail, and a rebuild is in progress.
- Drive predictive failure
- Selected drive failure on Disk 2 of a B200, B230 or B250 blade
- Selected drive failure on Disk 1 of a B200, B230 or B250 blade

Procedure

Step 1 Monitor the fault LEDs of each disk drive in the affected server(s).

Step 2 If a fault LED on a server turns any color, such as amber, or blinks for no apparent reason, create technical support file for each affected server and contact Cisco Technical Assistance Center.

Cisco UCS Manager Reports More Disks in Server than Total Slots Available

Problem—Cisco UCS Manager reports that a server has more disks than the total disk slots available in the server. For example, Cisco UCS Manager reports three disks for a server with two disk slots as follows:

```
RAID Controller 1:
           Local Disk 1:
               Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted
               PID: A03-D073GC2
               Serial: D3B0P99001R9
               Presence: Equipped
           Local Disk 2:
               Product Name:
               Presence: Equipped
               Size (MB): Unknown
           Local Disk 5:
               Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted
               Serial: D3B0P99001R9
               HW Rev: 0
               Size (MB): 70136
```

Possible Cause—This problem is typically caused by a communication failure between Cisco UCS Manager and the server that reports the inaccurate information.

Procedure

Step 1 Upgrade the Cisco UCS domain to the latest release of Cisco UCS software and firmware.

Step 2 Decommission the server.

Step 3 Recommission the server.

Troubleshooting Post-Upgrade IQN Issues

Clearing the Duplicate IQN Fault and Reconfiguring IQN Initiator Names

Problem—After an upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2), Cisco UCS Manager raises an IQN-related fault on one or more service profiles when you attempt to perform an action on a service profile, such as modifying the host firmware package.

Possible Cause—One or more iSCSI vNICS used within a single service profile or across multiple service profiles did not have a unique IQN initiator name.

Procedure

Step 1 Log into the Cisco UCS Manager CLI.

Step 2 Run the following command to view a list of the IQNs in the Cisco UCS domain:

UCS-A# **show identity iqn** | **include** *iqn name*

Step 3 In Cisco UCS PowerTool, run the script to identify the iSCSI vNICs which include the duplicate IQNs.

Step 4 In the service profile to which the IQN initiator name is not registered, change the initiator identity to the default IQN pool or manually assign a unique IQN.

Step 5 In the service profile in which you changed the initiator identity, change the initiator assignment to the name or pool you assigned, as follows:

a) UCS-A # **scope org** *org-name*

Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

b) UCS-A /org # **scope service-profile** *profile-name*

Enters service profile organization mode for the service profile.

c) UCS-A/org# scope vnic-iscsi *iscsi_vnic_name*

Enters the mode for the specified iSCSI vNIC.

Note This vNIC is not registered or visible through **show identity iqn**.

d) UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

e) UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**

Commits the transaction to the system configuration.

Note Changing initiator names also involves storage side configuration, which is beyond the scope of this document.

Step 6 Perform an action on the service profile to register the initiator names in the Cisco UCS database.

For example, you can upgrade the firmware on the associated server or modify the description or label of the service profile.

Step 7 Run the following command to verify that the IQN changes were registered:

UCS-A**show identity iqn** | **include** *iqn name*

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\windowspowershell\v1.0\powershell.exe
-NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.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.

Reconfiguring IQN Initiator Names on a Service Profile Bound to an Updating Service Profile Template

Problem—After an upgrade from Cisco UCS, Release 2.0(1) to Release 2.0(2), Cisco UCS Manager raises an IQN-related fault on one or more service profiles and you cannot reconfigure the duplicate IQN initiator name on the service profile.

Possible Cause—The service profile that does not have a unique IQN initiator name is based on an updating service profile template.

Procedure

Step 1 Log into the Cisco UCS Manager CLI.

Step 2 UCS-A # **scope org** *org-name*

Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

Step 3 UCS-A /org # **scope service-profile** *profile-name*

Enters service profile organization mode for the service profile.

Step 4 UCS-A/org# scope vnic-iscsi *iscsi_vnic1_name*

Enters the mode for the first iSCSI vNIC assigned to the service profile.

Step 5 UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

Step 6 UCS-A /org/service-profile/vnic-iscsi* # **exit**

Exits the mode for the specified iSCSI vNIC

Step 7 UCS-A/org# scope vnic-iscsi *iscsi_vnic2_name*

Enters the mode for the second iSCSI vNIC assigned to the service profile.

Step 8 UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}

Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.

Step 9 UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**

Commits the transaction to the system configuration.

Step 10 In the Cisco UCS Manager GUI, unbind the service profile from the updating service profile template.

Troubleshooting Issues with Registering Cisco UCS Domains in Cisco UCS Central

…

Date and time mismatch is the most common issue with registration.

To ensure that the date and time between Cisco UCS Central and Cisco UCS domains are in sync, try the following:

- Ensure that you have a valid NTP configuration with Cisco UCS Central and the Cisco UCS domains.
- Ensure that Cisco UCS Central is running behind the time for the Cisco UCS domains. This ensures that the start date of a certificate issued by Cisco UCS Central is not in the future.
- If the certificate is not valid, regenerate the default keyring certificate from Cisco UCS Central using the following commands:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring default
UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

- If you have issues after correcting the configuration, you may need to update the shared secret in Cisco UCS Manager.

```
UCSM# scope system
UCSM /system # scope control-ep policy
UCSM /system/control-ep # set shared-secret
     Shared Secret for Registration:
UCSM /system/control-ep* # commit-buffer
```

Important Before calling Cisco TAC, make sure that:

- You synchronize the date and time in Cisco UCS Central and registered Cisco UCS domains.
- Cisco UCS Domain is not in suspended or lost visibility state.
- The registration status for the domain displays **Registered**.