Using Cisco UCS Manager for RAID Configuring and Monitoring

Cisco UCS Manager Configuration

This chapter describes monitoring and configuring your RAID controller using Cisco UCS Manager. The Cisco B-Series servers have built-in monitoring and configuration tools for storage, including RAID.

Note Cisco UCS Manager is used both with B-series blade servers and C-series rack servers that have been integrated.

Cisco UCS Manager interfaces with the LSI controllers and software and creates RAID configurations as part of creating local disk configuration policies, which allow the same configuration steps to be applied to many servers at once.

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the on-board RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- No Local Storage—For a diskless server or a SAN-only configuration. If you select this option, you cannot associate any service profile that uses this policy with a server that has a local disk.
- RAID 0 Striped—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- RAID 1 Mirrored—Data is written to two disks, which provides complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.

- Any Configuration—For a server configuration that carries forward the local disk configuration without any changes.
- No RAID—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- RAID 5 Striped Parity—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- RAID 6 Striped Dual Parity—Data is striped across all disks in the array, and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- RAID10 Mirrored and Striped— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.

You must include this policy in a service profile, and that service profile must be associated with a server for the policy to take effect.

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

- No Mixed HDDs and SSDs

  Mixing HDD and SSDs in a single server or RAID configuration is not supported.

  Block size should be same for each disk involved.

- Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

  Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or reassign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes the Any Configuration or JBOD modes.

- Impact of Upgrade to Release 1.3(1i) or Higher

  An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade.

- Unassociated Servers

  After you upgrade the Cisco UCS domain, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.

Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

- Associated Servers

  Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

  When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Guidelines for Local Disk Configuration Policies Configured for RAID

- No Mixed HDDs and SSDs

  Do not include HDDs and SSDs in a single RAID configuration.

- Server May Not Boot After RAID 1 Cluster Migration if Any Configuration Mode Specified in Service Profile

  After RAID 1 clusters are migrated, you must associate a service profile with the server. If the local disk configuration policy in the service profile is configured with Any Configuration mode rather than RAID 1, the RAID LUN remains in an “inactive” state during and after association. As a result, the server cannot boot.

  To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the Any Configuration mode.

- Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

  If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server.

  If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

- Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

  Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with MegaRAID storage controllers. JBOD mode and operations are not supported on these servers.

- Maximum of One RAID Volume Using RAID 0 or RAID 1 Disk Policy

  A rack-mount server that has been integrated with Cisco UCS Manager can have a maximum of one RAID 1 or RAID 0 volume using the Local Disk Policy irrespective of how many hard drives are present on the server. If you require multiple volumes you must use the “Any Configuration” local drive policy and configure the volumes using the LSI tools outside of UCSM.

- Number of Disks Selected in Mirrored RAID Should Not Exceed Two

  If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

Creating a Local Disk Configuration Policy

SUMMARY STEPS

1. In the Navigation pane, click the **Servers** tab.
2. On the Servers tab, expand **Servers** > **Policies**.
3. Expand the node for the organization where you want to create the policy.
4. Right-click **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.
5. In the **Create Local Disk Configuration Policy** dialog box, complete the following fields:
6. Click **OK**.

DETAILED STEPS

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td>In the Navigation pane, click the Servers tab.</td><td></td></tr>
<tr><td>Step 2</td><td>On the Servers tab, expand Servers > Policies.</td><td></td></tr>
<tr><td>Step 3</td><td>Expand the node for the organization where you want to create the policy.</td><td>If the system does not include multi-tenancy, expand the root node.</td></tr>
<tr><td>Step 4</td><td>Right-click Local Disk Config Policies and choose Create Local Disk Configuration Policy.</td><td></td></tr>
<tr><td>Step 5</td><td>In the Create Local Disk Configuration Policy dialog box, complete the following fields:</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Name field</td><td>The name of the policy.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</td></tr>
<tr><td>Description field</td><td>A description of the policy. We recommend that you include information about where and when the policy should be used.

Enter up to 256 characters. You can use any characters or spaces except ^ (carat), \ (back slash), > (greater than), < (less than), ' (single quote), " (double quote), ` (accent mark), or = (equal sign).</td></tr>
</table>
</td></tr>
</table>

	Command or Action	Purpose	
		Option	**Description**
		Mode drop-down list	

	Command or Action	Purpose	
		Option	**Description**
			This can be one of the following local disk policy modes: • No Local Storage—For a diskless server or a SAN-only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk. • RAID 0 Striped—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails. • RAID 1 Mirrored—Data is written to two disks, which provides complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives. • Any Configuration—For a server configuration that carries forward the local disk configuration without any changes. • No RAID—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered. • RAID 5 Striped Parity—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates. • RAID 6 Striped Dual Parity—Data is striped across all disks in the array nd two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored. • RAID10 Mirrored and Striped—

	Command or Action	Purpose	
		Option	**Description**
			RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates. **Note** If you choose No RAID and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the No RAID mode. To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the No RAID configuration mode.

	Command or Action	Purpose
		Option / **Description** **Protect Configuration** check box: If checked, the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile. **Caution** Protect Configuration becomes non functional if one or more disks in the server are defective or faulty. This property is checked by default. When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile. **Note** If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.
Step 6	Click **OK**.	

Changing a Local Disk Configuration Policy

This procedure describes how to change a local disk configuration policy from an associated service profile. You can also change a local disk configuration policy from the Policies node of the Servers tab.

SUMMARY STEPS

1. In the Navigation pane, click the **Servers** tab.
2. On the Servers tab, expand **Servers** > **Service Profiles**.
3. Expand the organization that includes the service profile with the local disk configuration policy you want to change.
4. In the Work pane, click the **Policies** tab.
5. In the **Actions** area, click **Change Local Disk Configuration Policy**.

6. In the **Change Local Disk Configuration Policy** dialog box, choose one of the following options from the **Select the Local Disk Configuration Policy** drop-down list.
7. Click **OK**.
8. (Optional) Expand the Local Disk Configuration Policy area to confirm that the change has been made.

DETAILED STEPS

	Command or Action	Purpose
Step 1	In the Navigation pane, click the **Servers** tab.	
Step 2	On the Servers tab, expand **Servers** > **Service Profiles**.	
Step 3	Expand the organization that includes the service profile with the local disk configuration policy you want to change.	If the system does not include multi-tenancy, expand the **root** node.
Step 4	In the Work pane, click the **Policies** tab.	
Step 5	In the **Actions** area, click **Change Local Disk Configuration Policy**.	
Step 6	In the **Change Local Disk Configuration Policy** dialog box, choose one of the following options from the **Select the Local Disk Configuration Policy** drop-down list.	**Option** / **Description** **Use a Disk Policy** — Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile. Create a Local Disk Policy — Enables you to create a local disk configuration policy that can only be accessed by the selected service profile. No Disk Policy — Does not use a local disk configuration policy for the selected service profile.
Step 7	Click **OK**.	
Step 8	(Optional) Expand the Local Disk Configuration Policy area to confirm that the change has been made.	

Deleting a Local Disk Configuration Policy

SUMMARY STEPS

1. In the Navigation pane, click the **Servers** tab.
2. On the Servers tab, expand **Servers** > **Policies** > **Organization_Name**.
3. Expand the **Local Disk Config Policies** node.
4. Right-click the policy you want to delete and choose **Delete**.
5. If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

DETAILED STEPS

	Command or Action	Purpose
Step 1	In the Navigation pane, click the **Servers** tab.	
Step 2	On the Servers tab, expand **Servers** > **Policies** > **Organization_Name**.	
Step 3	Expand the **Local Disk Config Policies** node.	
Step 4	Right-click the policy you want to delete and choose **Delete**.	
Step 5	If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.	

Server Disk Drive Monitoring

The disk drive monitoring for Cisco UCS provides Cisco UCS Manager with blade-resident disk drive status for supported blade servers in a Cisco UCS domain. Disk drive monitoring provides a unidirectional fault signal from the LSI firmware to Cisco UCS Manager to provide status information.

The following server and firmware components gather, send, and aggregate information about the disk drive status in a server:

- Physical presence sensor—Determines whether the disk drive is inserted in the server drive bay.
- Physical fault sensor—Determines the operability status reported by the LSI storage controller firmware for the disk drive.
- IPMI disk drive fault and presence sensors—Sends the sensor results to Cisco UCS Manager.
- Disk drive fault LED control and associated IPMI sensors—Controls disk drive fault LED states (on/off) and relays the states to Cisco UCS Manager.

Support for Disk Drive Monitoring

Disk drive monitoring only supports certain blade servers and a specific LSI storage controller firmware level.

Through Cisco UCS Manager, you can monitor disk drives for the following servers:

- B200 blade server
- B230 blade server
- B250 blade server
- B440 blade server

Cisco UCS Manager cannot monitor disk drives in any other blade server or rack-mount server. The storage controller on a supported server must have LSI firmware. Cisco UCS Manager cannot disk drives in servers with a different version of the storage controller firmware.

In addition to the supported servers and storage controller firmware version, you must ensure that the following prerequisites have been met for 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

SUMMARY STEPS

1. In the Navigation pane, click the **Equipment** tab.
2. On the Equipment tab, expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.
3. Click the server for which you want to view the status of the disk drive.
4. In the Work pane, click the **Inventory** tab.
5. Click the **Storage** sub-tab.
6. Click the down arrows to expand the Disks bar and view the following fields in the States section for each disk drive:

DETAILED STEPS

	Command or Action	Purpose
Step 1	In the Navigation pane, click the **Equipment** tab.	
Step 2	On the Equipment tab, expand **Equipment** > **Chassis** > **Chassis Number** > **Servers**.	
Step 3	Click the server for which you want to view the status of the disk drive.	
Step 4	In the Work pane, click the **Inventory** tab.	
Step 5	Click the **Storage** sub-tab.	

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 6</td><td>Click the down arrows to expand the Disks bar and view the following fields in the States section for each disk drive:</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Operability field</td><td>The operational state of the disk drive, which can be one of the following:
Operable—The disk drive is operable.
Inoperable—The disk drive is inoperable, possibly due to a hardware issue such as bad blocks.
N/A—The operability of the disk drive cannot be determined, which could be due to the server or firmware not being supported for disk drive monitoring, or because the server is powered off.
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 POST (Power On Self Test) has not completed.</td></tr>
<tr><td>Presence field</td><td>The presence of the disk drive, and whether it can be detected in the server drive bay, regardless of its operational state, which can be either of the following:
Equipped—A disk drive can be detected in the server drive bay.
Missing—No disk drive can be detected in the server drive bay.</td></tr>
</table>
</td></tr>
</table>

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 disk 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 property values.

Table 1: Disk States

Operability Status	Presence Status	Interpretation
Operable	Equipped	No fault condition. The disk drive is in the server and can be used.
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 POST (Power On Self Test) has not completed.

RAID Controllers in UCS Servers

Table 2: C-Series RAID Controllers

Server Model	Onboard Controller	Integrated Controller	MegaRAID Controller
C200 LFF	Intel ICH10R	LSI 1064E	LSI MR 9260-4i LSI MR 9280-4i4e
C200 SFF	Intel ICH10R	LSI 1068E	LSI MR 9260-8i LSI MR 9280-4i4e
C210	Intel ICH10R	LSI 1064E	LSI MR 9280-4i4e LSI MR 9261-8i
C250	—	LSI SAS 3081E-R	LSI MR 9261-8i
C260	—	—	LSI MR 9261-8i
C460	—	—	LSI MR 9240-8i LSI MR 9260-8i
C220	Embedded MegaRAID	Cisco SAS 2008M-8i	LSI MR 9266-8i LSI MR SAS 9266CV-8i LSI MR 9285CV-8e
C240	Embedded MegaRAID	Cisco SAS 2008M-8i	LSI MR 9266-8i LSI MR SAS 9266CV-8i LSI MR 9285CV-8e

All B-series servers use a fixed onboard controller that is not field replaceable. The controller uses the same integrated SAS or MegaRAID firmware as the C-series servers, but except as noted, configuration and other software tasks are done using Cisco UCS Manager. Table 3-3 shows the B-series RAID Controllers

Table 3: B-Series RAID Controllers

Server Model	SAS Controller	MegaRAID Controller
B200 (M1 and M2)	LSI 1064E	—
B200 M3	LSI SAS 2004	—
B230	—	LSI SAS 2008 (onboard version of the LSI MegaRAID 9240) **Note** This server model only has 2 disks

Server Model	SAS Controller	MegaRAID Controller
B250 (M1 and M2)	LSI 1064E	—
B440	—	LSI SAS 2108 (onboard version of the LSI MegaRAID 9260)
B22	LSI SAS 2002	—

Determining Which Controller is in Your Server

You can use the Cisco UCS Manager GUI Inventory tab to determine which controller is installed in a server. CIMC has a similar functionality.

If you do not have a record of which device is used in the server, you can read the on-screen messages that are displayed during system bootup. These messages display information about the devices that are installed in your server.

- Information about the models of card installed are displayed as part of the verbose boot. You are also prompted to press Ctrl-H to launch configuration utilities for those cards. For servers running CIMC firmware earlier than release 1.2(1), see also Disabling Quiet Boot for CIMC Firmware Earlier than Release 1.2(1).
- If a mezzanine-style card is enabled, you are prompted to press Ctrl-C to launch the configuration for these cards.
- If no models of card are displayed but there is a RAID configuration, your server is using the onboard ICH10R controller. You are also prompted to press Ctrl-M to launch the configuration utilities for this controller.

RAID Controllers

You can order or configure the B-Series servers with the following RAID controller options:

- The Cisco UCS B200 and B250 servers have an LSI 1064E controller on the motherboard. The controller supports RAID 0 and 1 for up to two SAS or two SATA drives. The controller must be enabled in Cisco UCS Manager before configuring RAID. All RAID options can be configured from Cisco UCS Manager.
- The Cisco UCS B440 servers have the LSI MegaRAID controller (the model varies by server). Depending on the license key installed, these controllers provide RAID 0, 1, 5, 6, and 10 support for up to four SAS or SATA drives.
- The Cisco B200 M3 servers have an LSI SAS 2004 RAID controller on the motherboard. The controller supports RAID 0 and 1 for up to two SAS or two SATA drives.

Note If you ever need to move a RAID cluster from one server to another, both the old and new servers for the cluster must use the same LSI controller. For example, migration from a server with an LSI 1064E to a server with an LSI MegaRAID is not supported.

If there is no record of which option is used in the server, disable the quiet boot feature and read the messages that appear during system boot. Information about the models of installed RAID controllers appears as part of the verbose boot feature. You are prompted to press Ctrl-H to launch configuration utilities for those controllers.

Disabling Quiet Boot

When the quiet boot feature is disabled, the controller information and the prompts for the option ROM-based LSI utilities are displayed during bootup.

SUMMARY STEPS

1. Boot the server and watch for the F2 prompt during the boot process.
2. To enter the BIOS Setup Utility, press **F2** when prompted.
3. On the Main page of the BIOS Setup Utility, set Quiet Boot to **disabled**.
4. Press **F10** to save the changes and exit the utility.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Boot the server and watch for the F2 prompt during the boot process.	
Step 2	To enter the BIOS Setup Utility, press **F2** when prompted.	
Step 3	On the Main page of the BIOS Setup Utility, set Quiet Boot to **disabled**.	This action allows non default messages, prompts, and POST messages to display during bootup instead of the Cisco logo window.
Step 4	Press **F10** to save the changes and exit the utility.	

Accessing ROM-Based Controller Utilities

To change the RAID configurations on your hard drives, use the host-based utilities that were installed on top of the host OS. You can also use the LSI option ROM-based utilities that are installed on the server.

SUMMARY STEPS

1. Boot the server with Quiet mode disabled.
2. During the verbose boot process, enter one of the following control commands when the prompt for the desired controller appears.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Boot the server with Quiet mode disabled.	Information about the controller appears along with the prompts for the key combination to launch the LSI option ROM-based utilities for your controller.

	Command or Action	Purpose
Step 2	During the verbose boot process, enter one of the following control commands when the prompt for the desired controller appears.	• When the Ctrl-H prompt appears, press **Ctrl-H** to enter the LSI controller card utility. • When the Ctrl-M prompt appears, press **Ctrl-M** to enter the onboard Intel ICH10R controller utility.

Documentation About RAID Controllers and LSI Utilities

The LSI utilities have manufacturer documentation. For non Cisco UCS-specific information on RAID and how to use the LSI utilities, see the following documentation:

- *LSI MegaRAID SAS Software User's Guide (for LSI MegaRAID)*
- *LSI Fusion-MPT Device Management User's Guide (for LSI 3081E)*
- *LSI SAS2 Integrated RAID Solution User Guide (for LSI SAS1064E)*

Moving a RAID Cluster Using UCS Software Version 1.4(1)

You can set a server to recognize a RAID cluster created on another server. This procedure is useful when upgrading from the M1 version of a server to the M2 version of a server. You can also use this procedure whenever data on a RAID cluster needs to be moved between servers.

Note Both the old and new servers for the cluster must use the same LSI controller. For example, migration from a server with an LSI 1064E to a server with an LSI MegaRAID is not supported.

Before you begin

Verify that the service profiles for both the source and destination servers have an identical local disk configuration policy and can boot successfully.

SUMMARY STEPS

1. Put both the start and destination servers for the RAID cluster in the associated state.
2. Shut down both servers.
3. After the servers power off, physically move the drives in the array to the destination server. If you are changing servers but keeping the drives in the same slots, insert the new server into the slot of the original server.
4. Connect the KVM dongle.
5. Connect a monitor, keyboard, and mouse to the destination server.
6. Boot the destination server, using the power switch on the front of the server. If necessary, disable the quiet boot feature and boot again.
7. Wait for the LSI Configuration Utility banner.
8. To enter the LSI Configuration Utility, press **Ctrl-C**.
9. From the **SAS Adapter List** window, choose the SAS adapter used in the server.

10. Choose **RAID Properties**. The **View Array** window appears.
11. Choose **Manage Array**. The **Manage Array** window appears.
12. Choose **Activate Array**. When the activation is complete, the RAID status changes to Optimal.
13. On the **Manage Array** window, choose **Synchronize Array**.
14. Wait for the mirror synchronization to complete, and monitor the progress bar that comes up.
15. When the mirror synchronization is complete, press the **ESC** key several times to go back through each of the widows (one at a time) and then exit the LSI Configuration Utility.
16. Choose the **reboot** option to implement the changes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Put both the start and destination servers for the RAID cluster in the associated state.	
Step 2	Shut down both servers.	**Note** When using this procedure during an M1 to M2 upgrade or a direct replacement within a slot, at this point in process the destination server is not yet associated and does not have a disk policy. When the destination server is inserted into the slot where the start server was located, the destination server inherits policies from the start server. The raid controller and the PnuOS reads the disk and RAID volume details during the subsequent association (when PnuOS boots).
Step 3	After the servers power off, physically move the drives in the array to the destination server. If you are changing servers but keeping the drives in the same slots, insert the new server into the slot of the original server.	
Step 4	Connect the KVM dongle.	
Step 5	Connect a monitor, keyboard, and mouse to the destination server.	
Step 6	Boot the destination server, using the power switch on the front of the server. If necessary, disable the quiet boot feature and boot again.	
Step 7	Wait for the LSI Configuration Utility banner.	
Step 8	To enter the LSI Configuration Utility, press **Ctrl-C**.	
Step 9	From the **SAS Adapter List** window, choose the SAS adapter used in the server.	
Step 10	Choose **RAID Properties**. The **View Array** window appears.	
Step 11	Choose **Manage Array**. The **Manage Array** window appears.	

	Command or Action	Purpose
Step 12	Choose **Activate Array**. When the activation is complete, the RAID status changes to Optimal.	
Step 13	On the **Manage Array** window, choose **Synchronize Array**.	
Step 14	Wait for the mirror synchronization to complete, and monitor the progress bar that comes up.	The time to complete the synchronization can vary depending upon the size of the disks in the RAID array.
Step 15	When the mirror synchronization is complete, press the **ESC** key several times to go back through each of the widows (one at a time) and then exit the LSI Configuration Utility.	
Step 16	Choose the **reboot** option to implement the changes.	

Moving a RAID Cluster Using UCS Software Version 1.4(2) and Later Releases

You can set a server to recognize a RAID array created on another server. This procedure is useful when upgrading from the M1 version of a server to the M2 version of a server. You can also use this procedure whenever data on a RAID array needs to be moved between servers.

Note Both the old and new servers for the cluster must use the same LSI controller family. For example, migration between a server with an LSI 1064 to a server with an LSI MegaRAID is not supported.

Before you begin

Verify that the service profiles for both the source and destination servers have an identical local disk configuration policy and can boot successfully.

SUMMARY STEPS

1. Decommission both the source and destination servers from Cisco UCS Manager.
2. Wait for the servers to shut down (Decommission Server prompts you to shut down the server).
3. After the servers power off, physically move the drives in the array to the destination server.
4. Power on the servers by pressing the front power button of each of the servers.
5. Choose Reacknowledge Slot for each of the slots (Source and Destination). If Cisco UCS Manager prompts you to Resolve Slot Issue, choose the here link in the Resolve Slot window and resolve the slot issue before server discovery begins.
6. Wait for server discovery and association to complete for each server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Decommission both the source and destination servers from Cisco UCS Manager.	

	Command or Action	Purpose
Step 2	Wait for the servers to shut down (Decommission Server prompts you to shut down the server).	**Note** When you use this procedure during an M1 to M2 upgrade or a direct replacement within a slot, at this point in the process the destination server is not yet associated and does not have a disk policy. When the destination server is inserted into the slot where the start server was located, the destination server inherits policies from the start server. The RAID controller and the PnuOS reads the disk and RAID volume details during the subsequent association (when PnuOS boots).
Step 3	After the servers power off, physically move the drives in the array to the destination server.	If you are changing servers but keeping the drives in the same slots, insert the new server into the slot of the original server.
Step 4	Power on the servers by pressing the front power button of each of the servers.	
Step 5	Choose Reacknowledge Slot for each of the slots (Source and Destination). If Cisco UCS Manager prompts you to Resolve Slot Issue, choose the here link in the Resolve Slot window and resolve the slot issue before server discovery begins.	
Step 6	Wait for server discovery and association to complete for each server.	If each of the preceding steps runs without issues, the servers boot up with the OS that was installed on the respective RAID volumes prior to the RAID Cluster Migration.

Moving a RAID Cluster Between B200 M3 Servers

You can set a server to recognize a RAID cluster created on another server. You can also use this procedure whenever data on a RAID cluster needs to be moved between servers.

Before you begin

Verify that the service profiles for both the source and destination servers have an identical local disk configuration policy and can boot successfully.

SUMMARY STEPS

1. Shut down the source server's operating system from within that operating system.
2. Disassociate the service profile currently applied to the B200M3 server.
3. Physically move the drives in the array to the destination server.
4. Reassociate the service profile to the new blade, keeping the same LD Config Policies as were previously used.
5. Power on the servers by pressing the front power button of each of the servers.
6. Open a KVM connection to the new server and wait for the Storage Web BIOS Utility.
7. Follow the web BIOS Utility prompts to migrate the RAID LUN.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Shut down the source server's operating system from within that operating system.	Before proceeding, verify that the OS has shut down completely and not restarted itself.
Step 2	Disassociate the service profile currently applied to the B200M3 server.	
Step 3	Physically move the drives in the array to the destination server.	If you are changing servers, you must keep the drives in the same slot in the new server as they were in the original server.
Step 4	Reassociate the service profile to the new blade, keeping the same LD Config Policies as were previously used.	
Step 5	Power on the servers by pressing the front power button of each of the servers.	
Step 6	Open a KVM connection to the new server and wait for the Storage Web BIOS Utility.	
Step 7	Follow the web BIOS Utility prompts to migrate the RAID LUN.	

Replacing a Failed Drive in a RAID Cluster

We recommend that you follow the industry standard practice of using drives of the same capacity when creating RAID volumes. If you use drives of different capacities, the usable portion of the smallest drive is used on all drives that make up the RAID volume.

Before you begin

Replace a failed HDD or SSD only with a drive that has the same Cisco product ID (PID). Before changing an HDD in a running system, check the service profile in Cisco UCS Manager to make sure that the new hardware configuration is within the parameters allowed by the service profile.

SUMMARY STEPS

1. Connect the KVM dongle to the server with the failed drive.
2. Connect a monitor, keyboard, and mouse to the destination server.
3. Physically replace the failed drive.
4. Boot the server, using the power switch on the front of the server.
5. Wait for the LSI Configuration Utility banner.
6. To enter the LSI Configuration Utility, press **Ctrl-C**.
7. From the **SAS Adapter List** window, choose the SAS adapter used in the server.
8. Choose **RAID Properties**.
9. Choose **Manage Array**.
10. Choose **Activate Array**.
11. On the **Manage Array** screen, choose **Synchronize Array**.
12. Wait for the mirror synchronization to complete, and monitor the progress bar that comes up.

13. When the mirror synchronization is complete, press the **ESC** key several times to go back through each of the windows (one at a time) and then exit the LSI Configuration Utility.
14. Choose the **reboot** option to implement the changes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Connect the KVM dongle to the server with the failed drive.	
Step 2	Connect a monitor, keyboard, and mouse to the destination server.	
Step 3	Physically replace the failed drive.	If needed, refer to the service note for your server model. In general, the steps are similar for most models.
Step 4	Boot the server, using the power switch on the front of the server.	If necessary, disable the quiet boot feature and boot again. See Disabling Quiet Boot, on page 16.
Step 5	Wait for the LSI Configuration Utility banner.	
Step 6	To enter the LSI Configuration Utility, press **Ctrl-C**.	
Step 7	From the **SAS Adapter List** window, choose the SAS adapter used in the server.	To determine which RAID controller is being used, refer to RAID Controllers, on page 15.
Step 8	Choose **RAID Properties**.	The **View Array** window appears.
Step 9	Choose **Manage Array**.	The **Manage Array** window appears.
Step 10	Choose **Activate Array**.	When the activation is complete, the RAID status changes to Optimal.
Step 11	On the **Manage Array** screen, choose **Synchronize Array**.	
Step 12	Wait for the mirror synchronization to complete, and monitor the progress bar that comes up.	**Note** The time to complete the synchronization can vary depending upon the size of the disks in the RAID array.
Step 13	When the mirror synchronization is complete, press the **ESC** key several times to go back through each of the windows (one at a time) and then exit the LSI Configuration Utility.	
Step 14	Choose the **reboot** option to implement the changes.	