Managing Storage Adapters

This chapter includes the following sections:

Managing Storage Adapters

Self Encrypting Drives (Full Disk Encryption)

Cisco IMC supports self encrypting drives (SED). A special hardware in the drives encrypts incoming data and decrypts outgoing data in real-time. This feature is also called Full Disk Encryption (FDE).

The data on the drive is encrypted on its way into the drive and decrypted on its way out. However, if you lock the drive, no security key is required to retrieve the data.

When a drive is locked, an encryption key is created and stored internally. All data stored on this drive is encrypted using that key, and stored in encrypted form. Once you store the data in this manner, a security key is required in order to un-encrypt and fetch the data from the drive. Unlocking a drive deletes that encryption key and renders the stored data unusable. This is called a Secure Erase. The FDE comprises a key ID and a security key.

The FDE feature supports the following operations:

- Enable and disable security on a controller

- Create a secure virtual drive

- Secure a non-secure drive group

- Unlock foreign configuration drives

- Enable security on a physical drive (JBOD)

- Clear secure SED drives

- Clear secure foreign configuration

Scenarios to consider While Configuring Controller Security in a Dual SIOC Environment

Note   Dual SIOC connectivity is available only on some servers.

Controller security can be enabled, disabled, or modified independently. However, local and remote key management applies to all the controllers on the server. Therefore security action involving switching the key management modes must be performed with caution. In a scenario where both controllers are secure, and you decide to move one of the controllers to a different mode, you need to perform the same operation on the other controller as well.

Consider the following two scenarios:

- Scenario 1—Key management is set to remote; both controllers are secure and use remote key management. If you now wish to switch to local key management, switch the key management for each controller and disable remote key management.

- Scenario 2—Key management is set to local; both controllers are secure and use local key management. If you now wish to switch to remote key management, enable remote key management and switch the key management for each controller.

If you do not modify the controller security method on any one of the controllers, it renders the secure key management in an unsupported configuration state.

Creating Virtual Drive from Unused Physical Drives

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	In the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3	In the **Actions** area, click **Create Virtual Drive from Unused Physical Drives**.
	The **Create Virtual Drive from Unused Physical Drives** dialog box displays.
Step 4	In the **Create Virtual Drive from Unused Physical Drives** dialog box, select the RAID level for the new virtual drives:

This can be one of the following:

- **Raid 0**—Simple striping.

- **Raid 1**—Simple mirroring.

- **Raid 5**—Striping with parity.

- **Raid 6**—Striping with two parity drives.

- **Raid 10**—Spanned mirroring.

- **Raid 50**—Spanned striping with parity.

             • **Raid 60**—Spanned striping with two parity drives.

Step 5   In the **Create Drive Groups** area, choose one or more physical drives to include in the group.

          Use the **>>** button to add the drives to the **Drive Groups** table. Use the **<<** button to remove physical drives from the drive group.

        Note   The size of the smallest physical drive in the drive group defines the maximum size used for all the physical drives. To ensure maximum use of space for all physical drives, it is recommended that the size of all the drives in the drive group are similar.

        Note   Cisco IMC manages only RAID controllers and not HBAs attached to the server.

Step 6   In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.
Write Policy drop-down list	This can be one of the following • **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. • **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. • **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following • **Unchanged**— The disk cache policy is unchanged. • **Enabled**— Allows IO caching on the disk. • **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following • **Read Write**— Enables host to perform read-write on the VD. • **Read Only**— Host can only read from the VD. • **Blocked**— Host can neither read nor write to the VD.

Name	Description
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: • MB • GB • TB

Step 7 Click the **Generate XML API Request** button to generate an API request.

Step 8 Click **Close**.

Step 9 Click **Create Virtual Drive**.

Creating Virtual Drive from an Existing Drive Group

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **Actions** area, click **Create Virtual Drive from an Existing Virtual Drive Group**.

The **Create Virtual Drive from an Existing Virtual Drive Group** dialog box displays.

Step 4 In the **Create Virtual Drive from an Existing Virtual Drive Group** dialog box, select the virtual drive whose drive group you want to use to create a new virtual drive.

Step 5 In the **Virtual Drive Properties** area, update the following properties:

Name	Description
Virtual Drive Name field	The name of the new virtual drive you want to create.
Read Policy drop-down list	The read-ahead cache mode.
Cache Policy drop-down list	The cache policy used for buffering reads.
Strip Size drop-down list	The size of each strip, in KB.

Name	Description
Write Policy drop-down list	This can be one of the following **Write Through**— Data is written through the cache and to the physical drives. Performance is improved, because subsequent reads of that data can be satisfied from the cache. **Write Back**— Data is stored in the cache, and is only written to the physical drives when space in the cache is needed. Virtual drives requesting this policy fall back to **Write Through** caching when the BBU cannot guarantee the safety of the cache in the event of a power failure. **Write Back Bad BBU**—With this policy, write caching remains **Write Back** even if the battery backup unit is defective or discharged.
Disk Cache Policy drop-down list	This can be one of the following **Unchanged**— The disk cache policy is unchanged. **Enabled**— Allows IO caching on the disk. **Disabled**— Disallows disk caching.
Access Policy drop-down list	This can be one of the following **Read Write**— Enables host to perform read-write on the VD. **Read Only**— Host can only read from the VD. **Blocked**— Host can neither read nor write to the VD.
Size field	The size of the virtual drive you want to create. Enter a value and select one of the following units: - MB - GB - TB

Step 6   Click the **Generate XML API Request** button to generate an API request.

Step 7   Click **Close**.

Step 8   Click **Create Virtual Drive**.

Setting a Virtual Drive to Transport Ready State

You can move a virtual drive from one MegaRAID controller to another using the **Set Transport Ready** feature. This allows all the pending IOs of the virtual drive to complete their activities, hide the virtual drive from the operating system, flush cache, pause all the background operations, and save the current progress in

disk data format, allowing you to move the drive. When you move a virtual drive, all other drives belonging to the same drive group inherit the same change as the moved drive.

When the last configured physical drive on the group is removed from the current controller, the drive group becomes foreign and all foreign configuration rules apply to the group. However, the Transport Ready feature does not change any foreign configuration behavior.

You can also clear a virtual drive from the Transport Ready state. This makes the virtual drive available to the operating systems.

Following restrictions apply to a transport ready virtual drive:

- Only a maximum of 16 transport ready drive groups are currently supported.

- This feature is not supported on high availability.

- A virtual drive cannot be set as transport ready under these conditions:

    - When a virtual drive of a drive group is being reconstructed

    - When a virtual drive of a drive group contains a pinned cache

    - When a virtual drive of a drive group is marked as cacheable or associated with a cachecade virtual drive

    - If a virtual drive is a cachecade virtual drive

    - If a virtual drive is offline

    - If a virtual drive is a bootable virtual drive

Setting a Virtual Drive as Transport Ready

Before you begin

- You must log in with admin privileges to perform this task.

- The virtual drive must be in optimal state to enable transport ready.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	On the **Storage** menu, click the appropriate LSI MegaRAID Controller.
Step 3	On the **Work** pane, click the **Virtual Drive Info** tab.
Step 4	In the **Virtual Drives** area, choose the drive that you want set as transport ready.
Step 5	In the **Actions** area, click **Set Transport Ready**.
	The **Set Transport Ready** dialog box displays.
Step 6	Update the following properties in the dialog box:

Name	Description
Initialize Type drop-down list	Allows you to select the initialization type using which you can set the selected virtual drive as transport ready. This can be one of the following: • **Exlude All**— Excludes all the dedicated hot spare drives. • **Include All**— Includes any exclusively available or shared dedicated hot spare drives. • **Include Dedicated Hot Spare Drive**— Includes exclusive dedicated hot spare drives.
Set Transport Ready button	Sets the selected virtual drive as transport ready.
Cancel button	Cancels the action.

Note When you set a virtual drive to transport ready all the physical drives associated with it are displayed as **Ready to Remove**.

Clearing a Virtual Drive from Transport Ready State

Before you begin

• You must log in with admin privileges to perform this task.

• The virtual drive must be transport ready.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 On the **Work** pane, click the **Virtual Drive Info** tab.

Step 4 In the **Virtual Drives** area, choose the drive to set as transport ready.

Step 5 In the **Actions** area, click **Clear Transport Ready**.

This reverts the selected transport ready virtual drive to its original optimal state.

Clearing Foreign Configuration

☞

Important This task clears all foreign configuration on the controller. Also, all configuration information from all physical drives hosting foreign configuration is deleted. This action cannot be reverted.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.
In the **RAID Controller** area, the **Controller Info** tab displays by default.

Step 3 In the **Actions** area, click **Clear Foreign Config**.

Step 4 Click **OK** to confirm.

Clearing Controller Configuration

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 In the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3 In the **Controller Info** area, click **Clear All Configuration**.

Step 4 Click **OK** to confirm.

This clears the existing controller configuration.

Preparing a Drive for Removal

Note You can perform this task only on physical drives that display the **Unconfigured Good** status.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1 In the **Navigation** pane, click the **Storage** menu.

Step 2 On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   In the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4   In the **Physical Drives** area, select the drive you want to remove.

Step 5   In the **Actions** area, click **Prepare for Removal**.

Step 6   Click **OK** to confirm.

Undo Preparing a Drive for Removal

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** menu.

Step 2   On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   On the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4   In the **Physical Drives** area, select a drive with a status of **Ready to Remove**.

Step 5   In the **Actions** area, click **Undo Prepare for Removal**.

Step 6   Click **OK** to confirm.

Making a Dedicated Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** tab.

Step 2   On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   On the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4   In the **Physical Drives** area, select an unconfigured good drive you want to make a dedicated hot spare.

Step 5   In the **Actions** area, click **Make Dedicated Hot Spare**.

The **Make Dedicated Hot Spare** dialog box displays.

Step 6   In the **Virtual Drive Details** area, update the following properties:

Name	Description
Virtual Drive Number drop-down list	Select the virtual drive to which you want to dedicate the physical drive as hot spare.

Name	Description
Virtual Drive Name field	The name of the selected virtual drive.
Make Dedicated Hot Spare button	Creates the dedicated hot spare.
Cancel button	Closes the dialog box without saving any changes made while the dialog box was open.

Step 7   Click **Make Dedicated Hot Spare** to confirm.

Making a Global Hot Spare

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** tab.

Step 2   On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   In the **RAID Controller** area, click the **Physical Drive Info** tab.

Step 4   In the **Physical Drives** area, select an unconfigured good drive you want to make a global hot spare.

Step 5   In the **Actions** area, click **Make Global Hot Spare**.

Removing a Drive from Hot Spare Pools

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** menu.

Step 2   On the **Storage** tab, click the appropriate LSI MegaRAID controller.

Step 3   On the **Work** pane, click the **Physical Drive Info** tab.

Step 4   In the **Physical Drives** area, select the global or dedicated hot spare you want to remove from the hot spare pools.

Step 5   In the **Actions** area, click **Remove From Hot Spare Pools**.

Initializing a Virtual Drive

All data on a virtual drive is lost when you initialize the drive. Before you run an initialization, back up any data on the virtual drive that you want to save.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3	In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4	In the **Virtual Drives** area, choose the drive that you want to initialize.
Step 5	In the **Actions** area, click **Initialize**.
	The **Initialize Virtual Drive** dialog box displays.
Step 6	Choose the type of initialization you want to use for the virtual drive.
	This can be one of the following:
	• **Fast Initialize**—This option allows you to start writing data to the virtual drive immediately.
	• **Full Initialize**—A complete initialization is done on the new configuration. You cannot write data to the new virtual drive until the initialization is complete.
Step 7	Click **Initialize VD** to initialize the drive, or **Cancel** to close the dialog box without making any changes.
Step 8	To view the status of the task running on the drive, in the **Operations** area, click **Refresh**.
	The following details are displayed:

Name	Description
Operation	Name of the operation that is in progress on the drive.
Progress in %	Progress of the operation, in percentage complete.
Elapsed Time in secs	The number of seconds that have elapsed since the operation began.

Set as Boot Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3	In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4	In the **Virtual Drives** area, choose the drive from which the controller must boot.
Step 5	In the **Actions** area, click **Set as Boot Drive**.
Step 6	Click **OK** to confirm.

Deleting a Virtual Drive

☞

Important   This task deletes a virtual drive, including the drives that run the booted operating system. So back up any data that you want to retain before you delete a virtual drive.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3	In the **RAID Controller** area, click the **Virtual Drive Info** tab.
Step 4	In the **Virtual Drives** area, select the virtual drive you want to delete.
Step 5	In the **Actions** area, click **Delete Virtual Drive**.
Step 6	Click **OK** to confirm.

Hiding a Virtual Drive

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1	In the **Navigation** pane, click the **Storage** menu.
Step 2	On the **Storage** menu, click the appropriate LSI MegaRAID controller.
Step 3	On the **RAID Controller** area, click the **Virtual Drive Info** tab.

Step 4   In the **Virtual Drives** area, select the virtual drive you want to hide.

Step 5   In the **Actions** area, click **Hide Drive**.

Step 6   Click **OK** to confirm.

Starting Learn Cycles for a Battery Backup Unit

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** menu.

Step 2   On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   In the **RAID Controller** area, click the **Battery Backup Unit** tab.

Step 4   From the **Actions** pane, click **Start Learn Cycle**.

A dialog prompts you to confirm the task.

Step 5   Click **OK**.

Viewing Storage Controller Logs

Before you begin

You must log in with admin privileges to perform this task.

Procedure

Step 1   In the **Navigation** pane, click the **Storage** menu.

Step 2   On the **Storage** menu, click the appropriate LSI MegaRAID controller.

Step 3   In the **RAID Controller** area, click **Storage Log** tab and review the following information:

Name	Description
Time column	The date and time the event occurred.

Name	Description
Severity column	The event severity. This can be one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Description column	A description of the event.

Compatibility of UCS-E M3 Module with 4K Native Drives

Data on a disk has historically been relegated to a standard 512 bytes of data per sector. 4K Native (4Kn) Drives or Advanced Format (AF) refers to the next generation in default media allocation size.

4K-sized sectors provide quicker paths to higher areal densities and hard drive capacities as well as more robust error correction. With the ever-increasing demand for higher density storage and with file sizes ever increasing, 4Kn drives are the only option available because 4Kn drives are the most cost-efficient. For example, 512 bytes goes into 4K exactly 8 times. This means that as long as we are aligned in storage parlance, we minimize the amount of unnecessary disk activity.

The software emulation layer uses the 4Kn drives with legacy OS, applications, and existing VMs to run on newer 4Kn drives. Readiness of the support for 4 KB logical sectors within operating systems differs among their types, vendors and versions. For example, Microsoft Windows supports 4Kn drives since Windows 8 and Windows Server 2012.

Note Ensure your application is 4Kn ready to avoid mismatch of what is intended and what actually occurs. The most critical are applications like databases.

Some of the benefits of 4Kn drives over 512 sector size drives are:

• Higher capacity and improved performance from the more optimized placement of data on the drive.

• Efficient space utilization with optimized meta-data giving up to 10% more available data.

• Improved drive reliability and error correction with larger meta-data by increasing the ECC block from 50 to 100 bytes. This provides a much-needed improvement in error correction efficiency.

Limitations of 4Kn Drives

- Only local SAS, SATA HDDs are supported

- Ensure to use VMFS6

- The BIOS must be configured in full UEFI mode while booting from 4Kn drives

- 4Kn SSD, NVMe, and RDM to GOS are not supported

- Third party multi-pathing plugins are not supported

How to use 4Kn Drives as Boot Drives on UCS-E M3 Modules

- Set boot order rules in CIMC's BIOS configuration to 'loose'.

- Check the box for UEFI secure boot in CIMC's BIOS boot order configuration or scope BIOS in CLI. This sets the module in full UEFI mode on next reboot, so that no legacy boot options appears.

- Map the OS installation image in vKVM or the host image mapping in CIMC (or use physical DVD). If you are installing VMware ESXi, use the ESXi 6.7 version or later.

- Reboot the server and press F6 to enter boot override menu when the logo screen appears.

- Select the UEFI option corresponding to your installation media. For instance, "UEFI: CIMC-mapped vDVD".

- When you start the OS installation, check for the 4Kn HDD, and then start the installation on the 4Kn drive.