E-Series

Controller Upgrade Guide

April 2018 | 215-11799_C0
doccomments@netapp.com

NetApp®

Contents

Deciding whether to use this guide

This guide describes how to upgrade a storage array through the replacement of existing controllers. Information pertaining to controller upgrade compatibility, preparation, installation, and reinitialization is detailed within this guide. Specific procedures for single controller and dual controller swaps are also included. Procedures contained within this guide require that the storage array be taken off line.

Use the procedures described within this guide to replace all of the controllers in a controller-drive tray. You typically use these procedures when you choose to upgrade all of the controllers to a different model or platform. You might also use these procedures in the following situations:

- When all controllers in a controller-drive tray encounter hardware failures and are no longer functional
- To upgrade the dual inline memory modules (DIMMs) in your controller-drive tray by replacing both controllers with the same model of controllers, but with different DIMMs

Certain upgrade scenarios are not covered within this guide. Instead, procedures for these scenarios are provided within various E-Series flyer instructions. Examples of scenarios covered within the E-Series flyers include:

- Upgrading the host interface cards (HICs) in your controller-drive tray by replacing both controllers with the same model of controller but with different HICs
- Upgrading the HICs in your controller-drive tray to a different HIC and then converting the host protocol
- Upgrading a controller and HICs currently operating in split-mode protocol

To access the E-series flyers or the other documentation for E-Series storage arrays, go to the NetApp E-Series Systems Documentation Center.

Related information

NetApp E-Series Systems Documentation Center

Controller upgrade considerations

You should keep in mind important considerations for upgrading your controllers, such as requirements for powering off duplex and simplex controllers, managing mirroring features, ensuring battery compatibility, and changing vendor identification.

Duplex and simplex controller upgrades

For duplex controller-drive trays, you replace both controllers. For simplex controller-drive trays, you replace the one controller. In both cases, you must power off the controller-drive tray. As a result, you cannot access data on the storage array until you successfully complete the replacement.

Remote volume and Asynchronous Mirroring

If your storage array participates in remote volume mirroring, only iSCSI or Fibre Channel connections are supported between the primary site and the remote site. If the HIC configuration in your new controllers does not include iSCSI or Fibre Channel connections, remote volume mirroring will not be supported.

For Asynchronous Mirroring, the local storage array and remote storage array can run different versions of firmware. The minimum firmware version supported is SANtricity firmware version 7.84.

Controller batteries

A new controller is shipped without a battery installed. When possible, you should remove the battery from your old controller and then install that battery in the new controller. However, for some controller upgrades, the battery from the old controller is not compatible with the new controller. In those cases, you must order a battery along with your new controller, and have that battery available before you begin these tasks. See *Controller upgrade compatibility* on page 6 for detailed information on controller battery compatibility.

Vendor Identification

Some controller upgrades result in the Vendor ID in SCSI Inquiry Data changing from `LSI` to `NETAPP`. When the Vendor ID changes from `LSI` to `NETAPP`, additional steps are required on the Windows, VMware, and AIX operating systems to reclaim devices. Steps for these operating systems are included in this document.

Controller upgrade compatibility

If you are replacing the controllers to upgrade to a new model, keep in mind that your current storage array might have premium features installed that the new model cannot support. For example, E2700 controllers do not support the legacy Snapshot premium feature. If you replace E2600 controllers with E2700 controllers, and your storage array was using the legacy Snapshots feature, you must disable that feature and delete or convert all volumes (that is, snapshots, repositories) associated with that feature before you replace the controllers. You can convert legacy Snapshots to Snapshots. Before you upgrade a controller-drive tray, you should disable any premium features used on your storage array that are not supported on the new controllers.

If you change your controllers from 5x00 models to 2x00 models, your new storage array configuration will support lower numbers of some objects (for example, volumes) in the storage management software than your old configuration. You must make sure that your old configuration does not exceed the object limits listed below before you replace the controller(s).

- Maximum number of volumes - 512
- Maximum number of partitions - 128
- Maximum number of snapshot volumes - 512
- Maximum number of member volumes per consistency group - 32
- Maximum number of consistency groups - 16
- Maximum number of views - 256
- Maximum number of legacy RVM mirrors - 16
- Maximum number of ARVM mirrors - 32
- Maximum number of ARVM mirrors per mirror group - 32
- Maximum total number or mirrors (Legacy RVM + ARVM) - 32
- Maximum number of volume copies - 511
- Maximum number of thin provisioned volumes - 512
- Maximum number of drive slots in the storage array (controller-drive tray + all attached drive trays) - 192

	To E2x00	To E5x00	To EF5x0
From E2x00	**Battery** - Reuse the old battery. **Vendor ID** - Additional steps required. **Feature Support** - Legacy snapshots are not supported on the E2700. E2800 controllers must not be placed into SAS-2* shelves.	**Battery** - Order a new battery. **Vendor ID** - Additional steps are required when upgrading from E2600 to E5500 or E5600, or when upgrading from E2700 to E5400. **Feature Support** - Legacy snapshots are not supported on the E5500 or E5600. Legacy RVM is not supported on the E5500 or E5600 with iSCSI HICs. Data Assurance is not supported on the E5500 or E5600 with iSCSI HICs. E5400, E5500, and E5600 controllers must not be placed into SAS-3** shelves. E5700 controllers must not be placed into SAS-2* shelves.***	Upgrades are not supported.
From E5x00	**Battery** - Order a new battery. **Vendor ID** - Additional steps are required when upgrading from E5500 or E5600 to E2600, or when upgrading from E5400 to E2700. **Feature Support** - Legacy snapshots are not supported on the E2700.	**Battery** - Reuse the old battery. **Vendor ID** - Additional steps required when upgrading from E5400 to E5500 or E5600. **Feature Support** - No legacy snapshots for E5500 or E5600. No legacy RVM or Data Assurance for E5400/ E5500 with iSCSI HICs. E5400, EF550, and EF560 controllers must not be placed into SAS-3*** shelves. E5700 controllers must not be placed into SAS-2* shelves.***	Upgrades are not supported.

	To E2x00	To E5x00	To EF5x0
From EF5x0	Upgrades are not supported.	Upgrades are not supported.	**Battery** - Reuse the old battery **Vendor ID** - Additional steps required when upgrading from EF540 to EF550 or EF560. **Feature Support** - No Legacy Snapshots for EF550/EF560. No Data Assurance for EF550/EF560 with iSCSI. EF540, EF550, and EF560 controllers must not be placed into SAS-3*** shelves. EF570 controllers must not be placed into SAS-2* shelves.***

* SAS-2 shelves include the following models:

- DE1600, DE5600, and DE6600 drive trays
- E5400, E5500, and E5600 controller-drive trays
- EF540, EF550 and EF560 flash arrays
- E2600 and E2700 controller-drive trays

** SAS-3 shelves include the following models:

- E28XX controller shelves
- E57XX controller shelves
- DE212C, DE224C, DE460C drive shelves

***SAS-2 to SAS-3 investment protection:

- You can reconfigure your SAS-2 system to be used behind a new SAS-3 controller shelf (E57XX/EF570/E28XX).
- For more information, see *Reconfiguring a SAS-2 system for use behind a new SAS-3 controller shelf (E57XX/EF570/E28XX)* on page 39.

Attention: Possible loss of data access – Before you replace the controllers, make sure that any premium features that are installed and any configuration of objects in the storage management software can be supported with your new controllers. Failure to do this will result in an out-of-compliance condition or configuration errors. Contact technical support if you encounter configuration errors.

Attention: Possible loss of data access – If any controller that you are replacing manages any secure volumes, the new controller needs the correct security key to gain access to those volumes. After you replace the controller and restore power to the controller-drive tray, you can use SANtricity Storage Manager (or System Manager) to load the key from the file in which it was saved. Be sure that such a file exists and that you know the pass phrase required to install the security key before you replace the controller.

Related information

NetApp Hardware Universe

E5700 and E2800 - Drive security and controller replacement compatibility

Dual and single controller replacements are supported for a variety of E2800 and E5700 controller configurations. Dual controller replacements are performed for duplex systems (E5700 and E2800 configurations) while single controller replacements can be performed for simplex and duplex systems (E2800 configurations only). A complete replacement of existing controllers in a configuration is known as a controller hardware upgrade (or headswap). This procedure requires that the controller replacements be compatible and the drives may need to be manually unlocked.

If the upgrade is a controller hardware upgrade (or headswap), firmware levels and drive security settings of the base controller determine the result of the controller replacement, including whether secured drives unlock. The following sections provide a workflow summary for the most common E5700 and E2800 controller replacement use cases. For assistance with all other controller replacement scenarios, including downgrade controller replacement use cases, please contact Technical Support.

Note: If possible, transition to internal key management before performing the controller replacement. Transitioning to internal key management also generates a backup of the security key.

E5700-E2800 Dual controller replacement (controller hardware upgrade)

When performing a dual controller replacement, a copy of the original controller's firmware image is stored on the drives for reference. Unless you are also replacing the drives (or they are locked), the image on the drives can used to update the controllers and synchronize them with each other. The image is used when the controller board IDs are the same. When the controller board IDs are different, the dual controller swap will be treated like a hardware upgrade.

Completing E5700-E2800 controller replacement with secured drives and internal key management enabled

When performing a complete controller replacement (controller hardware upgrade) with secured drives and internal key management enabled, you must import the security key manually to unlock the drives. Once the drives are unlocked, the controller reboots to optimal to access the drives.

For more information on completing a controller replacement with secured drives and internal key management enabled, refer to *Controller swap with internal key management and one or more drives secured* on page 30.

Completing E5700-E2800 controller replacement with a mix of secured/ unsecured drives and internal key management

When performing a complete controller replacement (controller hardware upgrade) with a mix of secured and unsecured drives and internal key management enabled, you must first create an internal security key and then import the security key manually to unlock the secured drives. After the drives are unlocked, you can access the drives.

Attention: If you receive a seven-segment display lock-down code of `L5` after performing a controller replacement of mixed secured drives with internal key management, contact Technical Support.

For more information on completing a controller replacement with a mix of secured/unsecured drives and internal key management, see *Create internal security key* on page 29 and *Controller swap with internal key management and one or more drives secured* on page 30.

Completing E5700-E2800 controller replacement with secured drives and external key management

When performing a complete controller replacement (controller hardware upgrade) with secured drives and external key management enabled, you must reconfigure the external key management attributes/certificates to acquire the security key and unlocks the secured drives. Once the drives are unlocked, the controller reboots to optimal to access the drives.

For detailed information on completing a controller replacement with secured drives and external key management, refer to *Controller swap with external key management and all drives secured* on page 34.

Completing E5700-E2800 controller replacement with partially secured drives and external key management

When performing a complete controller replacement (controller hardware upgrade) with a mix of secured and unsecured drives and external key management enabled, the controllers automatically reconnect to the external key management service using the attributes/certificates stored on the unlocked drives; effectively unlocking the secured drives.

Attention: If you receive a seven-segment display lock-down code of `L5` after performing a controller replacement of mixed secured drives with external key management, contact Technical Support.

Cabling considerations for controller-drive tray hardware upgrades

Compare your current host cabling to the supported cabling for your new controllers to determine whether you can reuse SFPs, QSFPs or cables from your old cabling configuration. The HBAs, HCAs, or Ethernet adapters, as well as switches in the network fabric used to connect your hosts to your storage array must match the HICs in your controller canisters.

Supported cables for E5700 controller shelfs and EF570 flash arrays

HICs and Base Ports		Cable		
Data rate and protocol	**Number and type of connectors**	**Connector**	**Type**	**Length**
100 Gb/s, 56 Gb/s, or 40Gb/s Infiniband	2 HIC ports	QSFP+Twin-Ax	Passive copper	3m
		QSFP+	Optical	5-100m
32 Gb/s, 16 Gb/s, or 8 Gb/s Fibre Channel	4 HIC ports	SFP+	OM2 optical	2,3,5,10,25 m
			OM3 optical	50-100m
			OM4 optical	1,2,3,4,5m

HICs and Base Ports		**Cable**		
Data rate and protocol	**Number and type of connectors**	**Connector**	**Type**	**Length**
25 Gb/s, or 10 Gb/s iSCSI	4 HIC ports	SFP28	OM3 optical	1-30m
			OM4 optical	1,2,3,5,7m
		SFP28 with Twin-Ax	Passive copper	Up to 3m
		SFP+	OM2 optical	1-25m
			OM3 optical	25-300m
			OM4 optical	1,2,3,5,7m
		SFP+ Twin-Ax	Passive Copper	Up to 5m
12 Gb/s, 6 Gb/s, or 3 Gb/s SAS	4 HIC ports	MiniSAS-HD	Passive copper	1-5m
				2m
			Active optical	20-100m
		MiniSAS	Passive copper	1-5m
16 Gb/s, 8 Gb/s, or 4 Gb/s Fibre Channel	2 base ports	SFP+	OM2 SW optical	1,2,3,5,10,25m
			OMW3 SW optical	50-100m
			OM4 optical	1,2,3,4,5m
10 Gb/s or 1 Gb/s iSCSI	2 base ports	SFP+	OM2 optical	1,2,3,10,25m
			OM3 optical	25-300m
			OM4 optical	1,2,3,4,5m
		Twin-Ax (DAC)	Passive cooper	2-7m
1 Gb/s iSCSI	2 base ports	RJ-45	Cat6 passive copper	Up to 70m

Note: The E5700 controller shelf does not support bifurcated SAS cable configurations.

Supported cables for E5500 and E5600 controller-drive trays and the EF550 and EF560 flash arrays

HIC		Cable		
Data Rate and Protocol	**Number of Connectors**	**Connector**	**Type**	**Length**
12 Gb/s SAS	4	MiniSAS-HD	passive copper	1-5m
		MiniSAS-HD	active copper	8-15m
		MiniSAS-HD	optical	5-100m
		Fan-out cable type #2	passive copper	2m
		Fan-out cable type #3	passive copper	2m
6 Gb/s SAS	4	MiniSAS-HD	passive copper	1-10m
		MiniSAS-HD	active copper	5-20m
		Fan-out cable type #1	passive copper	2m
56 Gb/s InfiniBand[1]	2	QSFP+	passive copper	1-3m
		QSFP+	optical	5-100m
40 Gb/s InfiniBand[2]	2	QSFP+	passive copper	1-5m
		QSFP+	optical	10-300m
16 Gb/s Fibre Channel	4	SFP+	OM2 SW optical	2, 3, 5, 10, 25m
		SFP+	OM3 SW optical	50-150m
		SFP+	OS2 LW optical	50-300m
10 Gb/s iSCSI	4	SFP+	OM2 optical	2, 3, 5, 10, 25m
		SFP+	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
1 Gb/s iSCSI	4	SFP+[3]	OM2 optical	2, 3, 5, 10, 25m
		SFP+[3]	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
		RJ-45[4]	passive copper	2-70m

[1]This information applies to HICs with a maximum data rate of 56 Gb/s. These HICs can also be operated at 40 Gb/s.

[2]This information applies to HICs with a maximum data rate of 40 Gb/s. These HICs can also be operated at 20 Gb/s. These HICs can be used only in the E5500 and EF550 models.

[3]Optical cables for 1-Gb/s iSCSI connections require a 1-Gb/s SFP.

[4] Copper cables with RJ-45 connectors for iSCSI connections require an SFP adapter.

Supported cables for E2800 controller shelf

HICs and base ports		Cable		
Data rate and protocol	**Number and type of connectors**	**Connector**	**Type**	**Length**
12 Gb/s SAS or 6 Gb/s SAS	4 or 2 HIC ports	MiniSAS-HD	passive copper	1-5m
		MiniSAS-HD	optical	5-100m
		Fan-out cable type #3	passive copper	2m
6 Gb/s SAS only	4 or 2 HIC ports	Fan-out cable type #2	passive copper	2m
16 Gb/s, 8 Gb/s, or 4 Gb/s Fibre Channel	4 or 2 HIC optical ports	SFP+	OM2 SW optical	2,3,5,10,25 m
		SFP+	OM3 SW optical	50-100m
	2 base optical ports	SFP+	OM2 SW optical	2,3,5,10,25 m
		SFP+	OM3 SW optical	50-100m
		SFP+	OS1 LW optical	50-300m
10 Gb/s iSCSI or 1 Gb/s iSCSI	4 HIC optical ports	SFP+	OM2 optical	2,3,5,10,25 m
		SFP+	OM3 optical	50-300m
		Twin-Ax (DAC)	passive copper	2-7m
	2 base optical ports	SFP+	OM2 optical	2,3,5,10,25 m
		Twin-Ax (DAC)	passive copper	2-7m
	2 base RJ-45 ports	RJ-45	Cat6a passive copper	2-100m
	2 HIC optical ports	SFP+	OM2 optical	2,3,5,10,25 m
		SFP+	OM3 optical	50-300m
		Twin-Ax (DAC)	passive copper	2-7m
	2 HIC RJ-45 ports	RJ-45	Shielded Cat6a passive copper	2-100m
1 Gb/s iSCSI only	4 HIC optical ports	RJ-45 with 1 Gb/s SFP	Cat5 passive copper	2-100m
	2 HIC optical ports	RJ-45 with 1 Gb/s SFP	Cat5 passive copper	2-70m

Supported cables for E2700 controller-drive trays

HIC		Cable		
Data Rate and Protocol	**Number of Connectors**	**Connector**	**Type**	**Length**
12 Gb/s SAS	4	MiniSAS-HD	passive copper	1-5m
		MiniSAS-HD	active copper	8-15m
		MiniSAS-HD	optical	5-100m
	2	MiniSAS-HD	passive copper	1-5m
		MiniSAS-HD	active copper	8-15m
		MiniSAS-HD	optical	5-100m
	4	Fan-out cable type #2	passive copper	2m
		Fan-out cable type #3	passive copper	2m
16 Gb/s Fibre Channel	4	SFP+	OM2 SW optical	2,3,5,10,25 m
		SFP+	OM3 SW optical	50-150m
		SFP+	OS2 LW optical	50-300m
	2	SFP+	OM2 SW optical	2,3,5,10,25 m
		SFP+	OM3 SW optical	50-150m
		SFP+	OS2 LW optical	50-300m
10 Gb/s iSCSI	4	SFP+	OM2 optical	2,3,5,10,25 m
		SFP+	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
	2	SFP+	OM2 optical	2,3,5,10,25 m
		SFP+	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
		RJ-45	Cat6a passive copper	2-100m

HIC		**Cable**		
Data Rate and Protocol	**Number of Connectors**	**Connector**	**Type**	**Length**
1 Gb/s iSCSI	4	SFP+[1]	OM2 optical	2, 3, 5, 10, 25m
		SFP+[1]	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
		RJ-45[2]	passive copper	2-70m
	2	SFP+[1]	OM2 optical	2, 3, 5, 10, 25m
		SFP+[1]	OM3 optical	50-150m
		Twin-Ax	passive copper	2-7m
		RJ-45[2]	Cat5 passive copper	2-70m
		RJ-45	Cat6a passive copper	2-100m

[1]Optical cables for 1-Gb/s iSCSI connections require a 1-Gb/s SFP.

[2] Copper cables with RJ-45 connectors for iSCSI connections require an SFP adapter.

Related information

NetApp Hardware Universe

Items needed before upgrading or replacing controller canisters

Before upgrading or replacing a controller canister, make sure you have the appropriate accessories to complete the procedure.

To complete the upgrade or replacing a controller canister procedure, you will need antistatic protection and one or two new controller canisters. You might also need new controller batteries. If your new controller canisters do not have the same host interface cards as the controller canisters you are replacing, you might need new host bus adapters, cables and Small Form-factor Pluggable (SFP) transceivers to re-cable your host connections. If the new controller canisters support different drive cabling from the old controller canisters, you might also need different drive cables.

Preparing to replace the controllers

Before removing a controller canister, you must perform a number of steps in SANtricity Storage Manager to prepare your system. These steps include saving the drive security key, gathering support data, and taking the controller offline.

Steps

1. Make sure that the existing storage array is updated to the latest released operating system (controller firmware) version available for your current controllers.

   - If you are upgrading to controllers that support SANtricity OS version 8.40, you must download and install the latest versions of SANtricity OS and the latest NVSRAM after you install and power on the new controllers.

     Note: If you do not perform this upgrade, you might not be able to configure the storage array for Automatic Load Balancing (ALB). See the *E2700 and E5600 SANtricity Software and Firmware Upgrade Guide* for the procedure to install SANtricity OS and NVSRAM.

2. If performing a complete controller replacement when using drive security, complete the following steps:

Security type and context	Steps
Internal key management, one or more drives locked	**a.** Export the internal security key file to a known location on the management client (the system with a browser used for accessing System Manager). Use the `export storageArray securityKey` command. You must provide the pass phrase associated with the security key and specify the location where you want to save the command. For information about using this command, see the *Command Line Reference*. **b.** Know the pass phrase associated with the internal security key.

Security type and context	Steps
External key management, all drives locked, you are able to transition to internal key management temporarily for the controller replacement (recommended).	Perform the following steps, in order: **a.** Record the External KMS server address and port number using the **Settings >> System >> Security Key Management >> View/Edit Key Management Server Settings** dialog. **b.** Ensure that the client and server certificates are available on your local host so the storage array and key management server can authenticate each other after the controller replacement is finished. Use the `save storageArray keyManagementCertificate` command to save the certificates. Be sure the run the command twice, once with the `certificateType` parameter set to `client`, and the other with the parameter set to `server`. For information about using this command, see the *Command Line Reference*. **c.** Transition to internal key management by running the `disable storageArray externalKeyManagement` command. **d.** Export the internal security key file to a known location on the management client (the system with a browser used for accessing System Manager). Use the `export storageArray securityKey` command. You must provide the pass phrase associated with the security key and specify the location where you want to save the command. For information about using this command, see the *Command Line Reference*. **e.** Know the pass phrase associated with the internal security key.
External key management, all drives locked, you are not able to transition to internal key management temporarily for the controller replacement.	Perform the following steps, in order: **a.** Record the External KMS server address and port number using the **Settings >> System >> Security Key Management >> View/Edit Key Management Server Settings** dialog. **b.** Ensure that the client and server certificates are available on your local host so the storage array and key management server can authenticate each other after the controller replacement is finished. Use the `save storageArray keyManagementCertificate` command to save the certificates. Be sure the run the command twice, once with the `certificateType` parameter set to `client`, and the other with the parameter set to `server`. For information about using this command, see the *Command Line Reference*.
External key management, partial drives locked	No additional steps are necessary.

3. Record the serial number for your storage array:

a. In the **EMW** tree view, double-click your storage array.

The **System Manager** opens.

b. Select **Support > Support Center > Support Resources** tab.

c. Scroll down to **Launch detailed storage array information**, and then select **Storage Array Profile**.

The Report appears on your screen.

d. To locate the chassis serial number under the storage array profile, type **serial number** in the **Find** text box, and then click **Find**.

   All matching terms are highlighted. To scroll through all the results one at a time, continue to click **Find**.

e. Make a record of the `Chassis Serial Number`.

   You need this serial number to perform the steps in *Powering on the storage array.* on page 26

4. Gather support data about your storage array by using one of these methods:

- Use the storage management software to collect and save a support bundle of your storage array. From the Array Management Window toolbar, select **Monitor > Health > Collect Support Data Manually**. Then name and specify a location on your system where you want to store the support bundle.
- Use the command line interface (CLI) to run the `save storageArray supportData` command to gather comprehensive support data about the storage array. For more information about this command, refer to the current version of the *Command Line Interface and Script Commands Programming Guide*.

Note: Gathering support data can temporarily impact performance on your storage array.

5. Ensure that no I/O operations are occurring between the storage array and all connected hosts. For example, you can perform these steps:

- Stop all processes that involve the LUNs mapped from the storage to the hosts.
- Ensure that no applications are writing data to any LUNs mapped from the storage to the hosts.
- Unmount all file systems associated with volumes on the array.

Note: The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.

Attention: Possible data loss – If you continue this procedure while I/O operations are occurring, you might lose data.

6. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.

7. If you are using asynchronous mirroring or synchronous mirroring, perform the following to delete any mirrored pairs and deactivate any mirroring relationships:

Mirroring Relationship	Steps
Synchronous Mirroring (supported for Fibre Channel only)	**a.** In the Array Management Window, select **Help > Contents**, and search for the topics related to Synchronous Mirroring. **b.** Follow the guidelines and instructions in the online help to identify all synchronous mirroring volumes that might exist. **c.** In the Logical pane, right-click a synchronous mirroring volume, and select **Copy Services > Synchronous Mirroring > Remove Mirror Relationship**. **d.** Select all volumes, and click **Remove**. **e.** After you delete all mirroring relationships, deactivate Synchronous Mirroring by selecting **Copy Services > Mirroring > Deactivate**. **f.** Select the **synchronous mirroring** check box from the pop-up window. **Attention:** If you do not delete all mirroring relationships before deactivating mirroring, you receive an error.
Asynchronous Mirroring (supported for iSCSI and Fibre Channel only)	**a.** In the Array Management Window, access the online help and search for the topics related to Asynchronous Mirroring. **b.** Follow the instructions in the online help to remove all asynchronous mirrored pairs from the asynchronous mirror groups. **Note:** When removing each pair, select the **Delete all repositories associated with this mirrored pair** check box. **c.** Follow the instructions in the online help to delete all asynchronous mirror groups.

8. If there is a thin provisioned volume that is reported to the host as thin volume and the old array is running firmware (8.25 firmware or above) that supports UNMAP feature, disable Write Back Caching for all thin volumes:
   a. Select **Storage > Volumes**.
   b. Select any volume, and then select **More > Change cache settings**.

      The Change Cache Setting dialog box appears. All volumes on the storage array appear in this dialog box.
   c. Select the **Basic** tab to change the settings for read caching and write caching.
   d. Click **Save** to change the cache settings.
9. Wait five minutes to allow any data in cache memory to be flushed to disk.
10. From the **Home** page, select **View Operations in Progress**.
11. Wait for all operations shown on the **Operations in Progress** window to complete before continuing with the next step.
12. Turn off power to the controller-drive tray.
13. Wait for all of the LEDs on the controller-drive tray to go dark.
14. Turn off power to each drive tray that is connected to the controller-drive tray.
15. Wait two minutes for all of the drives to spin down.

Related tasks

Powering on the storage array on page 26

Removing controller canisters from a controller-drive tray

When you remove a controller canister, you must disconnect all cables and remove any SFP transceivers. Then, you can slide the controller canister out of the controller-drive tray.

About this task

Attention: Possible hardware damage – To prevent electrostatic discharge damage to the tray, use proper antistatic protection when handling tray components.

Steps

1. Put on antistatic protection.

   Attention: Potential degraded performance – To prevent degraded performance, do not twist, fold, pinch, or step on the cables. Many cables have a minimum bending radius. Check the specifications for your cables, and do not bend any cable tighter than the minimum specified radius.

2. Label each cable that is attached to the old controller canister. Depending on the HIC configuration, you might be able to reconnect some cables after you replace the controller canister.
3. Disconnect all of the interface and Ethernet cables from the old controller canister.

   If fiber-optic cables are present, you can use the two release levers to partially remove the controller canister. Opening these release levers makes it easier to press down the fiber-optic cable release tab.
4. If the old controller canister contains a Fibre Channel HIC or an InfiniBand HIC, remove the small form-factor pluggable (SFP+) transceivers (for Fibre Channel) or quad SFP (QSFP+) transceivers (for InfiniBand) from the HIC, and save them for possible reuse.
5. Remove controller A.
   a. Unlock and rotate the release handles out to release the controller canister.
   b. Using the release handles and your hands, pull the controller canister out of the controller-drive tray.
6. Set the old controller canister on a flat, static-free surface near the controller-drive tray with the release levers up. Position the controller canister so that you can access the top cover.
7. Choose one of the following options:
   - If you will reuse the battery from the old controller in the new controller, continue with step *8* on page 22.
   - If you will install a new battery in the new controller, go to step *11* on page 23.
8. Press down on both of the top cover latch buttons on the old controller canister, and slide the top cover to the rear of the canister.
9. Perform one of the following options, depending on your model of controller-drive tray, to release the old battery:
   - For the E2600 controller-drive tray or the E2700 controller-drive tray, unscrew the thumb screw that secures the battery to the controller canister.

- For the E5400 controller-drive tray, the EF540 controller-drive tray, the E5500 controller-drive tray, the EF550 controller-drive tray, the E5600 controller-drive tray, or the EF560 controller-drive tray, release the tab that secures the battery to the controller canister.

10. Remove the battery by sliding it towards the rear of the old controller canister.

11. For a duplex controller-drive tray, repeat step *2* on page 22 through step *10* on page 23 for the second controller canister.

Installing new controller canisters in the controller-drive tray

After you have removed the old controllers, you can install new controllers in the controller-drive tray.

About this task

Perform the following steps for each controller in the controller-drive tray.

Steps

1. Unpack a new controller canister.
   a. Set the new controller canister on a flat, static-free surface near the controller-drive tray with the top cover up.
   b. Save all of the packing materials so that you can, if necessary, ship the old controller canister.
2. Push down the two top cover latch buttons that secure the top cover to the new controller canister.
3. Remove the top cover by sliding it to the rear of the new controller canister.
4. Choose one of the following options:
   - If you are installing the battery in E2600 or E2700 controller-drive tray, go to step *9* on page 24.
   - If you are installing a battery on another model, continue with the next step.
5. Insert the battery (either the new battery that you ordered or the battery that you removed from the old controller canister) into the new controller canister. Slide the battery into the canister, making sure it stays below the rivets on the wall of the new canister.
6. Keeping the locking handle at a 45 degree angle, align the connectors at the bottom of the battery with the connectors on the canister.
7. Push the battery down until you hear it click, and move the locking handle up to secure the controller battery to the controller canister.

   Attention: To make sure that the controller battery is seated correctly in an E5XX controller-drive tray, you might need to slide it out and insert it again. You know it is secure when you hear it click into place, and when the locking handle does not move out of its upright position when you wiggle it.
8. Go to step *11* on page 24.
9. Insert the battery circuit board (either the new battery circuit board that you ordered or the battery circuit board that you removed from the old controller canister) by sliding it towards the front of the new controller canister.

   Note: To ensure that the battery is seated correctly in an E2600 controller-drive tray or an E2700 controller-drive tray, you might need to back it out of the connector to make sure that it is correctly aligned with the thumbscrew.
10. Tighten the thumbscrew to secure the battery circuit board in the new controller canister card.
11. Reinstall the top cover on the new controller canister by sliding it forward until the top latch covers click.

12. Slide the new controller canister all the way into the controller-drive tray. Rotate the release levers towards the center of the controller canister to lock it into place.

13. If your new controller canister has a Fibre Channel HIC or an InfiniBand HIC, install the SFP+ transceivers (Fibre Channel) or QSFP+ transceiver (InfiniBand) into the controller canister.

    Depending on the HICs involved in your upgrade, you might be able to reuse SFP+ transceiver or QSFP+ transceivers that you removed from your old controller canister. See *Cabling considerations for controller-drive tray hardware upgrades* on page 10 for details about cabling requirements.

14. Reconnect all of the cables between the controller-drive tray and the drive trays.

    Note: If you are upgrading to E2700 controllers from an earlier model, the drive cabling configuration might be different from the configuration used for the old controllers.

    If the drive cabling configuration is the same as it was with your old controllers, use the labels that you attached to the cables to reconnect the cables correctly.

Powering on the storage array

After replacing a controller canister, you must bring the controller online and confirm that the storage array is working correctly. Then, you can collect support data and resume operations.

About this task

If the controller upgrade involves a protocol change (for example, Fibre Channel to iSCSI), any host groups, hosts, and volume-to-LUN mappings defined in the host mappings tab remain intact. However, you must take steps to associate the new host ports with the hosts. If the controller upgrade does not involve a protocol change, all host port mappings will remain intact and no additional steps are required.

Steps

1. Turn on the Power switch on the rear of each drive tray that is connected to the controller-drive tray.
2. Wait two minutes for the drives to spin up.
3. Turn on the Power switch on the rear of the controller-drive tray.
4. Wait three minutes for the power-up process to complete.

   Note: For a controllers running SANtricity OS 8.20, you must reboot each controller through the SANtricity Storage Manager or command line interface (CLI) after powering on the storage array for the first time after performing a controller upgrade.

5. If you are performing a complete controller replacement for either E2800 or E5700 controllers, proceed to one of the following procedures based on your drive security scenario.

Complete controller replacement type	Procedure and prerequisites
All unsecured drives, neither External or Internal Key Management	Proceed to step 6.
Mix of secured and unsecured drives, Internal Key Management	You first must create an internal security key and then import the security key manually to unlock the secured drives. After the drives are unlocked, you can access the drives. **a.** *Create internal security key* on page 29 **b.** *Controller swap with internal key management and one or more drives secured* on page 30
All secured drives, Internal Key Management	*Controller swap with internal key management and one or more drives secured* on page 30
Mix of secured and unsecured drives, External Key Management	Proceed to step 6. **Attention:** After performing the controller replacement, the controllers will automatically resynchronize with the External Key Management Server and the drives will unlock and be accessible. **Note:** If you receive a seven-segment display lock-down code of `L5` after performing a controller replacement of mixed secured drives with internal key management, contact technical support.

Complete controller replacement type	Procedure and prerequisites
All secured drives, External Key Management, you have temporarily switched back to Internal Key Management for the controller replacement procedure	You must first unlock the secured drives using the Internal Key Management procedure. After the drives are unlocked, then you transition back to External Key Management by creating a new external security key for the storage array. **a.** *Controller swap with internal key management and one or more drives secured* on page 30 **b.** *Create an external security key* on page 32
All secured drives, External Key Management, you have not temporarily switched to Internal Key Management for the controller replacement procedure	*Controller swap with external key management and all drives secured* on page 34

After performing one of the appropriate procedures based on your controller replacement scenario, proceed to the following steps.

6. Look at the LEDs on controller A to make sure that it is booting correctly.

   The Host Link Service Action Required LEDs turn green during the reboot. The seven-segment display shows the sequence OS+ Sd+ blank- to indicate that the controller is performing Start-of-day (SOD) processing. After the controller successfully completes rebooting, the seven-segment display shows the tray ID matching the seven-segment display on the second controller. You can then discover the new controller canister by using the storage management software.

7. Perform these steps if any of the controller-drive tray's Service Action Required LEDs are *on*, or if the Controller Service Action Required LED is *on*:

   a. Check that the controller canister has been installed correctly and that all of the cables are correctly seated. Reinstall the controller canister, if necessary.

   b. Check the controller-drive tray's Service Action Required LEDs and the Controller Service Action Required LED again. If the problem is not corrected, contact technical support.

8. For a duplex configuration, repeat step 6 through step 7 for controller B.

9. Using the LEDs and the storage management software, check the status of all of the trays in the storage array.

Does any component have a Needs Attention status?	Procedure
Yes	Click the Recovery Guru toolbar button in the Array Management Window , and complete the recovery procedure. If the problem is not resolved, contact technical support.
No	Go to step *10* on page 27.

10. Remove the antistatic protection.

11. If you are upgrading to controllers that run SANtricity 11.40 and controller firmware 8.40, download and install the latest NVSRAM after you power on the new controllers. See the *E2700 and E5600 SANtricity Software and Firmware Upgrade Guide* for the procedure to install NVSRAM.

12. If your controller upgrade involves a protocol change (for example, Fibre Channel to iSCSI), and you already have hosts defined for your storage array, associate the new host ports with your hosts:

a. Within System Manager, select **Storage > Host**.

b. Select the host to which the ports will be associated, and then click **View/Edit Settings**.

   A dialog box appears that shows the current host settings.

c. Click the **Host Ports** tab.

   The dialog box shows the current host port identifiers.

d. To update the host port identifier information associated with each host, replace the host port IDs from the old host adapters with the new host port IDs for the new host adapter.

e. Repeat step d for each host.

f. Click **Save**.

13. Enable Write Back Caching for all thin volumes if it had been disabled in preparing for the headswap.

14. Gather support data about your updated storage array by using one of these methods:

- Use the storage management software to collect and save a support bundle of your storage array. From the System Manager, first select **Support > Support Center > Diagnostics** tab. Then select **Collect Support Data** and click **Collect**.
  The file is saved in the Downloads folder for your browser with the name `support-data.7z`.
  If your shelf contains drawers, the diagnostics data for that shelf is archived in a separate zipped file named `tray-componet-state-capture.7z`
- Use the CLI to run the `save storageArray supportData` command to gather comprehensive support data about the storage array.

Note: Gathering support data can temporarily impact performance on your storage array.

15. Open a non-technical case with NetApp technical support. This action alerts NetApp technical support to the changes that you made to the configuration of your storage array.

a. Get the serial number of the controller-drive tray that you recorded in *Preparing to replace the controllers* on page 17.

b. Go to the NetApp support site at *mysupport.netapp.com/eservice/assistant*.

c. If the **Login** page appears, enter your username and password, and select **Login**.

   The **Give Us Feedback** page opens.

d. Select **Product Registration** from the drop-down list under **Category 1**.

e. Enter the following text in the **Comments** text box, substituting the serial number of your controller-drive tray for *`serial number`*:

   `Please create alert against Serial Number: serial number. The alert name should be “E-Series Upgrade”. The alert text should read as follows:`

   `“Attention: The controllers in this system have been upgraded from the original configuration. Verify the controller configuration before ordering replacement controllers and notify dispatch that the system has been upgraded.”`

f. Click the **Submit** button at the bottom of the form.

Create internal security key

To use the Drive Security feature, you can create an internal security key that is shared by the controllers and secure-capable drives in the storage array. Internal keys are maintained on the controller's persistent memory.

Before you begin

- Secure-capable drives must be installed in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
- The Drive Security feature must be enabled. Otherwise, a Cannot Create Security Key dialog box opens during this task. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

Note: If both FDE and FIPS drives are installed in the storage array, they all share the same security key.

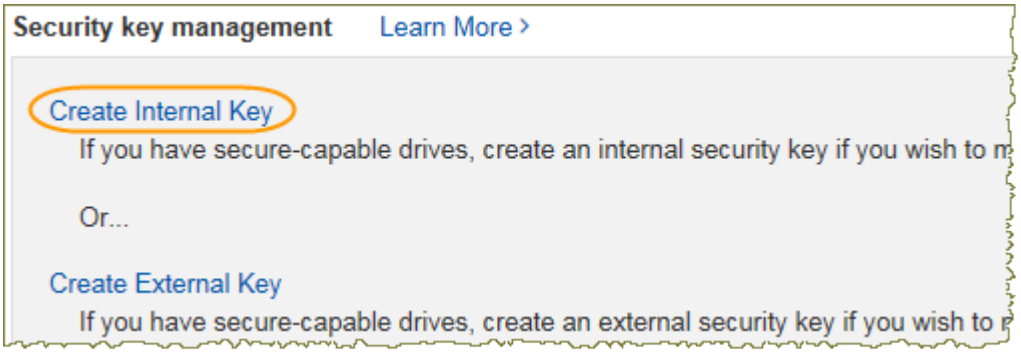
About this task

In this task, you define an identifier and a pass phrase to associate with the internal security key.

Note: The pass phrase for Drive Security is independent from the storage array's Administrator password.

Steps

1. Select **Settings** > **System**.
2. Under **Security key management**, select **Create Internal Key**.



If you have not yet generated a security key, the Create Security Key dialog box opens.

3. Enter information in the following fields:
   - **Define a security key identifier** – You can either accept the default value (storage array name and time stamp, which is generated by the controller firmware) or enter your own value. You can enter up to 189 alphanumeric characters without spaces, punctuation, or symbols.

     Note: Additional characters are generated automatically, appended to both ends of the string you enter. The generated characters ensure that the identifier is unique.

   - **Define a pass phrase/Re-enter pass phrase** – Enter and confirm a pass phrase. The value can have between 8 and 32 characters, and must include each of the following:
     - An uppercase letter (one or more). Keep in mind that the pass phrase is case sensitive.

- A number (one or more).
- A non-alphanumeric character, such as !, *, @ (one or more).

Important: Be sure to record your entries for later use. If you need to move a secure-enabled drive from the storage array, you must know the identifier and pass phrase to unlock drive data.

4. Click **Create**.

   The security key is stored on the controller in a non-accessible location. Along with the actual key, there is an encrypted key file that is downloaded from your browser.

   Note: The path for the downloaded file might depend on the default download location of your browser.

5. Record your key identifier, pass phrase, and the location of the downloaded key file, and then click **Close**.

Result

You can now create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

Note: Whenever power to the drives is turned off and then on again, all the secure-enabled drives change to a Security Locked state. In this state, the data is inaccessible until the controller applies the correct security key during drive initialization. If someone physically removes a locked drive and installs it in another system, the Security Locked state prevents unauthorized access to its data.

After you finish

You should validate the security key to make sure the key file is not corrupted.

Controller swap with internal key management and one or more drives secured

If you swap both controllers in a dual-controller system, or one controller in a simplex system, are using an internal security key, and one or more drives in the storage array are locked, you must import the appropriate security key to the new storage array. Importing the key allows you to unlock access to the drives.

Before you begin

Note: If you receive a seven-segment display lock-down code of `L5` after performing a controller replacement of mixed secured drives with internal key management, contact technical support.

- For the drives that are locked in the storage array, you must know the security key identifier and the pass phrase.

  Note: The pass phrase is not the same as the storage array's Administrator password.

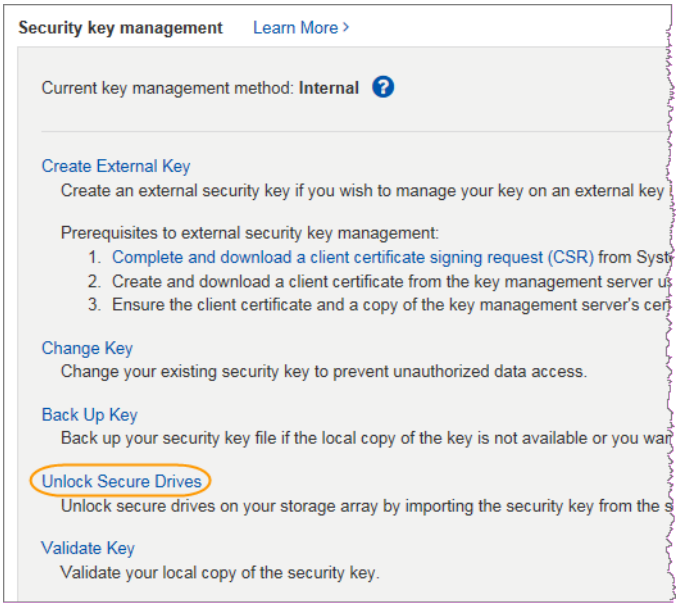
- The security key file is available on the management client (the system with a browser used for accessing System Manager).
- You must first create a new internal security key on the new replacement controllers before importing the original security key that was in place on the array prior to the controller replacement.

About this task

After the array discovers the drives, a `Needs Attention` condition appears along with a status of `Security Key Needed` for these re-located drives. You can unlock drive data by importing their security key into the storage array. During this process, you select the security key identifier from a drop-down list, and then enter the pass phrase for the key.

Steps

1. Import the security key that you saved in *Preparing to Replace the Controllers* on page 17 by selecting the **Storage Array** menu and then selecting **Security** > **Drive Security** > **Import Key**.
   - If there were only secured drives (no unsecured drives) in the storage array, the controllers automatically reboot to complete the import operation. Wait for all controllers to boot up. When a controller finishes booting, its icon appears in the Enterprise Management Window (EMW).
2. Select **Settings** > **System**.
3. Under **Security key management**, select **Unlock Secure Drives**.



   The Unlock Secure Drives dialog box opens.
4. From the drop-down list in the first field (click the arrow on the far right), select the security key identifier that is associated with the drives you want to unlock.

   When you select an identifier, the associated drive information appears below the field and the **Browse** button becomes available. The drives are identified by shelf number, drawer number, and bay number.
5. Click **Browse**, and then select the security key file that corresponds to the identifier.

   The key file you selected appears below the field.
6. Enter the pass phrase associated with this key file.

   The characters you enter are masked.
7. Click **Unlock**.

   If the unlock operation is successful, the dialog box displays the following message:

   `The associated secure drives have been unlocked.`

When all drives are locked and then unlocked, each controller in the storage array reboots. However, if there are already some unlocked drives in the target storage array, then the controllers will not reboot.

8. If the storage array began with a mix of secured and unsecured drives, set the formerly secured drives to a native state:

   a. Run the `set drives=( trayID1,[drawerID1,]slotID1 ... trayIDn, [drawerIDn,]slotIDn) nativeState` SMcli command.

      The drive you specify are the drives that were secured when you began the controller replacement.

   b. Reset all controllers using SANtricity System Manager.

   c. Wait for all controllers to boot up. When a controller has finished booting, it appears in the EMW.

Create external security key

To use the Drive Security feature with a key management server, you must create an external key that is shared by the key management server and the secure-capable drives in the storage array.

Before you begin

- Secure-capable drives must be installed in the array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

  Note: If both FDE and FIPS drives are installed in the storage array, they all share the same security key.

- The Drive Security feature must be enabled. Otherwise, a Cannot Create Security Key dialog box opens during this task. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.
- The client and server certificates are available on your local host so the storage array and key management server can authenticate each other. The client certificate validates the controllers, while the server certificate validates the key management server.

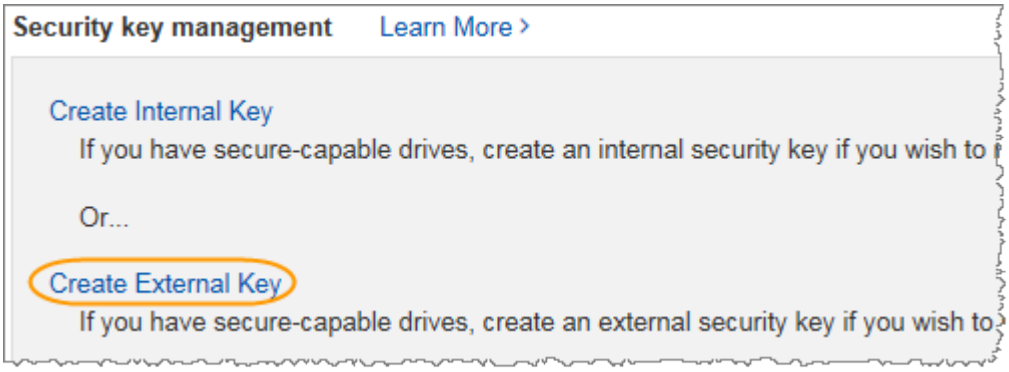
About this task

In this task, you define the IP address of the key management server and the port number it uses, and then load certificates for external key management.

Steps

1. Select **Settings > System**.
2. Under **Security key management**, select **Create External Key**.

   Note: If internal key management is currently configured, a dialog box opens and asks you to confirm that you want to switch to external key management.



The Create External Security Key dialog box opens.

3. Under **Connect to Key Server**, enter information in the following fields:
   - **Key management server address** – Enter the fully qualified domain name or the IP address (IPv4 or IPv6) of the server used for key management.
   - **Key management port number** – Enter the port number used for the Key Management Interoperability Protocol (KMIP) communications. The most common port number used for key management server communications is 5696.
   - **Select client certificate** – Click the first **Browse** button to select the certificate file for the storage array's controllers.
   - **Select key management server's server certificate** – Click the second **Browse** button to select the certificate file for the key management server.
4. Click **Next**.
5. Under **Create/Backup Key**, enter information in the following field:
   - **Define a pass phrase/Re-enter pass phrase** – Enter and confirm a pass phrase. The value can have between 8 and 32 characters, and must include each of the following:
     - An uppercase letter (one or more). Keep in mind that the pass phrase is case sensitive.
     - A number (one or more).
     - A non-alphanumeric character, such as !, *, @ (one or more).

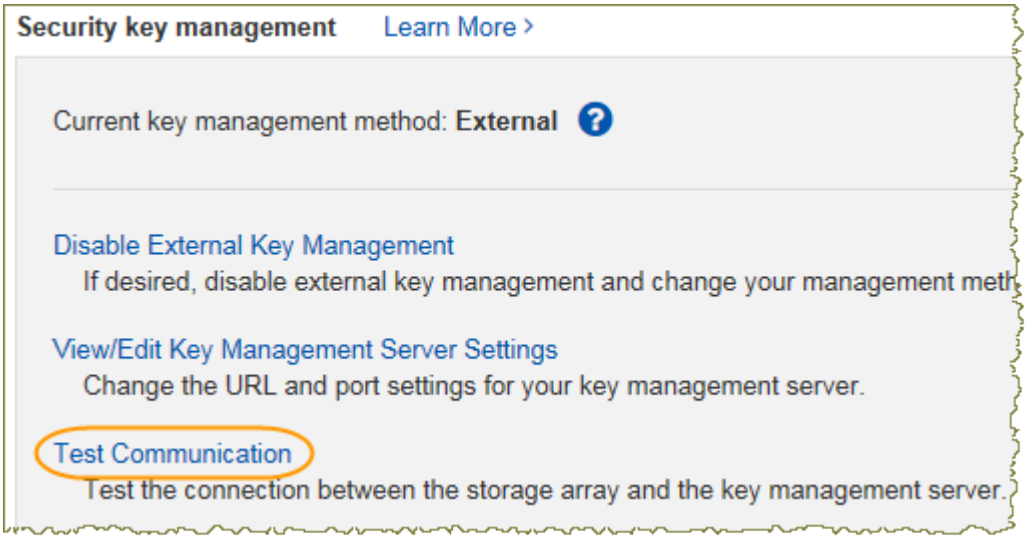
   Important: Be sure to record your entries for later use. If you need to move a secure-enabled drive from the storage array, you must know the pass phrase to unlock drive data.
6. Click **Finish**.

   The system connects to the key management server with the credentials you entered. A copy of the security key is then stored on your local system.

   Note: The path for the downloaded file might depend on the default download location of your browser.
7. Record your pass phrase and the location of the downloaded key file, and then click **Close**.

   The page displays the following message with additional links for external key management:

   `Current key management method: External`
8. Test the connection between the storage array and the key management server by selecting **Test Communication**.



Test results display in the dialog box.

Result

When external key management is enabled, you can create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

Note: Whenever power to the drives is turned off and then on again, all the secure-enabled drives change to a Security Locked state. In this state, the data is inaccessible until the controller applies the correct security key during drive initialization. If someone physically removes a locked drive and installs it in another system, the Security Locked state prevents unauthorized access to its data.

After you finish

- You should validate the security key to make sure the key file is not corrupted.

Controller swap with external key management and all drives secured

If you swap both controllers in a dual-controller system, or one controller in a simplex system, are using an external security key, and all drives in the storage array are locked, you must reestablish communication with the external key management server to unlock access to the drives.

Before you begin

- Both the External KMS and the controller are on the same subnet.
- You recorded the External KMS server address and port number in *Preparing to Replace the Controllers* on page 17.
- You retrieved the client and server certificates and stored them on your local host in *Preparing to Replace the Controllers* on page 17. These certificates are needed so the storage array and key management server can authenticate each other. The client certificate validates the controllers, while the server certificate validates the key management server.
- You know the pass phrase associated with the external security key.

Steps

1. Select **Settings** > **System**.

2. Under **Connect to Key Server**, enter information in the following fields:
   - **Key management server address** – Enter the fully qualified domain name or the IP address (IPv4 or IPv6) of the server used for key management.
   - **Key management port number** – Enter the port number used for the Key Management Interoperability Protocol (KMIP) communications. The most common port number used for key management server communications is 5696.
   - **Select client certificate** – Click the first **Browse** button to select the certificate file for the storage array's controllers.
   - **Select key management server's server certificate** – Click the second **Browse** button to select the certificate file for the key management server.
3. Click **Next**.
4. Click **Finish**.

   The system connects to the key management server with the credentials you entered. A copy of the security key is then stored on your local system.

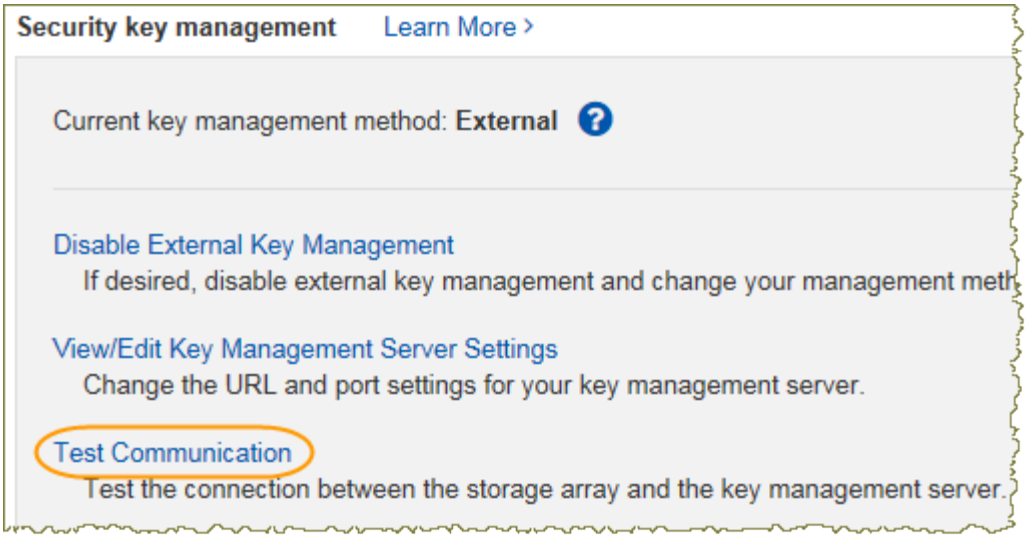
   Note: The path for the downloaded file might depend on the default download location of your browser.

5. Record the location of the downloaded key file, and then click **Close**.

   The page displays the following message with additional links for external key management:

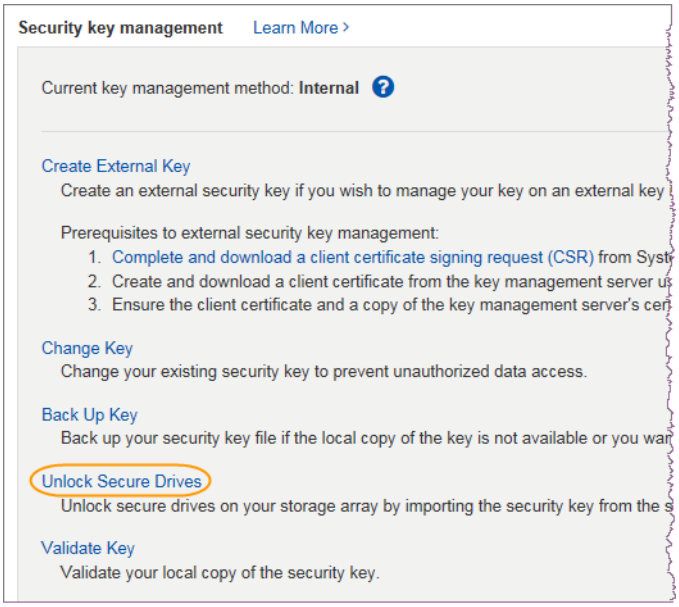
   `Current key management method: External`

6. Test the connection between the storage array and the key management server by selecting **Test Communication**.



   Test results display in the dialog box.

7. Select **Settings > System**.
8. Under **Security key management**, select **Unlock Secure Drives**.



The Unlock Secure Drives dialog box opens.

9. From the drop-down list in the first field (click the arrow on the far right), select the security key identifier that is associated with the drives you want to unlock.

   When you select an identifier, the associated drive information appears below the field and the **Browse** button becomes available. The drives are identified by shelf number, drawer number, and bay number.

10. Click **Browse**, and then select the security key file that corresponds to the identifier.

    The key file you selected appears below the field.

11. Enter the pass phrase associated with this key file.

    The characters you enter are masked.

12. Click **Unlock**.

    If the unlock operation is successful, the dialog box displays: "The associated secure drives have been unlocked."

Result

When all drives are locked and then unlocked, each controller in the storage array will reboot. However, if there are already some unlocked drives in the target storage array, then the controllers will not reboot.

Remounting volumes after changing the vendor from LSI to NETAPP

If your controller upgrade results in changing the vendor ID from LSI to NETAPP, you must take steps on each Windows, VMware or AIX host that uses volumes from the updated storage array. Refer to the task for the corresponding operating system on each host.

Remounting volumes on a Windows host

These steps enable attached hosts can perform I/O operations with volumes on the upgraded storage array.

Steps

1. In the **Device Manager**, select **Show Hidden Devices**.
2. For each NETAPP SCSI Disk Device listed in the **Device Manager**, right-click on the entry, and select **Uninstall**.

   If Windows displays a dialog box with a message indicating that you should reboot the host, finish uninstalling all of the volumes before you scan for hardware and reboot.
3. Right-click in the **Device Manager**, and select **Scan for Hardware Changes**.
4. Reboot the host.

Remounting volumes on an AIX host

After you replace the controllers, you might observer that host shows the new volumes on the storage array, but also shows the original volumes as failed.

About this task

If failed volumes appear, perform the following steps.

Step

1. Run the `cfgmgr` command.

Remounting volumes on a VMware host

Address problems that might appear on VMware hosts after the controller upgrade.

About this task

After you replace the controllers, you might observe the following conditions:

- VMware shows new paths for the volumes on the storage array, but also shows the original paths as dead paths.
- The hosts still list the volumes on the storage array as having LSI vendor IDs. This might occur when the volumes were claimed by the LSI rule at the start and so continue to use the same LSI rule when the volumes come back on line.

- The Display Name does not reflect the change from LSI to NetApp. This might occur because the display name became free test after initial discovery. In this case, you can change the Display Name manually.

If dead paths appear, perform the following steps.

Steps

1. Perform a rescan on the each host.
2. Halt all host I/O operations to this subsystem.
3. Reclaim the volumes under NetApp rule.
   a. Run the `esxcli storage core device list` command. Check the output from the command to identify volumes whose names have the form `aa.xxxx`.
   b. Run the command `do esxcli storage core claiming reclaim -d naa.xxxxx` to change the LSI vendor ID to NetApp.

Reconfiguring a SAS-2 system for use behind a new SAS-3 controller shelf (E57XX/EF570/E28XX)

You can convert the controller shelf in an approved SAS-2 array (E2700, E5500/EF550, E5600/EF560) to a drive shelf and then place that shelf and any associated approved SAS-2 expansion shelves (DE1600, DE5600, DE6600) behind a new approved SAS-3 array (E2800, E5700/EF570) and approved SAS-3 expansion shelves (DE212C, DE224C, DE460C) for maximum performance and investment protection.

About this task

Due to the complexity of this procedure, the following is recommended:

- If you are able to back up your data, you can perform this procedure without assistance from NetApp Professional Services.
- If you cannot back up your data, contact NetApp Professional Services for assistance with this procedure.

Note: If you do not need to preserve any data through this procedure, refer to *Reconfiguring a SAS-2 system for use behind a new SAS-3 controller shelf without data preservation* on page 40.

Steps

1. Make sure both of your arrays are prepared for the procedure:

Arrays	Description
Existing array	Existing array with SANtricity OS 8.25 or later that is powered up.
New array	New array unpacked and powered down.

2. Record the serial number from the SAS-2 controller shelf that you will be converting to a drive shelf.
3. If drive security is in use for the existing array, ensure that the security key is available.
4. Shut down all applications that are using the data volumes, and remove the host cables from both controllers.
5. On controllers with a Cache Active LED, wait until the LED goes dark on both controllers. Otherwise, wait 15 minutes to allow controller cache to flush.
6. Ensure that no background operations are in progress using the following CLI command:

   ```
   Show StorageArray longRunningOperations
   ```

7. Power down both controllers.
8. Remove the network cables from both controllers as well as any enclosure expansion cables.
9. Replace both controllers in the existing array with IOMs or ESMs.
10. If the new array has any drives, perform the following to remove the drives:

Enclosure	Drive removal method
DE460	Remove the drives completely out of the enclosures.
Non-DE460	Partially remove the drives from the enclosures, making sure that the drives are no longer connected to the mid-plane .

11. If possible, use the host cables and network cables from the existing array and connect them to the controllers in the new array.

    Note: Depending on the host connections of your net array, different cables may be required.

12. Cable the drive shelves behind the controllers in the new array.

    The existing array becomes a drive shelf and can be cabled to the controllers in the new array.

    Note: Connecting SAS-2 to SAS-3 requires SAS HD to miniSAS cables. For more detailed cabling information for your particular controller and expansion shelf configuration, refer to the *E-Series Hardware Cabling Guide*.

13. Power up the new array.

14. Configure the management port and the IP addresses by installing the Quick Connect utility from the *NetApp Support Site*.

15. If drive security was in use on the existing array, import the security key. For more information on how to perform this task refer to *Import storage array security key* on page 31.

16. Download the latest NVSRAM for SANtricity 11.40 (or newer) on the new array.

17. Reinsert all the drives into the new array's enclosure(s).

18. Send your configuration changes to NetApp Technical Support.

    a. Get the serial number of the old controller-drive tray that you recorded in Step 2.

    b. Log in to the NetApp Support Site: `mysupport.netapp.com/eservice/assistant`.

    c. From the drop-down list under **Category 1** on the **Give Us Feedback** page, select **Installed products**.

    d. From the drop-down list under **Category 2** on the **Give Us Feedback** page, select **Decommission request**.

    e. Enter the following text in the **Comments** text box, substituting the serial number of your controller-drive tray for *`serial number`*:

    ```
    Please decommission this serial number as the entitlement has been
    moved to another serial number in the system. Please reference this in
    the SN notes.
    ```

    f. Select **Submit**.

Reconfiguring a SAS-2 system for use behind a new SAS-3 controller shelf without data preservation

You can convert the controller shelf in an approved SAS-2 array (E2700, E550/EF5500, E5600/EF560) to a drive shelf and then place that shelf and any associated approved SAS-2 drive shelves (DE1600, DE5600, DE6600) behind a new approved SAS-3 array (E2800, E5700/EF570) and approved SAS-3 drive shelves (DE212C, DE224C, DE460C) without data preservation.

Steps

1. If the existing SAS-2 array is still accessible, delete all volume groups, power down both controllers, and remove all cables.

2. Record the serial number from the SAS-2 controller shelf that you will be converting to a drive shelf.

3. If drive security is in use for the existing array, ensure that the security key is available.
4. Replace both controllers in the existing array with IOMs or ESMs.
5. If possible, use the host cables and network cables from the existing array and connect them to the controllers in the new array.

   Note: Depending on the host connections of your new array, different cables may be required.

6. Cable the drive shelves behind the controllers in the new array.

   The existing controller-drive tray and any attached drive trays become drive shelves and can be cabled to the controllers in the new array.

   Note: Connecting SAS-2 to SAS-3 requires SAS HD to miniSAS cables. For more detailed cabling information for your particular controller and expansion shelf configuration, refer to the *E-Series Hardware Cabling Guide*.

7. Power up the new array including any attached drive shelves.
8. Configure the management port and the IP addresses by installing the Quick Connect utility from the *NetApp Support Site*.
9. If drive security was in use on the existing array, import the security key. For more information on how to perform this task refer to *Import storage array security key* on page 31.
10. If you were unable to delete the volume groups from your existing array before performing this procedure, you must set all foreign drives to appear as native. For detailed information on how to set drives to native, refer to the SANtricity Online Help.
11. Send your configuration changes to NetApp Technical Support.

    a. Get the serial number of the old controller-drive tray that you recorded in Step 2.

    b. Log in to the NetApp Support Site: `mysupport.netapp.com/eservice/assistant`.

    c. From the drop-down list under **Category 1** on the **Give Us Feedback** page, select **Installed products**.

    d. From the drop-down list under **Category 2** on the **Give Us Feedback** page, select **Decommission request**.

    e. Enter the following text in the **Comments** text box, substituting the serial number of your controller-drive tray for *`serial number`*:

       If you are unable to delete the volume groups from your existing ARRAY BEFORE PERFOMRING THIS PROCEDURE, you must set all foreign drives appear to native.

       ```
       Please decommission this serial number as the entitlement has been
       moved to another serial number in the system. Please reference this in
       the SN notes.
       ```

    f. Select **Submit**.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277