Controllers

E-Series Systems

NetApp
May 25, 2022

Table of Contents

Controllers

Upgrade controllers overview

You can upgrade your storage array through the replacement of existing controllers.

Controller components

A controller consists of a board, firmware, and software. It controls the drives, and also implements the management software functions.

When to use this procedure

You typically use this procedure when you want to upgrade all controllers to a different model or platform. This procedure involves replacing all controllers in a controller-drive tray.

You might also use this procedure 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.

> The HIC upgrade scenarios are not covered within this procedure. Instead, refer to the HIC add, upgrade and replacement procedures for your E-Series system.

Upgrade considerations

Before you upgrade controllers, review the following considerations.

Hardware and firmware requirements

- **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.

- **Trays and shelves**

  Storage arrays with an E2800 or E5700 controller shelf are typically managed with the SANtricity System Manager user interface. You might also use the SANtricity Storage Manager interface to manage E2800 or E5700 controller shelves. All other controller-drive trays referenced in this procedure use SANtricity Storage Manager.

- **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.

- **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 upgrade procedure.

- **Synchronous Mirroring and Asynchronous Mirroring**

  If your storage array participates in Synchronous Mirroring, only iSCSI or Fibre Channel connections are supported between the primary site and the remote site. If the host interface card (HIC) configuration in your new controllers does not include iSCSI or Fibre Channel connections, Synchronous 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.

- **Storage object limits**

  If you change your controllers from 5x00 models to 2x00 models, your new storage array configuration will support lower numbers of some storage 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 storage object limits. See Hardware Universe for more information.

Upgrade to newer models

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 Snapshots 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 the updated Snapshots feature. 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.

Upgrade compatibility

Review the supported upgrade paths for each storage array model.

From E2x00 to E2x00

- **Battery**: Reuse the old battery.
- **Vendor ID**: Additional steps required.
- **Feature support**: Legacy snapshots are not supported on the E2700.
- **SAS-2 shelves**: E2800 controllers must not be placed into SAS-2 shelves.

From E2x00 to E5x00

- **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 remote volume mirroring (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.
  - E5700 controllers must not be placed into SAS-2 shelves.
- **SAS-3 shelves**: E5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.

From E5x00 to E2x00

- **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.
- **SAS-3 shelves**: E5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.

From E5x00 to E5x00

- **Battery**: Reuse the old battery.
- **Vendor ID**: Additional steps required when upgrading from E5400 to E5500 or E5600.
- **Feature support**:
  - Legacy snapshots are not supported on the E5500 or E5600.
  - Legacy remote volume mirroring (RVM) is not supported on the E5400 or E5500 with iSCSI HICs.
  - Data Assurance is not supported on the E5400 or E5500 with iSCSI HICs.
  - E5700 controllers must not be placed into SAS-2 shelves.
- **SAS-3 shelves**: E5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.

From EF5x0 to EF5x0

- **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.
  - EF570 controllers must not be placed into SAS-3 shelves.
- **SAS-3 shelves**: EF540, EF550, and EF560 controllers must not be placed into SAS-3 shelves.

SAS enclosures

The E5700 supports DE5600 and DE6600 SAS-2 enclosures via head upgrade. When a E5700 controller is installed in SAS-2 enclosures, support for base host ports is disabled.

SAS-2 shelves	SAS-3 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: • E2800 controller shelves • E5700 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).

This procedure requires a Feature Product Variance Request (FPVR). To file an FPVR, contact your sales team.

Prepare to upgrade controllers

Prepare to upgrade controllers by saving the Drive Security key (if used), recording the serial number, gathering support data, disabling certain features (if used), and taking the controller offline.

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

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. From SANtricity System Manager, go to **Support › Upgrade Center** to view your software and firmware inventory.

   If you are upgrading to controllers that support SANtricity OS version 8.50, you must install the latest versions of SANtricity OS and the latest NVSRAM after you install and power on the new controllers. If you do not perform this upgrade, you might not be able to configure the storage array for Automatic Load Balancing (ALB).

2. If you are performing a complete controller replacement and are also using the Drive Security feature, complete the appropriate steps for your security type (internal or external) and drive state in the following table.

   Drive Security is a storage array feature that provides an extra layer of security with either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. When these drives are used with the Drive Security feature, they require a security key for access to their data.

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` CLI 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.
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. From System Manager, go to **Settings › System › Security Key Management › View/Edit Key Management Server Settings**. 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` CLI command to save the certificates. Be sure to 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` CLI 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` CLI 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.

Security type and context	Steps
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. From System Manager, go to **Settings › System › Security Key Management › View/Edit Key Management Server Settings**. 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` CLI command to save the certificates. Be sure to 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.

Your storage array must be in an optimal state to retrieve client and server certificates. If the certificates are not retrievable, then a new CSR must be created and signed and the server certificate downloaded from the EKMS.

1. Record the serial number for your storage array:
   a. From System Manager, select **Support › Support Center › Support Resources tab**.
   b. Scroll down to **Launch detailed storage array information**, and then select **Storage Array Profile**.

      The Report appears on your screen.

   c. 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**.

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

      You need this serial number to perform the steps in Complete controller upgrade.

2. Gather support data about your storage array by using either the GUI or the CLI:
   - Use either System Manager or the Array Management Window in Storage Manager to collect and save a support bundle of your storage array.
     - From System Manager, select **Support › Support Center › Diagnostics tab**. Then select **Collect Support Data** and click **Collect**.
     - From the Array Management Window toolbar, select **Monitor › Health › Collect Support Data**

Manually. Then enter a name and specify a location on your system where you want to store the support bundle.

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-component-state-capture.7z`.

- Use the CLI to run the `save storageArray supportData` command to gather comprehensive support data about the storage array.

3. Ensure that no I/O operations are occurring between the storage array and all connected hosts:
   a. Stop all processes that involve the LUNs mapped from the storage to the hosts.
   b. Ensure that no applications are writing data to any LUNs mapped from the storage to the hosts.
   c. Unmount all file systems associated with volumes on the array.

> 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.

> **Possible data loss** — If you continue this procedure while I/O operations are occurring, you might lose data.

4. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
5. If you are using asynchronous or synchronous mirroring, delete any mirrored pairs and deactivate any mirroring relationships through the System Manager or the Array Management window.
6. If there is a thin provisioned volume that is reported to the host as a thin volume and the old array is running firmware (8.25 firmware or above) that supports the UNMAP feature, disable Write Back Caching for all thin volumes:
   a. From System Manager, 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 and change the settings for read caching and write caching.
   d. Click **Save**.
   e. Wait five minutes to allow any data in cache memory to be flushed to disk.
7. If the Security Assertion Markup Language (SAML) is enabled on the controller, contact technical support to disable the SAML authentication.

> After SAML is enabled, you cannot disable it through the SANtricity System Manager interface. To disable the SAML configuration, contact technical support for assistance.

8. Wait for all operations in progress to complete before continuing to the next step.
   a. From System Manager's **Home** page, select **View Operations in Progress**.

b. Make sure all operations shown on the **Operations in Progress** window are complete before continuing.

9. Turn off power to the controller-drive tray.

   Wait for all of the LEDs on the controller-drive tray to go dark.

10. Turn off power to each drive tray that is connected to the controller-drive tray.

    Wait two minutes for all of the drives to spin down.

What's next?

Go to Remove controllers.

Remove controllers

After preparing for the upgrade, you can remove the controllers, and if necessary, remove the battery.

Step 1: Remove controller

Remove the controller canister so you can upgrade it with a new one. You must disconnect all cables and remove any SFP transceivers. Then, you can slide the controller canister out of the controller shelf.

What you'll need

- An ESD wristband or take other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.

About this task

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

If you are upgrading controllers in a duplex controller-drive tray, repeat all steps to remove the second controller canister.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
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.

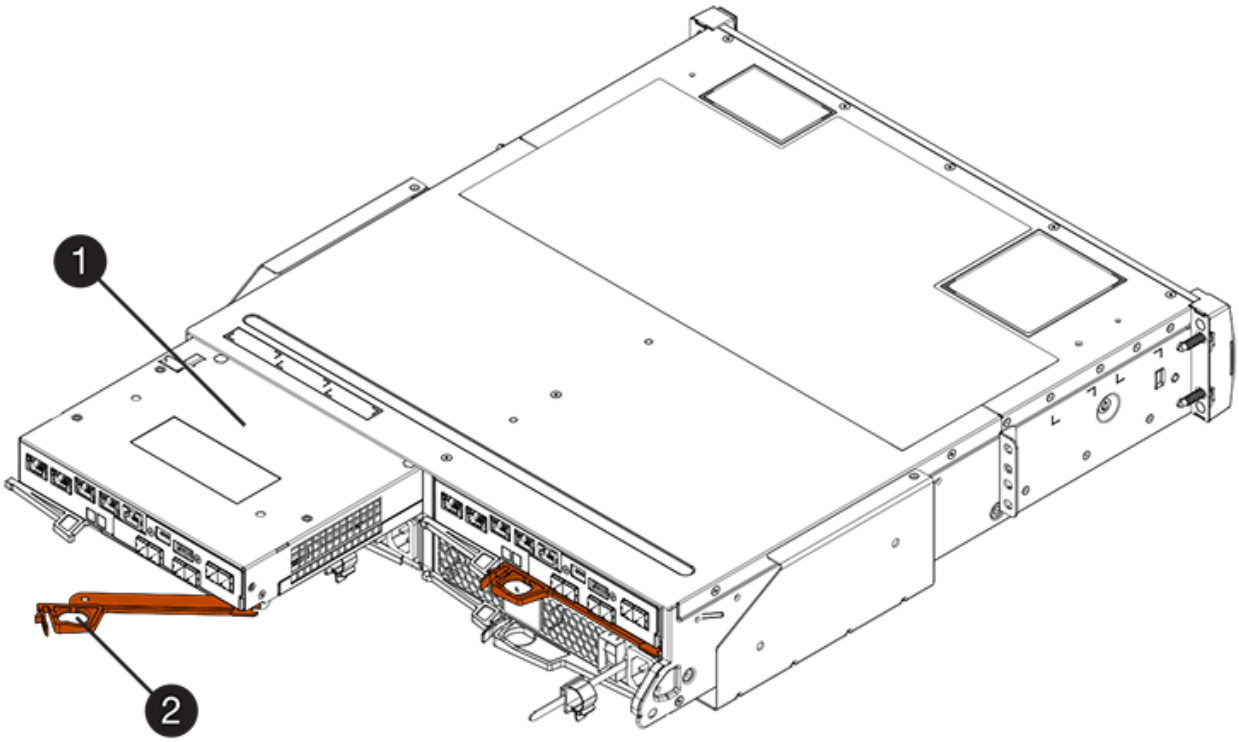
   

   To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

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.

The following figure is an example of the general location for the release handles on controller models. Controller shelves and controller-drive trays have a similar configuration for the release handles.



(1) *Controller canister*

(2) *Cam handle*

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. (Conditional) If you are upgrading controllers in a duplex controller-drive tray, repeat all steps to remove the second controller canister.

If you intend to use the battery from the old controller in the new controller, go to the next part of the section; otherwise go to Install new controllers.

Step 2: Remove battery

Remove the battery only if you intend to use the battery from the old controller canister in the new controller canister.

Steps

1. 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.
2. Perform one of the following options, depending on your model of controller-drive tray, to release the old battery:
   - For the E2600 or the E2700 controller-drive tray, unscrew the thumb screw that secures the battery to

the controller canister.

- For the E5400, EF540, E5500, EF550, E5600, or EF600 controller-drive tray, release the tab that secures the battery to the controller canister.

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

What's next?

Go to Install new controllers.

Install new controllers

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. If you are upgrading controllers in a duplex controller-drive tray, repeat all steps to install the second controller canister.

What you'll need

- An ESD wristband or take other antistatic precautions.
- A battery from the original controller canister or a new battery that you ordered.
- The new controller canister.

Step 1: Install battery

Install the battery that you removed from the original controller canister or a new battery that you ordered.

Steps

1. Unpack the new controller canister, and set it on a flat, static-free surface so that the removable cover faces up.
2. Press down on the cover button, and slide the cover off.
3. Orient the controller canister so that the slot for the battery faces toward you.
4. Depending on your controller model, do one of the following:
   - For E2600 or E2700 controller models:
     a. Insert the battery circuit board by sliding it towards the front of the new controller canister.
     b. Tighten the thumbscrew to secure the battery circuit board in the new controller canister card.
     c. Reinstall the top cover on the new controller canister by sliding it forward until the top latch covers click.

        When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

   - For other controller models:
     a. Insert the battery 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.

     b. Keeping the locking handle at a 45-degree angle, align the connectors at the bottom of the battery

with the connectors on the canister.

c. Push the battery down until you hear it click, and move the locking handle up to secure the controller battery to the controller canister.

> 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. 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.

d. Reinstall the top cover on the new controller canister by sliding it forward until the top latch covers click.

   When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

5. Turn the controller canister over to confirm that the battery is installed correctly.

Step 2: Install new controller canister

Install the new controller canister into the controller shelf.

Steps

1. 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.
2. 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 and reconnect the host cables.

   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.

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

   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.

> 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.

What's next?

If you are upgrading E2800 and E5700 controllers and the Drive Security feature is enabled, go to Unlock drives. Otherwise, go to Complete controller upgrade.

Unlock drives

If you are upgrading E2800 and E5700 controllers, the Drive Security feature for these controllers result in the locking of drives whether partially, externally, or internally. If the Drive Security feature is enabled, you must manually unlock these drives.

Follow the appropriate procedure for:

- Internal key management
- External key management

Internal key management

Follow these steps for internal key management when all drives are locked.

About this task

The newly swapped controllers will lock down with seven-segment display code of L5. This lock down occurs when no drives in the storage array are able to perform autocode synchronization (ACS). ACS resumes and updates the new controllers after the security key is imported.

> If you are not using management port 1, try with other default IP addresses:
> Ctrl A port 1: 192.168.128.101
> Ctrl A port 2: 192.168.128.102
> Ctrl B port 1: 192.168.129.101
> Ctrl B port 2: 192.168.129.102

Steps

1. Install the SANtricity client to a laptop or PC to be used in step 2 to connect directly to the array controller.
2. Connect the laptop or PC to controller A management port 1 directly via an RJ45 ethernet cable. This step might also require the laptop IP address be set to the same subnet.
3. Using the IP address 192.168.128.101 with username **admin** and the password blank, import the internal key using the `import storageArray securityKey file` CLI command, with the security key saved from Prepare to upgrade controllers. For information about using this command, see the *Command Line Reference*.

   Example: `SMcli 192.168.128.101 -u admin -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

Controllers will continue with the autocode synchronization process from the drives and reboot. After reboot the controllers will be accessible through the original IP configuration.

External key management

Follow these steps for external key management when all drives are locked.

About this task

The newly swapped controllers will lock down with seven-segment display code of L5. This lock down occurs when no drives in the storage array are able to perform autocode synchronization (ACS). ACS resumes and updates the new controllers after the security key is imported.

> Your storage array must be in an optimal state to retrieve client and server certificates. If the certificates are not retrievable, then a new CSR must be created and signed and the server certificate downloaded from the EKMS.

Steps

1. Install the SANtricity client to a laptop or PC to be used in step 2 to connect directly to the array controller.
2. Connect the laptop or PC to controller A management port 1 directly via an RJ45 ethernet cable. You might also need to set the laptop IP address to the same subnet.

3. Using default IP address 192.168.128.101 with username **admin** and the password blank, set up the external key management server using the `set storageArray externalKeyManagement` CLI command and provide the `serverAddress` and `serverPort` saved from Prepare to upgrade controllers. For information about using this command, see the *Command Line Reference*.

   Example: `SMcli 192.168.128.101 -u admin -c "set storageArray externalKeyManagement serverAddress=<ServerIPAddress> serverPort=<serverPort>;"`

4. Using the default IP address 192.168.128.101 with the username **admin** and the password remaining blank, download the certificates using the `storageArray keyManagementCertificate` CLI command: once for the client certificate and a second time for the server certificate. For information about using this command, see the *Command Line Reference*.

   Example A: `SMcli 192.168.128.101 -u admin -c "download storageArray keyManagementCertificate certificateType=client file=\"Directory&FileName\";"`

   Example B: `SMcli 192.168.128.101 -u admin -c "download storageArray keyManagementCertificate certificateType=server file=\"Directory&FileName\";"`

5. Using the security key saved from Prepare to upgrade controllers, import the external key to IP address 192.168.128.101 with the username **admin** and the password remaining blank. For information about using this command, see the *Command Line Reference*.

   Example: `SMcli 192.168.128.101 -u admin -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

Controllers will continue with the autocode synchronization process from the drives and reboot. After reboot the controllers will be accessible through the original IP configuration.

Complete controller upgrade

Complete the controller upgrade by powering on the controller shelf and validating the controller software version. Then, you can collect support data and resume operations.

If you are upgrading controllers in a duplex controller-drive tray, repeat all steps to complete the upgrade for the second controller.

Step 1: Power on controller

You must power on the controller shelf to confirm that it is working correctly.

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.
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 the next step.
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 b. Controller swap with internal key management and one or more drives secured
All secured drives, Internal Key Management	Controller swap with internal key management and one or more drives secured
Mix of secured and unsecured drives, External Key Management	Proceed to the next step. After performing the controller replacement, the controllers will automatically resynchronize with the External Key Management Server and the drives will unlock and be accessible. 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.
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 b. Create external security key
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

Step 2: Check status of controllers and trays

You can use the LEDs and the storage management software to check the status of your controllers and trays.

Steps

1. 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.

2. 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.
3. For a duplex configuration, repeat step 1 through step 2 for controller B.
4. Using the LEDs and the storage management software, check the status of all of the trays in the storage array. If any component has a Needs Attention status, use the Recovery Guru to troubleshoot. If the problem is not resolved, contact technical support.

Step 3: Validate controller software version

You must ensure that your new controllers are running with the correct operating system (controller firmware) level and NVSRAM.

Steps

1. Do one of the following:
   - If you are upgrading to controllers that do not support SANtricity 11.30 and controller firmware 8.30, make sure that the version running on the new controllers matches the version that was last running on the original controllers. Normally, this will be the most recent release supported by the old controllers. If necessary, install the appropriate version on the new controllers.
   - If you are upgrading to controllers that run SANtricity 11.30 and controller firmware 8.30, download and install the latest NVSRAM after you power on the new controllers.
2. 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. From System Manager, select **Storage › Hosts**.
   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**.

For information about compatible hardware, refer to the NetApp Interoperability Matrix and the NetApp Hardware Universe.

3. If Write Back Caching was disabled for all thin volumes in preparing for the headswap, re-enable Write Back Caching.
   a. From System Manager, 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 and change the settings for read caching and write caching.
   d. Click **Save**.
4. If SAML was disabled in preparing for the headswap, re-enable SAML.
   a. From System Manager, select **Settings › Access Management**.
   b. Select the **SAML** tab, and then follow the instructions on the page.
5. Gather support data about your storage array by using either the GUI or the CLI:
   - Use either System Manager or Storage Manager's Array Management Window to collect and save a support bundle of your storage array.
     - From System Manager, select **Support › Support Center › Diagnostics tab**. Then select **Collect Support Data** and click **Collect**.
     - From the Array Management Window toolbar, select **Monitor › Health › Collect Support Data Manually**. Then enter a name and specify a location on your system where you want to store the support bundle.

       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-component-state-capture.7z`
   - Use the CLI to run the `save storageArray supportData` command to gather comprehensive support data about the storage array.

     Gathering support data can temporarily impact performance on your storage array.
6. Alert 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 Prepare to upgrade controllers.
   b. Log in to the NetApp support site at mysupport.netapp.com/eservice/assistant.
   c. Select **Product Registration** from the drop-down list under **Category 1**.
   d. 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."

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

What's next?

If your controller upgrade results in changing the vendor ID from LSI to NETAPP, go to Remount volumes after changing the vendor from LSI to NETAPP; otherwise, your controller upgrade is complete and you can resume normal operations.

Remount volumes after changing the vendor from LSI to NETAPP

If your controller upgrade results in changing the vendor ID from LSI to NETAPP, follow the appropriate procedure for your host type:

- Remount volumes on an AIX host
- Remount volumes on a VMware host
- Remount volumes on a Windows host

Remount volumes on an AIX host

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

Step

If failed volumes appear, run the `cfgmgr` command.

Remount volumes on a VMware host

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.

Steps

1. Perform a rescan on 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.

Remount volumes on a Windows host

After you replace the controllers, you must remount volumes on a Windows host to enable attached hosts to perform I/O operations with the volumes located 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 then select **Scan for Hardware Changes**.
4. Reboot the host.

Reconfigure a SAS-2 system behind a new SAS-3 controller shelf

If necessary, you can reconfigure your SAS-2 system to be used behind a new SAS-3 controller shelf.

Approved SAS-2 arrays include the E2700, E550/EF5500, and E5600/EF560. Approved SAS-2 drive shelves include the DE1600, DE5600, and DE6600. Approved SAS-3 arrays include the E2800 and E5700/EF570. Approved SAS-3 drive shelves include DE212C, DE224C, and DE460C.

About this task

In this procedure, you convert the controller shelf in an approved SAS-2 array to a drive shelf, and then place that shelf behind a new approved SAS-3 array and drive shelves, without data preservation.

This procedure applies to IOM12 and IOM12B drive shelves.

> This procedure is for like-for-like shelf IOM hot-swaps or replacements. This means you can only replace an IOM12 module with another IOM12 module or replace an IOM12B module with another IOM12B module. (Your shelf can have two IOM12 modules or have two IOM12B modules.)

Before you begin

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

- You must have a Feature Product Variance Request (FPVR). To file an FPVR, contact NetApp Professional Services.

  > Failure to acquire an FPVR before attempting this procedure can result in drive failure and controller lock down.

- 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.
- Make sure both of your arrays are prepared for the procedure:
  - **Existing array**: Existing array with SANtricity OS 8.25 or later that is powered up.
  - **New array**: New array unpacked and powered down.
- Record the serial number from the SAS-2 controller shelf that you will be converting to a drive shelf.

Step 1: Power down the controllers (non-data preservation)

All operations must be shut down before you can power down the controllers.

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.

Step 2: Install the controllers (non-data preservation)

Upon successful shut down, you can replace the controllers in the array.

Steps

1. Replace both controllers in the existing array with IOMs or ESMs.
2. If possible, use the host cables and network cables from the existing array and connect them to the controllers in the new array.

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

3. 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.

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

Step 3: Power on the controllers (non-data preservation)

After installation is complete, power on the controllers and submit your configuration changes to NetApp Technical Support.

Steps

1. Power up the new array including any attached drive shelves.
2. Configure the management port and the IP addresses by installing the SANtricity Quick Connect utility.
3. If drive security was in use on the existing array, import the security key.

4. 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.
5. 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.
   c. From the drop-down list under **Feedback Category**, select **Installed products > Decommission Request**.
   d. Select **Create Case**. 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.
      ```

   e. Select **Submit**.

The completed SAS-2 to SAS-3 configuration changes are submitted to NetApp Technical Support.