Controllers

E-Series storage systems

NetApp
January 20, 2026

Table of Contents

Controllers

Learn about upgrading E-Series controllers

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.

E-Series upgrade considerations

Before you upgrade controllers, review the following considerations.

> ⓘ Refer to the E-Series hardware overview for specific information on supported configurations for each E-Series controller.

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 E-Series controller shelf are typically managed with the SANtricity System Manager user interface.

- **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.

- **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.

> ⓘ For E4000 controllers, mirroring is only supported on Fibre Channel connections.

- **Storage object limits**

  If you change your controllers from midrange to entry-level models (for example, 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.

  When upgrading your E-Series controller, you should disable any premium features used on your storage array that are not supported on the new controllers.

- **In-band management using the Access volume**
  - The E4000 does not support in-band management using the Access volume.

    Before upgrading to E4000 controllers, unmap the Access volume from all defined hosts and host clusters.

Upgrade compatibility

Review the supported upgrade paths for each storage array model.

E4000 controller upgrade compatibility

Upgrade path	Battery	Feature Support	SAS-3 shelves
From E2800 to E4000	Order a new battery.	• E4000 does not support ARVM iSCSI • E4000 baseboard port is iSCSI only and cannot be changed to FC • E4000 can only support 300 drives • E4000 can only support 512 volumes • E4000 does not support SAS configurations • E4000 does not support Remote Storage Volumes • The E4000 does not support in-band management using the Access volume.	E4000 controllers must use SAS-3 shelves.

Upgrade path	Battery	Feature Support	SAS-3 shelves
From E5700 to E4000	Order a new battery.	• E4000 does not support ARVM iSCSI • E4000 baseboard port is iSCSI only and cannot be changed to FC • E4000 can only support 300 drives ◦ E5700 can support up to 480 drives • E4000 can only support 512 volumes ◦ E5700 can support up to 2048 volumes • Infiniband Host interface card support is not available • E4000 does not support SAS configurations • E4000 does not support Remote Storage Volumes • The E4000 does not support in-band management using the Access volume.	E4000 controllers must use SAS-3 shelves.

EF600 and EF300 controller upgrade compatibility

Upgrade path	Battery	Feature Support	SAS-3 shelves
From EF600 to EF600 with a different Host Interface Card	Reuse the old battery.	• No support for thin provisioned volumes • No support Synchronous mirroring	EF600 controllers must use SAS-3 shelves.
From EF300 to EF600	Reuse the old battery.	• No support for thin provisioned volumes • No support Synchronous mirroring	EF600 controllers must use SAS-3 shelves.

Legacy controller upgrade compatibility

Upgrade path	Battery	Vendor ID	Feature Support	SAS-3 shelves
From E2x00 to E2x00	Reuse the old battery.	Additional steps required.	Legacy snapshots are not supported on the E2700.	E2800 controllers must not be placed into SAS-2 shelves.
From E2x00 to E5x00	Order a new battery.	Additional steps are required when upgrading from E2600 to E5500 or E5600, or when upgrading from E2700 to E5400.	• 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.	E5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.
From E5x00 to E2x00	Order a new battery.	Additional steps are required when upgrading from E5500 or E5600 to E2600, or when upgrading from E5400 to E2700.	Legacy snapshots are not supported on the E2700.	5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.

Upgrade path	Battery	Vendor ID	Feature Support	SAS-3 shelves
From E5x00 to E5x00	Reuse the old battery.	Additional steps required when upgrading from E5400 to E5500 or E5600.	• 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.	E5400, E5500, and E5600 controllers must not be placed into SAS-3 shelves.
From EF5x0 to EF5x0	Reuse the old battery.	Additional steps required when upgrading from EF540 to EF550 or EF560.	• No Legacy Snapshots for EF550/EF560. • No Data Assurance for EF550/EF560 with iSCSI. • EF570 controllers must not be placed into 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: • E4000 controller shelves • EF600 controller shelves [1] • EF300 controller shelves [1] • E2800 controller shelves • E5700 controller shelves • DE212C, DE224C, DE460C drive shelves

Notes:

1. EF600 and EF300 controllers can only use SAS-3 shelves as expansion.

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 E-Series 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 have secure-enabled drives installed and you plan to perform a complete controller replacement, refer to the following table to complete the appropriate steps for your security type (internal or external) and drive state. If you do **not** have secure-enabled drives installed, you can skip this step and go to step 3 below the table.

Some steps in the table require command line interface (CLI) commands. For information about using these commands, see the Command Line Interface reference.

Security type and context	Steps
Internal key management, one or more drives locked	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 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`. 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 key.
External key management, all drives locked, you are **not** able to transition to internal key management temporarily for the controller replacement.	Contact Customer Support.
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 you must create a new CSR, get the CSR signed, and download the server certificate from the external key management server (EKMS).

3. 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.
4. Gather support data about your storage array by using either the GUI or the CLI:
   - Use System 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**.

       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.
5. 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.
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 or synchronous mirroring, delete any mirrored pairs and deactivate any mirroring relationships through the System Manager or the Array Management window.
8. 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 disable 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.

9. 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.

10. 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.
11. Turn off power to the controller-drive tray.

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

12. 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 E-Series 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.

Before you begin

Make sure you have the following:

- 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

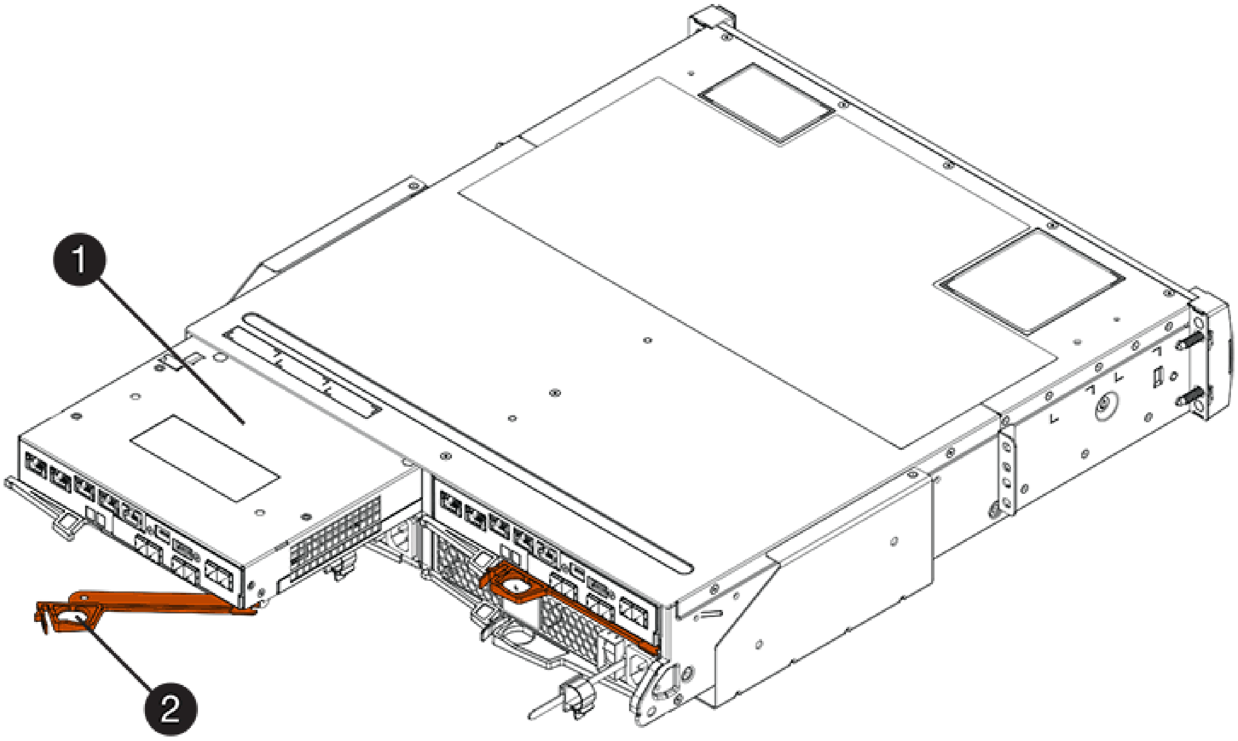
1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the old controller canister. Depending on the HIC configuration, you might be able to reconnect some cables after you replace the controller canister.
3. Disconnect all of the interface and Ethernet 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. On your model of controller-drive tray, release the tab that secures the battery to the controller canister to release the old battery.
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 E-Series 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.

Before you begin

Make sure you have the following:

- 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. 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.

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

   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.
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 handles 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.

What’s next?

If the Drive Security feature is enabled, go to Unlock drives. Otherwise, go to Complete controller upgrade.

Unlock E-Series drives

The Drive Security feature for these controllers will lock down the drives 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 a seven-segment display code of **L5**. This lock-down occurs when no drives can perform autocode synchronization (ACS). After the security key is imported, ACS resumes and updates the new controllers.

> If you are not using management port 1, try with other default IP addresses:
> Ctrl A port 1: 169.254.128.101
> Ctrl A port 2: 169.254.128.102
> Ctrl B port 1: 169.254.128.101
> Ctrl B port 2: 169.254.128.102

Steps

1. Make a direct, private ethernet connection between the storage array and the SANtricity client's laptop or PC. To do this:
   a. Use an RJ45 ethernet cable to connect the laptop to management port 1 on controller A.
   b. To complete the connection, you might need to assign the laptop to an IP address in the same subnet as controller A. During controller lockdown, controller A defaults to a management address of 169.254.128.101. So you can assign the laptop to a subnet such as "169.254.128.201".
2. Using the IP address 169.254.128.101 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 Interface reference.

   Example: `SMcli 169.254.128.101 -k -u admin -p "" -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

   Alternatively, you can import the internal key via the Rest API through the following call: `/storage-systems/{system-id}/security-key/import`

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 a seven-segment display code of **L5**. This lock-down occurs when no drives can perform autocode synchronization (ACS). After the security key is imported, ACS resumes and updates the new controllers.

Steps

1. Make a direct, private ethernet connection between the storage array and the SANtricity client’s laptop or PC. To do this:
    a. Use an RJ45 ethernet cable to connect the laptop to management port 1 on controller A.
    b. To complete the connection, you might need to assign the laptop to an IP address in the same subnet as controller A. During controller lockdown, controller A defaults to a management address of 169.254.128.101. So you can assign the laptop to a subnet such as "169.254.128.201".
2. Using the security key saved from Prepare to upgrade controllers, import the external key to IP address 169.254.128.101 with the username **admin** and the password remaining blank.

    Example: `SMcli 169.254.128.101 -k -u admin -p "" -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

    Alternatively, you can import the external key via the Rest API through the following call: `/storage-systems/{system-id}/security-key/import`

    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.

3. (Optional) If needed, the drives can be rekeyed by performing the following:

    Example: `SMcli <original_controller _ip> -u admin -p "<original_array_password>" -c "create storageArray securityKey" passPhrase=\"passPhraseString\" file=\"filename\";”`

Complete the E-Series 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.

Complete controller replacement type	Procedure and prerequisites
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 c. Run the SMclient command, `set allDrives nativeState`. d. Wait for both controllers to reboot.
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 c. Run the SMclient command, `set allDrives nativeState`. d. Wait for both controllers to reboot.
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. See External key management for detailed instructions.

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.

   After the controller successfully completes rebooting, 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. 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.

2. 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 enable the settings for read caching and write caching.

   d. Click **Save**.

3. 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.

4. Gather support data about your storage array by using either the GUI or the CLI:

   - Use System 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**.

       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.

5. 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?

Your controller upgrade is complete and you can resume normal operations.

Copyright information

Trademark information