



E-Series and SANtricity documentation

E-Series

NetApp

February 21, 2022

This PDF was generated from <https://docs.netapp.com/us-en/e-series/index.html> on February 21, 2022.
Always check docs.netapp.com for the latest.

Table of Contents

| | |
|---|-----|
| E-Series and SANtricity documentation | 1 |
| Release notes | 2 |
| What's new in SANtricity OS | 2 |
| Release notes | 8 |
| Get started | 9 |
| What this site includes | 9 |
| Learn about E-Series systems | 9 |
| Get up and running with E-Series | 19 |
| Install hardware | 22 |
| EF300 and EF600 | 22 |
| E2800 and E5700 | 34 |
| 3040 40U cabinet | 61 |
| Rack-mount hardware | 80 |
| Cabling | 80 |
| Deploy software | 102 |
| Linux express configuration | 102 |
| VMware express configuration | 241 |
| Windows express configuration | 262 |
| Upgrade systems | 284 |
| Controllers | 284 |
| SANtricity OS | 303 |
| Maintain systems | 319 |
| EF300 and EF600 | 319 |
| E2800 | 418 |
| E5700 | 584 |
| Manage storage | 714 |
| Online help for System Manager 11.7 | 714 |
| Online help for Unified Manager 5 | 714 |
| Command reference | 714 |
| Use SANtricity solutions | 715 |
| Web services proxy | 715 |
| Remote volume mirroring | 748 |
| Storage plugin for vCenter | 756 |
| Legacy solutions | 774 |
| Earlier versions | 797 |
| Hardware documentation for earlier releases | 797 |
| Software documentation for earlier releases | 797 |
| Technical reports | 798 |
| Browse platform technical reports | 798 |
| Browse security technical reports | 798 |
| Browse featured technical reports | 799 |
| Browse solution technical reports | 799 |
| Legal notices | 801 |

| | |
|----------------------|-----|
| Copyright | 801 |
| Trademarks | 801 |
| Patents | 801 |
| Privacy policy | 801 |
| Open source | 801 |

E-Series and SANtricity documentation

Release notes

What's new in SANtricity OS

The following table describes new features in SANtricity OS.



The Resource Provisioning capability, which is available only on EF300 and EF600 systems with specific NVMe SSDs, has been disabled in Versions 11.71 and 11.72 so that outstanding issues can be resolved. Note that in some System Manager views, components might be reported as resource-provisioning (or DULBE) capable, but the ability to create resource-provisioned volumes is not available.

New features in Version 11.72

| New feature | Description |
|--|--|
| SNMPv3 support | SNMPv3 is now supported for alert notifications, configurable in Settings > Alerts . SNMPv3 provides security through strong authentication and data encryption. |
| Support replicating keys to multiple key servers | For external key management for self-encrypting drives, the Create External Key Management dialog includes a new option for adding multiple key servers. |
| Updated browser versions | System Manager minimum browser versions have been updated. |

New features in Version 11.71

| New feature | Description |
|--|--|
| EF300 expansion | This release provides support for expansion to SAS-3 enclosures for the EF300 storage system. With this expansion, the 4KiB-block NVMe SSDs can coexist with 512e SAS SSDs and HDDs. However, drives with different block sizes cannot be configured in the same pool or volume group. |
| FEC mode option in iSCSI configuration | For storage arrays using the 25Gb iSCSI host interface card, a new option is available for setting the Forward Error Correction (FEC) mode when you configure iSCSI ports. |

| New feature | Description |
|--|---|
| Remote Storage Volumes | The optional Remote Storage Volumes feature allows you to import volumes from a remote storage system to a local E-Series storage system using an iSCSI connection. The remote storage may be the same brand as your E-Series system or from a different storage vendor, as long as it is accessible via iSCSI. |
| Sanitize (erase) capability added for non-FDE drives | The drive sanitize feature now includes non-FDE drives in the procedure. From the Hardware page, you can open the Drive's context menu and select "Erase" (previously, this selection was "Secure Erase"). |
| Secure connection for email alerts | To enable encrypted email notifications, you can optionally configure outgoing emails (alerts, ASUP dispatches) to supply authentication credentials. Encryption types include SMTPS and STARTTLS. |
| AutoSupport additions | An alert now appears in the Notifications area when AutoSupport is not enabled. |
| Syslog alert format change | The Syslog alert format now supports RFC 5424. |

New features in Version 11.70

| New feature | Description |
|--|---|
| New storage system model – EF300 | This release introduces the EF300 low-cost all-NVMe-flash storage system. The EF300 includes 24 NVME SSD drives and a single host interface card (HIC) per controller. The supported NVMe over Fabrics host interfaces include NVMe over IB, NVMe over RoCE, and NVMe over FC. The supported SCSI interfaces include FC, IB over iSER, and IB over SRP. Multiple EF300 storage systems and other E-Series storage systems can be viewed and managed in Unified Manager. |
| New Resource Provisioning feature (EF300 and EF600 only) | The Resource Provisioning feature is new for the EF300 and EF600 storage systems. Resource-provisioned volumes can be put in use immediately with no background initialization process. |

| New feature | Description |
|---|---|
| Add 512e block size option (EF300 and EF600 only) | For EF300 and EF600 storage systems, a volume can be set to support a 512-byte or a 4KiB block size. The 512e capability has been added to allow support of the iSCSI host interface and the VMware OS. If possible, System Manager suggests the appropriate default value. |
| New option for sending AutoSupport dispatches on demand | A new Send AutoSupport Dispatch feature allows you to send data to technical support without waiting for a scheduled dispatch. This option is available in the AutoSupport tab of the Support Center. |
| External Key Management Server enhancements | <p>The feature for connecting to an external key management server includes the following enhancements:</p> <ul style="list-style-type: none"> • Bypass the function for creating a backup key. • Choose an intermediate certificate for the key management server, in addition to the client and server certificates. |
| Certificate enhancements | This release allows for using an external tool such as OpenSSL to generate a Certificate Signing Request (CSR), which also requires you to import a private key file along with the signed certificate. |
| New Offline Initialization feature for Volume Groups | <p>For volume creation, System Manager provides a method for skipping the host assignment step so that newly created volumes are initialized offline. This capability is applicable only to RAID volume groups on SAS drives (i.e., not to dynamic disk pools or to the NVMe SSDs included in the EF300 and EF600 storage systems). This feature is for workloads that need to have the volumes at full performance when usage begins, rather than having initialization run in the background.</p> |

| New feature | Description |
|--|--|
| New Collect Configuration Data feature | This new feature saves RAID configuration data from the controller, which includes all data for volume groups and disk pools (the same information as the CLI command for save storageArray dbmDatabase). This capability has been added to aid technical support and is located in the Diagnostics tab of the Support Center. |
| Change default preservation capacity for disk pools in 12 drive case | Previously, a 12-drive disk pool was created with enough preservation (spare) capacity to cover two drives. The default is now changed to handle a single drive failure to offer a more cost-effective small pool default. |

New features in Version 11.62

| New feature | Description |
|---|---|
| Downloadable CLI | System Manager for the E5700, EF570, E2800, and EF280 arrays now includes the ability to download and install the SANtricity command line interface (CLI) via a link in the Settings > System > Add-ons page. This is the https-based version of the CLI (also referred to as "Secure CLI"). This capability was previously released with the EF600 array. |
| Mirroring configuration changes in System Manager and Unified Manager | The tasks for configuring synchronous and asynchronous mirrored pairs have moved from System Manager to Unified Manager. All other tasks for managing mirrored pairs remain in System Manager. |
| New 200Gb-capable HIC (EF600 arrays only) | This release adds a new 200Gb-capable HIC for EF600 storage arrays. Interfaces supported are NVMe/IB, NVMe/RoCE, and iSER/IB. Additionally, 100Gb SRP/IB is supported. |
| Additional options on 100Gb HIC (EF600 arrays only) | On the existing 100Gb HIC, iSER/IB and SRP/IB interfaces are now supported for EF600 storage arrays. (These interfaces are already supported for EF570 and E5700 arrays.) |

| New feature | Description |
|---|---|
| Delete mail server in System Manager | System Manager allowed a mail server to be configured, but did not have an easy mechanism to remove it. With this release, the mail server configuration in System Manager can now be removed from Alerts, so that alerts are no longer sent to the email addresses associated with this mail server. |
| Optimization capacity adjustments for pools and volume groups (SSD drives only) in System Manager | For SSD drives, a new optimization capacity slider is available in System Manager for the Pool settings and Volume Group settings. The slider enables you to adjust the balance of available capacity versus SSD write performance and drive wear life. |
| New host types in System Manager | When you create new hosts in System Manager, the presented host options are now organized into three categories to provide better guidance: Common, Uncommon, and Use only if directed. |

New features in Version 11.61

| New feature | Description |
|--------------------------------------|--|
| Fibre Channel support for the EF600 | This release adds Fibre Channel host support for the EF600 storage system. This is the first SCSI host supported by the EF600, which initially released with all NVMe over Fabrics host protocols. A single controller for the EF600 can be viewed and managed in System Manager. Multiple EF600 storage systems can be viewed and managed in Unified Manager. |
| Password requirements for admin user | For first-time login in Unified Manager, you must now enter a password for the administrator user. There is no longer a default "admin" password. |

New features in Version 11.60

| New feature | Description |
|----------------------------------|---|
| New storage system model – EF600 | <p>This release offers a new EF600 all-flash storage system. The EF600 includes NVMe-oF host interfaces and NVMe SSDs.</p> <p>The EF600 significantly increases throughput and reduces latency. The supported host interfaces include NVMe over IB, NVMe over RoCE, and NVMe over FC, which can be configured in System Manager. Multiple EF600 storage systems can be viewed and managed in Unified Manager.</p> |
| Downloadable CLI | <p>System Manager now includes the ability to download and install the SANtricity command line interface (CLI) via a link in the Settings > System > Add-ons page. This is the https- based version of the CLI. The legacy SANtricity Storage Manager package continues to include the CLI as well.</p> |

New features in Version 11.53

This version includes only minor enhancements and fixes.

New features in Version 11.52

| New feature | Description |
|-----------------------------|---|
| NVMe over FC host interface | <p>An NVMe over Fibre Channel host connection can now be ordered for EF570 or E5700 E-Series controllers, in addition to the existing support for NVMe over RoCE and NVMe over InfiniBand.</p> <p>System Manager includes statistics for this new connection type in Settings > System under "NVMe over Fibre Channel details."</p> |

New features in Version 11.51

This version includes only minor enhancements and fixes.

New features in Version 11.50

| New feature | Description |
|--|--|
| NVMe over RoCE interface | An NVMe over RoCE host connection can now be ordered for EF570 or E5700 E-Series controllers. System Manager includes new functions for configuring the network connection to the host (available from the Hardware page or from Settings > System), and functions for viewing data about the NVMe over RoCE connections to the storage array (available from Support > Support Center or from Settings > System). |
| Manual drive selection for volume groups | In addition to convenient automatic selection, a new option is available for selecting individual drives when you create a volume group. In general, automatic drive selection is recommended, but the individual drive selection option is available for environments with special drive location requirements. |
| SANtricity Unified Manager | Unified Manager is a separately installed, browser-based application that discovers and manages E2800 series controllers and E5700 series controllers. While this new application is not a new feature of System Manager, it does provide a new browser-based enterprise framework from which System Manager can be launched for discovered storage arrays. The new Unified Manager can be downloaded from the Support software downloads area. |

Release notes

Release Notes are available outside this site. You will be prompted to log in using your NetApp Support Site credentials.

- [11.70 Release notes](#)
- [11.60 Release notes](#)
- [11.50 Release notes](#)

Get started

What this site includes

This site includes information for specific E-Series releases, models, and components.

| What's included | What's <i>not</i> included |
|--|---|
| <p>This site includes information for the following releases and component types:</p> <ul style="list-style-type: none">• SANtricity software — version 11.50 and later.• Controller firmware — version 8.50 and later.• Controller types — All E2800, EF280, EF300, E5700, EF570, and EF600 models.• Interface types — Fibre Channel, iSCSI, iSER, SAS, and NVMe.• Operating systems installed on hosts — Linux, VMware, and Windows. <p> Additional interfaces and operating systems might be supported. For more information, contact technical support.</p> | <p>This site does <i>not</i> include information for releases <i>earlier than</i> software version 11.50 or firmware version 8.50. For earlier releases, go to the E-Series and SANtricity Document Resources page.</p> <p>For information on your site preparation requirements, go to NetApp Hardware Universe.</p> |

Learn about E-Series systems

E-Series terminology

Learn more about the terms used in E-Series.

| Term | Description |
|-------------------------------|--|
| controller | A controller consists of a board, firmware, and software. It controls the drives and implements the functions. |
| duplex/simplex configurations | Duplex is a two-controller module configuration within the storage array. Simplex is a single-controller module configuration. |
| HDD | Hard disk drives (HDDs) are data storage devices that use rotating metal platters with a magnetic coating. |

| Term | Description |
|--------------------|---|
| HIC | A host interface card (HIC) connects the array to the host. It can optionally be installed within a controller canister. |
| IB | InfiniBand (IB) is a communications standard for data transmission between high-performance servers and storage systems. |
| IOPS | IOPS is input/output operations per second. |
| mirroring | Mirroring is the replication of data volumes onto separate storage arrays to ensure continuous availability. |
| pool | A pool is a set of drives that is logically grouped. You can use a pool to create one or more volumes accessible to a host. |
| power/fan canister | A power/fan canister is an assembly that slides into a shelf. It includes a power supply and an integrated fan. |
| rack unit (U) | A rack unit (abbreviated U) is a unit of measure defined as 44.50 millimetres (1.75 in). |
| SAS | Serial Attached SCSI (SAS) is a point-to-point serial protocol that links controllers directly to disk drives. |
| RoCE | RDMA over Converged Ethernet (RoCE) is a network protocol that allows remote direct memory access (RDMA) over an Ethernet network. |
| shelf | A shelf is an enclosure installed in a cabinet or rack. It contains the hardware components for the storage array. There are two types of shelves: a controller shelf and a drive shelf. A controller shelf includes controllers and drives. A drive shelf includes input/output modules (IOMs) and drives. |
| snapshot | A snapshot image is a logical copy of volume data, captured at a particular point-in-time. Like a restore point, snapshot images allow you to roll back to a known good data set. |

| Term | Description |
|---------------|--|
| SSD | Solid-state disks (SSDs) are data storage devices that use solid state memory (flash) to store data persistently. SSDs emulate conventional hard drives, and are available with the same interfaces that hard drives use. |
| storage array | A storage array includes shelves, controllers, drives, software, and firmware. |
| volume | A volume is a container in which applications, databases, and file systems store data. It is the logical component created for the host to access storage on the storage array. |
| workload | A workload is a storage object that supports an application. For some applications, System Manager configures the workload to contain volumes with similar underlying volume characteristics. These volume characteristics are optimized based on the type of application the workload supports. |

E-Series hardware overview

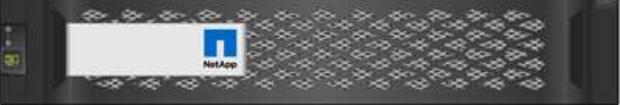
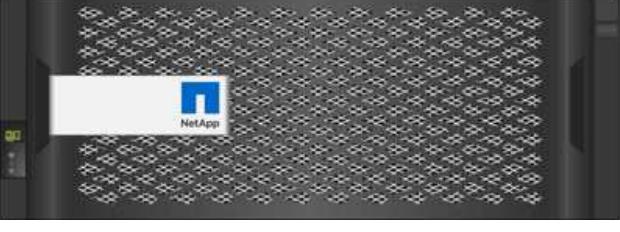
E-Series storage arrays are available in several configurations and models.

A storage array includes shelves, controllers, drives, software, and firmware. The array can be installed in a rack or cabinet, with customizable hardware for one or two controllers, in a 12-, 24-, or 60-drive shelf. You can connect the storage array to a SAN from multiple interface types and to a variety of host operating systems.

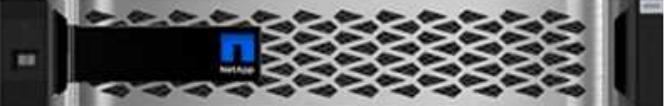
E-Series arrays are available in the following models:

- E2800 series — entry-level hybrid
- EF280 series — entry-level all flash
- EF300 series — entry-level all flash, all NVMe
- E5700 series — midrange hybrid
- EF570 series — midrange all flash
- EF600 series — midrange all flash, all NVMe

E2800 models

| Component | Specification |
|-------------|---|
| Rack sizes: | <ul style="list-style-type: none"> • 2U12 (2 rack units; 12 drives) • 2U24 (2 rack units; 24 drives)  <ul style="list-style-type: none"> • 4U60 (4 rack units; 60 drives)  |
| Drives: | <p>Supports the following drive types:</p> <ul style="list-style-type: none"> • 3.5" NL-SAS (up to 180) • 2.5" SAS SSD (up to 120) • 2.5" SAS HDD (up to 180) |
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 12Gb SAS • 10Gb or 25Gb iSCSI • 16Gb or 32Gb Fibre Channel |

EF280 models

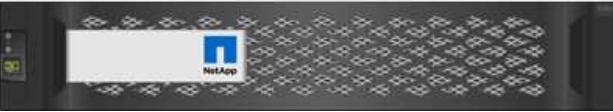
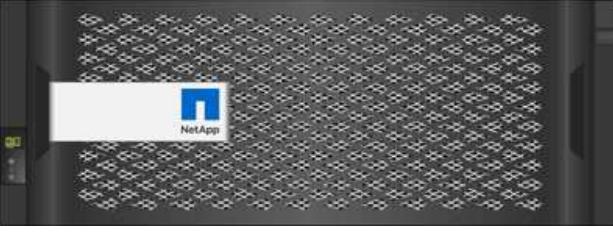
| Component | Specification |
|-------------|--|
| Rack sizes: | <p>2U24 (2 rack units; 24 drives)</p>  |
| Drives: | <p>Supports up to 96 SSD 2.5" drives</p> |

| Component | Specification |
|-------------|--|
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 12Gb SAS • 10Gb or 25Gb iSCSI • 16Gb or 32Gb Fibre Channel |

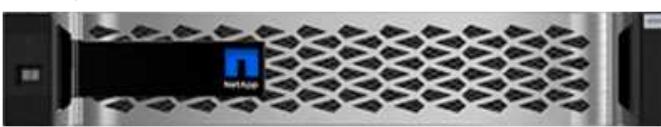
EF300 models

| Component | Specification |
|------------------|---|
| Rack sizes: | <p>2U24 (2 rack units; 24 drives)</p>  |
| Drives and HICs: | <p>Supports up to 24 NVMe SSDs, with a single host interface card (HIC) per controller.</p> |
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 25Gb iSCSI • 32Gb NVMe / Fibre Channel • 32Gb SCSI / Fibre Channel • 100Gb iSER / IB • 100Gb SRP / IB • 100Gb NVMe / IB • 100Gb NVMe / RoCE |

E5700 models

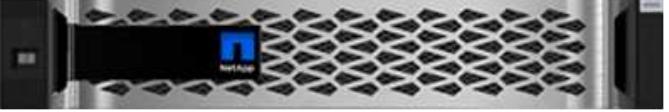
| Component | Specification |
|-------------|--|
| Rack sizes: | <ul style="list-style-type: none"> • 2U24 (2 rack units; 24 drives)  • 4U60 (4 rack units; 60 drives)  |
| Drives: | <p>Supports up to 480 of the following drive types:</p> <ul style="list-style-type: none"> • 3.5" NL-SAS drives • 2.5" SAS SSD drives • 2.5" SAS HDD drives |
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 12Gb SAS • 10Gb or 25Gb iSCSI • 16Gb or 32Gb Fibre Channel • 32Gb NVMe / Fibre Channel • 100Gb iSER / IB • 100Gb SRP / IB • 100Gb NVMe / IB • 100Gb NVMe / RoCE |

EF570 models

| Component | Specification |
|-------------|--|
| Rack sizes: | <p>2U24 (2 rack units; 24 drives)</p>  |
| Drives: | <p>Supports up to 120 SSD 2.5" drives</p> |

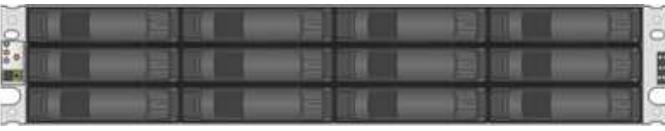
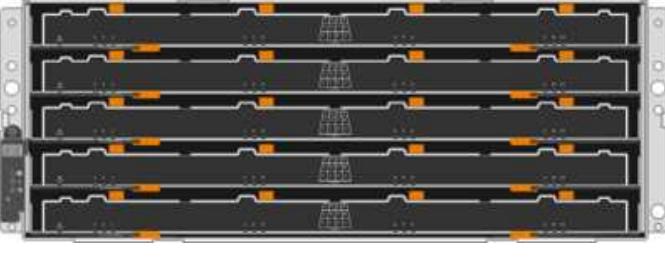
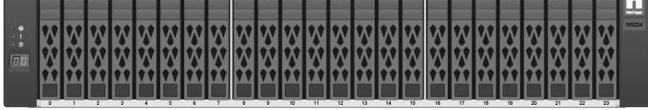
| Component | Specification |
|-------------|--|
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 12Gb SAS • 10Gb or 25Gb iSCSI • 16Gb or 32Gb Fibre Channel • 32Gb NVMe / Fibre Channel • 100Gb iSER / IB • 100Gb SRP / IB • 100Gb NVMe / IB • 100Gb NVMe / RoCE |

EF600 models

| Component | Specification |
|------------------|--|
| Rack sizes: | <p>2U24 (2 rack units; 24 drives)</p>  |
| Drives and HICs: | <p>Supports up to 24 NVMe SSDs, with two host interface cards (HICs) per controller.</p> |
| Interfaces: | <p>Available with the following interfaces:</p> <ul style="list-style-type: none"> • 25Gb iSCSI • 32Gb NVMe / Fibre Channel • 32Gb SCSI / Fibre Channel • 100Gb iSER / IB • 100Gb SRP / IB • 100Gb NVMe / IB • 100Gb NVMe / RoCE • 200Gb iSER / IB • 200Gb NVMe / IB • 200Gb NVMe / RoCE |

E-Series shelf types

E-Series systems are available in a variety of shelf sizes.

| Shelf type | Illustration |
|--|---|
| DE212C: <ul style="list-style-type: none"> • 2u12 (2 rack units; 12 drives) • 3.5" HDDs and/or 2.5" SSDs (with adapter) • E2800 controllers only |  |
| DE224C: <ul style="list-style-type: none"> • 2u24 (2 rack units; 24 drives) • 2.5" HDD and/or 2.5" SSD drives • E2800, EF280, E5700, and EF570 controllers |  |
| DE460C: <ul style="list-style-type: none"> • 4u60 (4 rack units; 60 drives) • 3.5" and 2.5" drives (NL-SAS, SAS, and SSD) • E2800 and E5700 controllers |  |
| NE224: <ul style="list-style-type: none"> • 2u24 (2 rack units; 24 drives) • 2.5" NVMe SSD drives • EF300 and EF600 controllers |  |

SANtricity software overview

E-Series systems include SANtricity software for storage provisioning and other tasks.

SANtricity software consists of these management interfaces:

- System Manager—a web-based interface used for managing one controller in a storage array.
- Unified Manager—a web-based interface used for viewing and managing all storage arrays in your network.
- Web Services Proxy—a REST API used for viewing and managing all storage arrays in your network.
- Command line interface (CLI)—a software application for configuring and monitoring storage arrays.



EF600 and EF300 storage arrays do not support mirroring, thin volumes, or SSD Cache features.

SANtricity System Manager

System Manager is web-based management software embedded on each controller. To access the user interface, point a browser to the controller's IP address. A setup wizard helps you get started with system

configuration.

System Manager offers a variety of management features, including:

| | | |
|---|--------------------------|---|
|  | Performance | View up to 30 days of performance data, including I/O latency, IOPS, CPU utilization, and throughput. |
|  | Storage | Provision storage using pools or volume groups, and create application workloads. |
|  | Data protection | Perform backup and disaster recovery using snapshots, volume copy, and remote mirroring. |
|  | Hardware | Check component status and perform some functions related to those components, such as assigning hot spare drives. |
|  | Alerts | Notify administrators about important events occurring on the storage array. Alerts can be sent through email, SNMP traps, and syslog. |
|  | Access Management | Configure user authentication that requires users to log in to the system with assigned credentials. |
|  | System Settings | Configure other system performance features, such as SSD cache and autoload balancing. |
|  | Support | View diagnostic data, manage upgrades, and configure AutoSupport, which monitors the health of a storage array and sends automatic dispatches to technical support. |

SANtricity Unified Manager

Unified Manager is web-based software used for managing your entire domain. From a central view, you can

see status for all newer E-Series and EF-Series arrays, such as the E2800, EF280, EF300, E5700, EF570, and EF600. You can also perform batch operations on selected storage arrays.

Unified Manager is installed on a management server along with the Web Services Proxy. To access Unified Manager, you open a browser and enter the URL pointing to the server where the Web Services Proxy is installed.

Unified Manager offers a variety of management features, including:

| | | |
|---|--------------------------------|---|
|  | Discover storage arrays | Find and add the storage arrays you want to manage in your organization's network. You can then view the status of all storage arrays from a single page. |
|  | Launch | Open an instance of System Manager to perform individual management operations on a particular storage array. |
|  | Import Settings | Perform a batch import from one storage array to multiple arrays, including settings for alerts, AutoSupport, and directory services. |
|  | Mirroring | Configure asynchronous or synchronous mirrored pairs between two storage arrays. |
|  | Manage Groups | Organize storage arrays into groups for easier management. |
|  | Upgrade Center | Upgrade the SANtricity OS software on multiple storage arrays. |
|  | Certificates | Create certificate signing requests (CSRs), import certificates, and manage existing certificates for multiple storage arrays. |



Access Management

Configure user authentication that requires users to log in to Unified Manager with assigned credentials.

SANtricity Web Services Proxy

The Web Services Proxy is a RESTful API server that can manage hundreds of new and legacy E-Series arrays. The proxy is installed separately on a Windows or Linux server.

Web Services includes API documentation that allows you to directly interact with the REST API. To access the Web Services API documentation, you open a browser and enter the URL pointing to the server where the Web Services Proxy is installed.

Command line interface (CLI)

The command line interface (CLI) is a software application that provides a way to configure and monitor storage arrays. Using the CLI, you can run commands from an operating system prompt, such as the DOS C: prompt, a Linux operating system path, or a Solaris operating system path.

E-Series videos

Access video demos to learn more about E-Series systems.

E-Series: Fast, Simple, Reliable Storage

This video highlights the key benefits of using NetApp E-Series systems versus using commodity servers for storage.

[NetApp video: Key benefits of using NetApp E-Series systems versus using commodity servers for storage](#)

System Manager: Easy Setup and Configuration

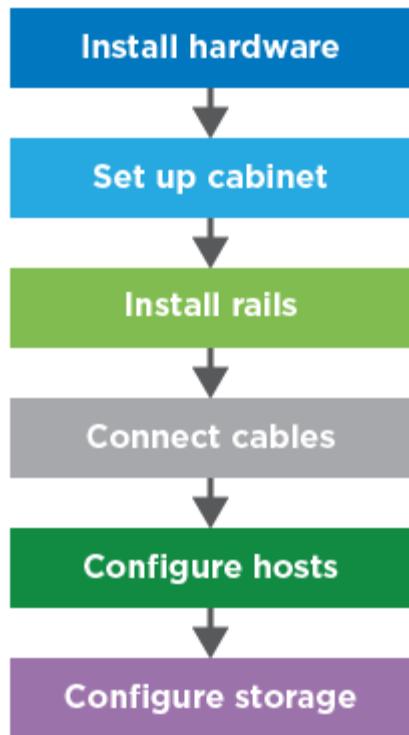
This Technical Demo shows how the web-based SANtricity System Manager interface enables easy set-up and configuration of the NetApp E2800.

[NetApp video: SANtricity System Manager: Easy Setup and Configuration](#)

Get up and running with E-Series

To get up and running with E-Series systems, you install hardware components, configure host systems, and configure storage.

Deploying the storage array involves the following workflow:



Step 1: Install hardware

To install the E-Series hardware, access the Installation and Setup instructions for your storage array and shelf type:

- [EF600 or EF300 series with 24-drive shelf](#)
- [E2800/EF280 or E5700/EF570 series with 12- or 24-drive shelves](#)
- [E2800 or E5700 series with 60-drive shelf](#)

Step 2: Set up cabinet

If you are setting up a new cabinet for the storage array, you need to move the cabinet to its permanent location, install the hardware, and connect it to a power source. To set up the cabinet, access the following instructions:

- [Install 3040 40U cabinet](#)

Step 3: Install rails

When shipped, each shelf includes rack-mounting hardware. For detailed instructions on installing the rails, select your rail types:

- [Install adjustable support rails](#)
- [Install 2U enclosure into a four-post rack](#)
- [Install DE224C shelf into a two-post rack](#)
- [Install SuperRail into a four-post rack \(DE224C/DE460C shelves\)](#)

Step 4: Connect cables

The Installation and Setup instructions (Step 1) include instructions for connecting cables. However, if you need lists of supported cables and transceivers, best practices for cabling, and detailed information about the host ports for your controller, access the following instructions:

- [Cable E-Series hardware](#)

Step 5: Configure hosts

To make storage available to a host, select a guide for the host's operating system type:

- [Linux express configuration](#)
- [VMware express configuration](#)
- [Windows express configuration](#)

Step 6: Configure storage

To configure storage, you can access the web-based interface, System Manager, by pointing a browser to the controller's IP address. A setup wizard helps you get started with system configuration. As an alternative, you can also use the command line interface (CLI).

Select the interface you want to use:

- [SANtricity System Manager Online Help for 11.7x](#)
- [SANtricity System Manager Online Help for 11.6x](#)

Install hardware

EF300 and EF600

Install and set up EF300 and EF600 storage systems

Learn how to install and set up the EF300 or EF600 storage system.

You can choose one of the following formats to guide you through installing and setting up your new storage system.

- **PDF**

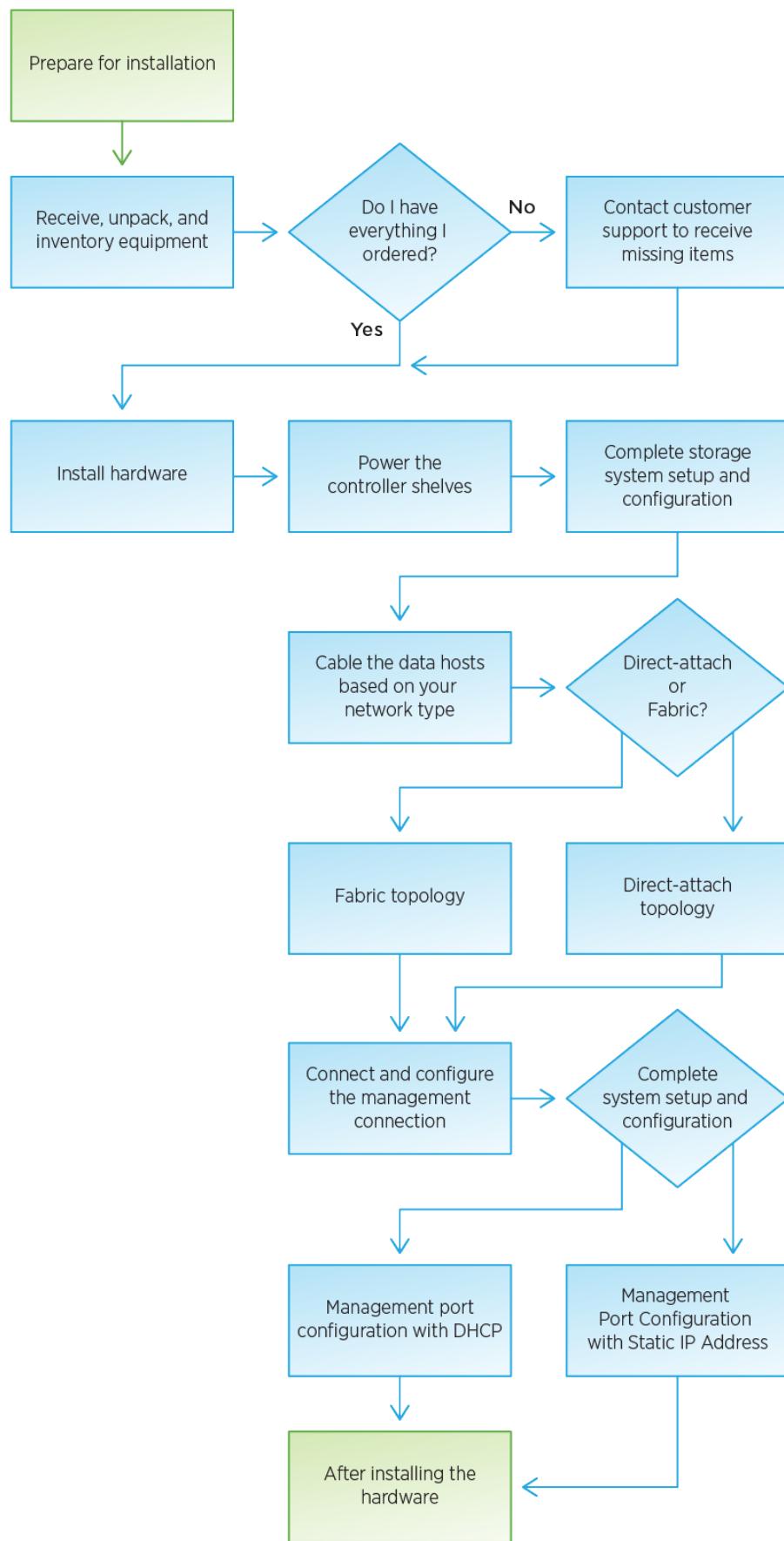
This is a [PDF poster](#) of step-by-step instructions with live links to additional content.

- **Online instructions**

These are the online setup instructions described on this site. Start with [Prepare for installation](#) to get started.

Install process

Before you install and set up your new storage system, familiarize yourself with the installation process:



Prepare for installation

Learn how to prepare for installation of your EF300 or EF600 series storage system.

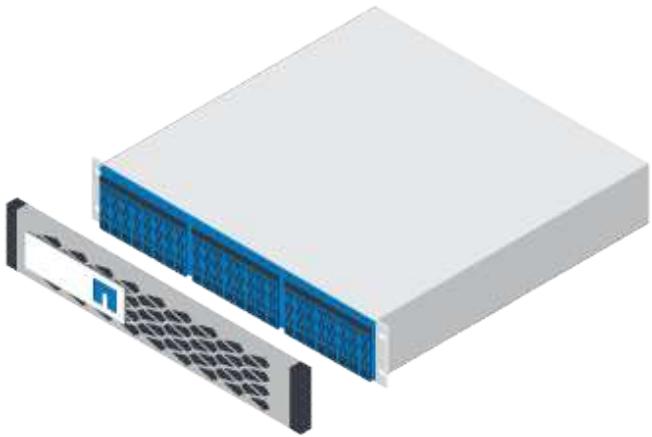
Before you begin

If you are cabling your EF300 for SAS expansion, review the following information:

- [Add SAS expansion cards](#) for SAS expansion card installation.
- [Cabling overview](#) for SAS expansion cabling.

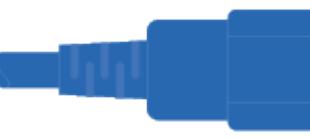
Steps

1. Create an account and register your hardware at [mysupport.netapp.com](#).
2. Ensure that the following items are in the box that you received.

| | |
|---|--|
|  | Shelf with drives installed (bezel and end caps packaged separately) |
|  | Rack-mount hardware |

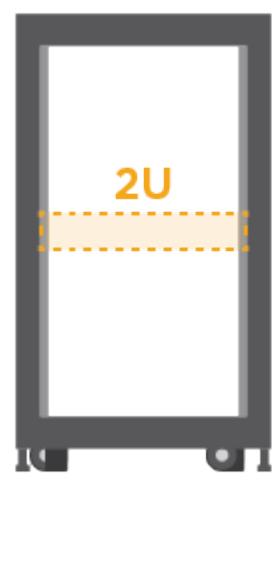
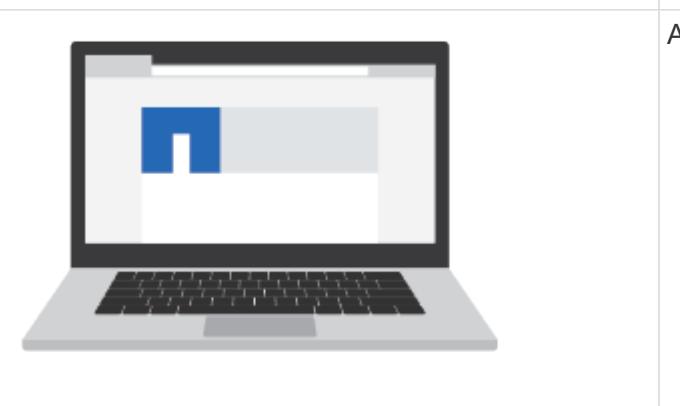
The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see [Hardware Universe](#) to locate the cable and identify its use.

| Connector type | Cable type | Use |
|---|---------------------------------------|-----------------------|
|  | RJ-45 Ethernet cables (if ordered) | Management connection |

| Connector type | Cable type | Use |
|---|------------------------------|--------------------------------|
|  | I/O cables (if ordered) | Cabling the data hosts |
|  | Power cables (if ordered) | Powering up the storage system |

3. Ensure that you provide the following items.

| | |
|---|-------------------------|
|  | Phillips #2 screwdriver |
|  | Flashlight |
|  | ESD strap |

| | |
|--|---|
|  | <p>2U rack space: A standard 19 in. (48.30 cm) rack to fit 2U shelves of the following dimensions.</p> <p>Depth: 19.0 in. (48.3 cm)</p> <p>Width: 17.6 in. (44.7 cm)</p> <p>Height: 3.34 in. (8.48 cm)</p> <p>Shelf: 24-drive</p> <p>Max Weight: 60.5 lb (27.4 kg)</p> <p> Using third-party cabinets might cause the power cables to restrict access to the controller.</p> |
|  | <p>A supported browser for the management software:</p> <ul style="list-style-type: none"> • Google Chrome (version 78 and later) • Microsoft Internet Explorer (version 11 and later) • Microsoft Edge (88 and later) • Mozilla Firefox (version 70 and later) • Safari (version 12 and later) |

Install the hardware

You can install an EF300 or EF600 storage system in a two-post rack or a NetApp system cabinet.

Before you begin

Before you install an EF300 or EF600 storage system, make sure you do the following:

- Register your hardware at mysupport.netapp.com.
- Prepare a flat, static-free work area.
- Take anti-static precautions.

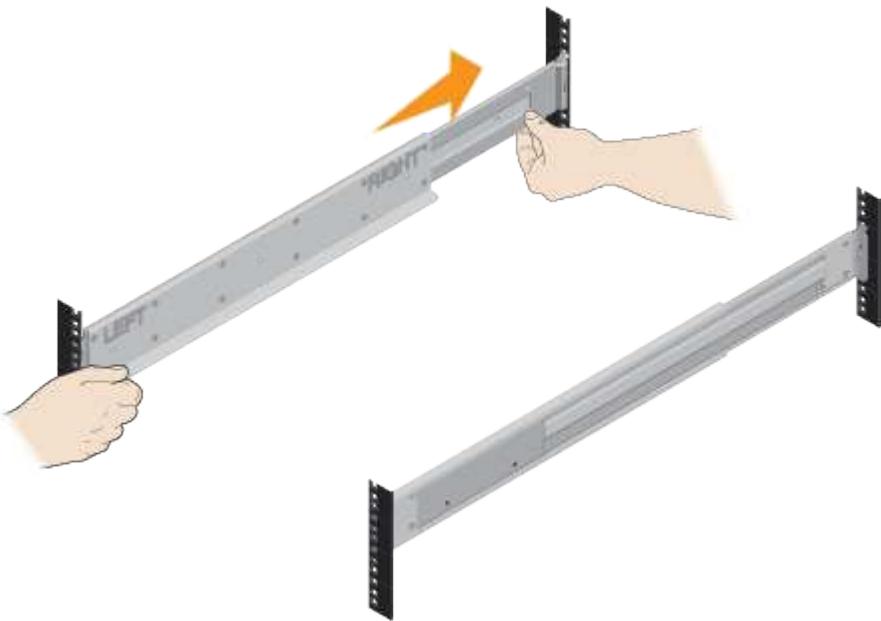
Steps

1. Unpack the hardware.
 - a. Unpack the contents and inventory the contained hardware against the packing slip.
 - b. Before proceeding, read through all the instructions.
2. Install the rails.



To prevent the equipment from toppling over, install the hardware from the bottom of the rack or cabinet up to the top.

If instructions were included with your rack-mounting hardware, refer to them to learn how to install the rails. For additional rack-mounting instructions, see [Rack-mount hardware](#).



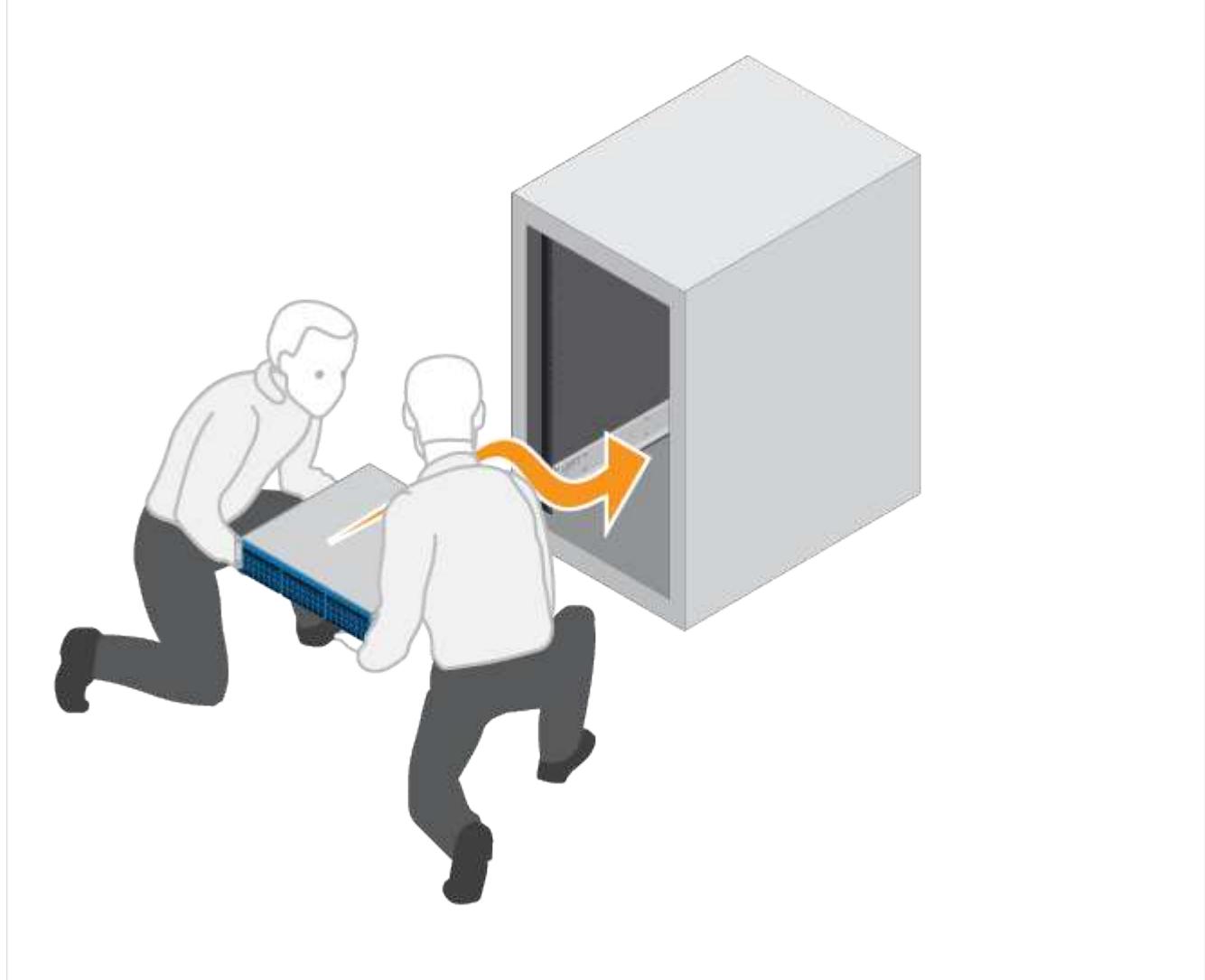
3. Install the shelf.

- a. If you are installing multiple shelves, begin installing from the bottom to the top of the cabinet. Position the back of the shelf onto the rails.



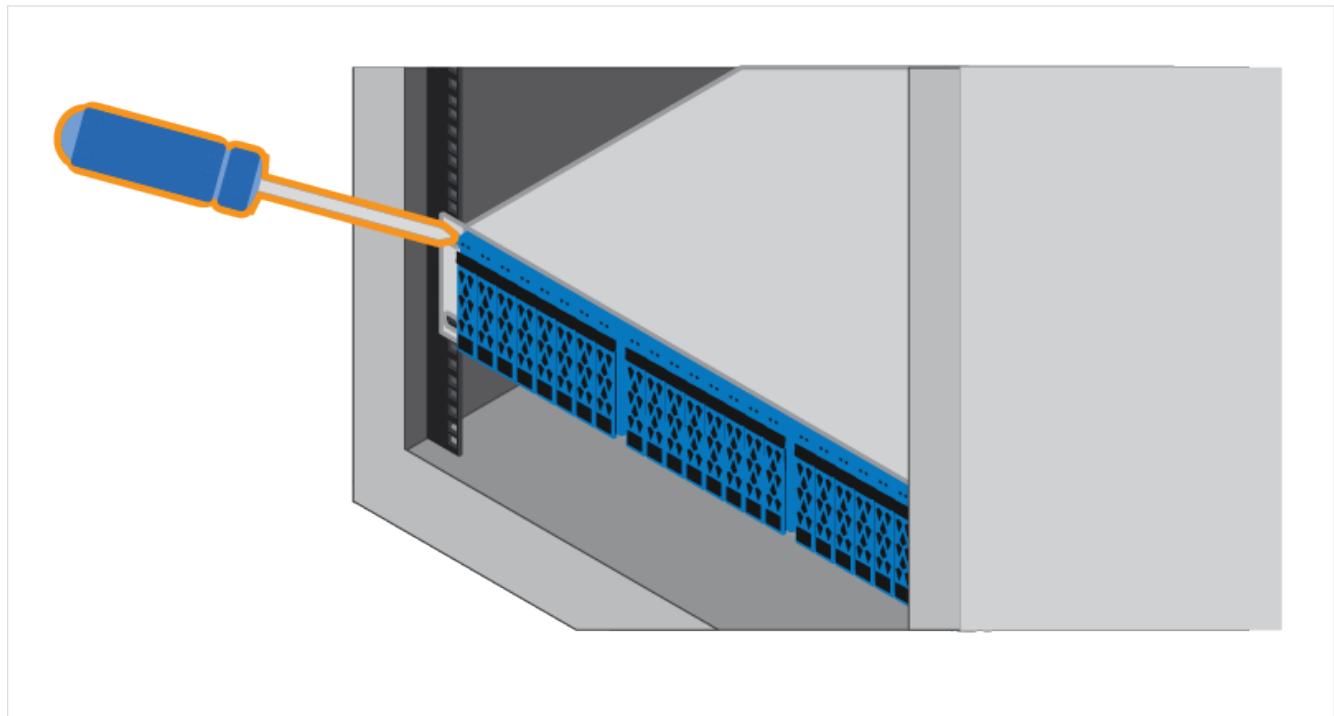
When installing the shelf, use a team-lift with two people.

- b. Supporting the shelf from the bottom, slide it into the cabinet.



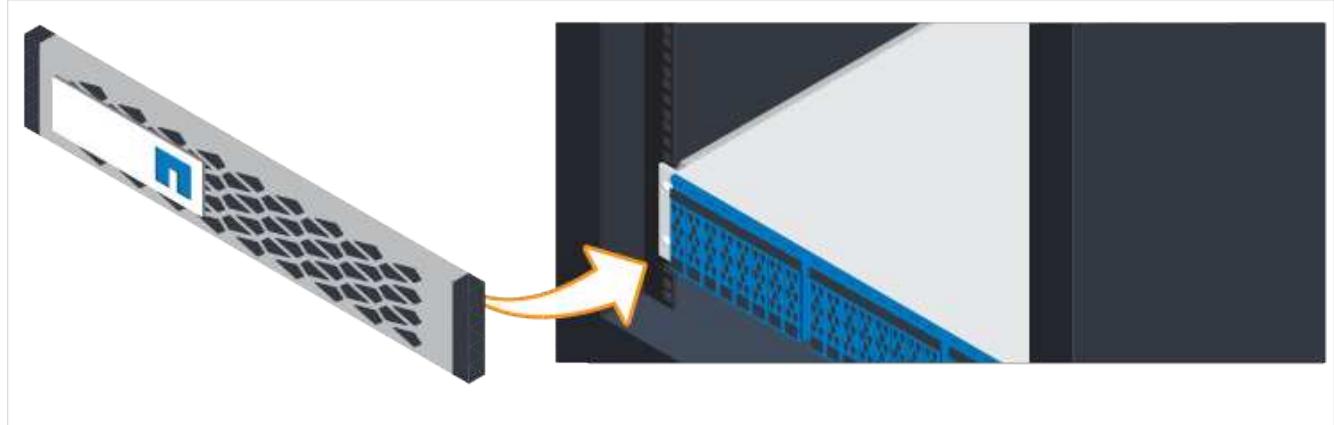
4. Secure the shelf.

For more information, see [Rack-mount hardware](#).



5. Install the faceplate.

- a. Align the faceplate with the shelf, and snap into place.



Power the controller shelves

Learn how to attach the power cables and power on the drive shelves.

Before you begin

Before you power the controller shelves, make sure to do the following:

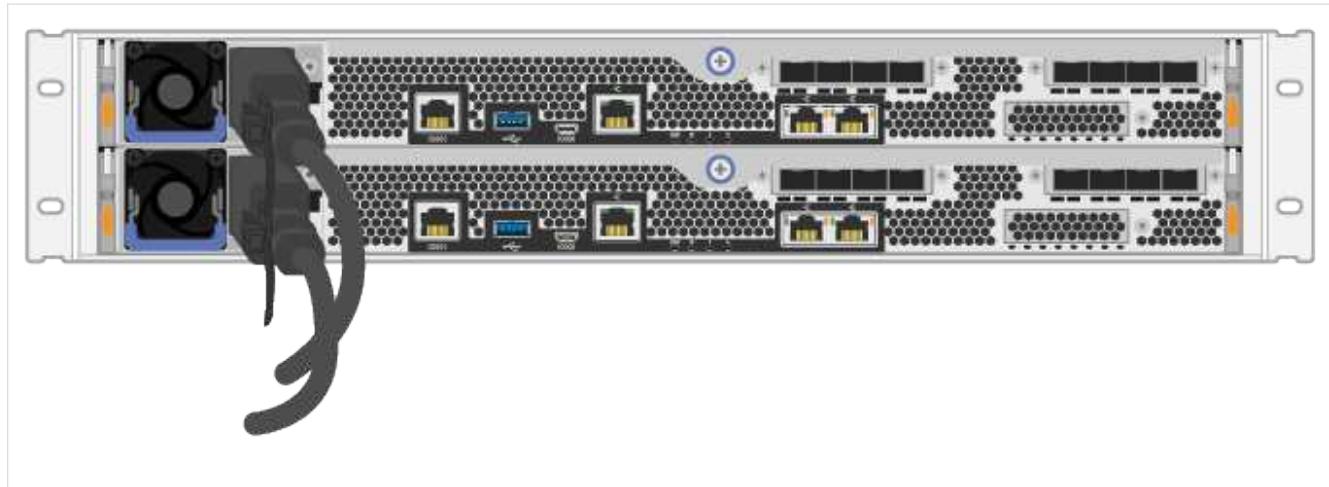
- Install your hardware.
- Take anti-static precautions.

Steps

1. Plug in the power cables, one to each controller (EF600 pictured below).



Power cables



2. Connect the two power cables, one from each controller, to two separate power distribution units (PDUs) in the cabinet or rack.



Accessing a EF300 or EF600 controller canister from the shelf can be blocked by third-party PDUs. Do not use power outlets directly behind the controller canister.

3. Allow the controller to boot for five minutes before completing the storage system set up and configuration.

Result

The controller boots automatically. The LEDs flash on and the fans start to indicate that the controller is powering on.



Fans are very loud when they first power on.

Complete storage system setup and configuration

Learn how to connect the controller cables to your network, and then complete the setup and configuration.

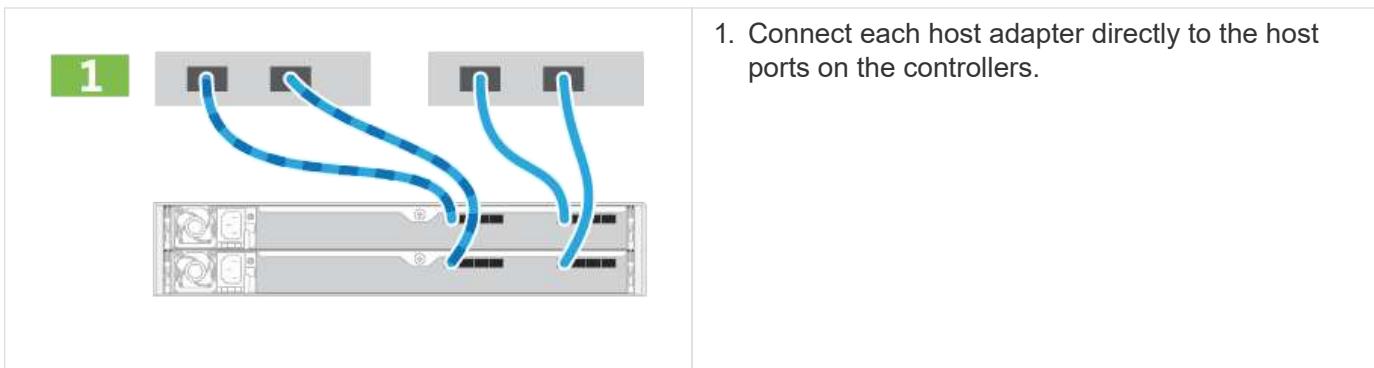
Step 1: Cable the data hosts

Cable the storage system according to your network topology.

Option 1: Direct-attach topology

The following example shows cabling to the data hosts using a direct-attach topology.

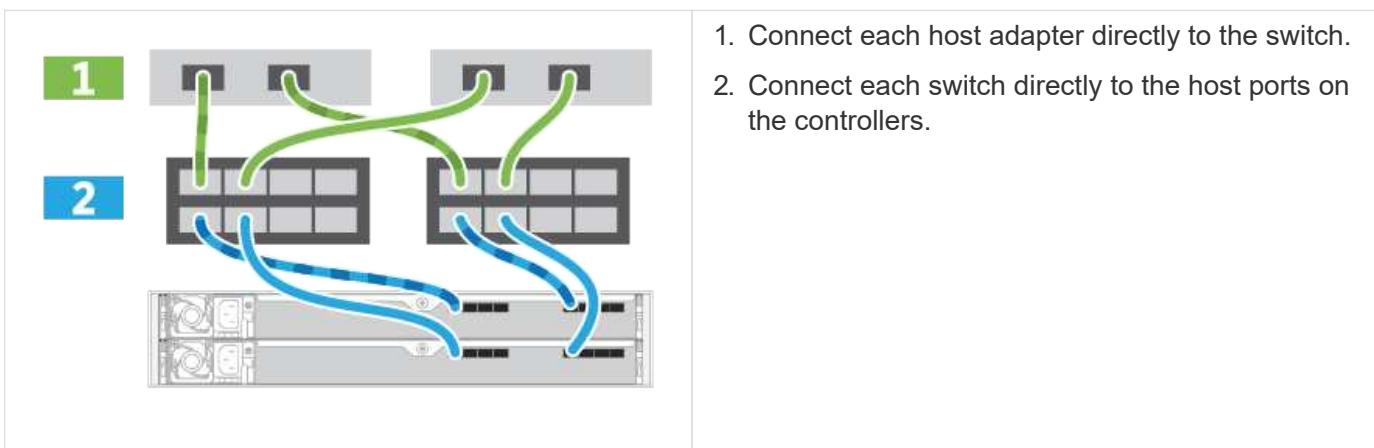
Table 1. Example A: Direct-attach topology



Option 2: Fabric topology

The following example shows cabling to the data hosts using a fabric topology.

Table 2. Example B: Fabric topology



Step 2: Connect and configure the management connection

You can configure the controller management ports using a DHCP server or a static IP address.

Option 1: DHCP server

Learn how to configure the management ports with a DHCP server.

Before you begin

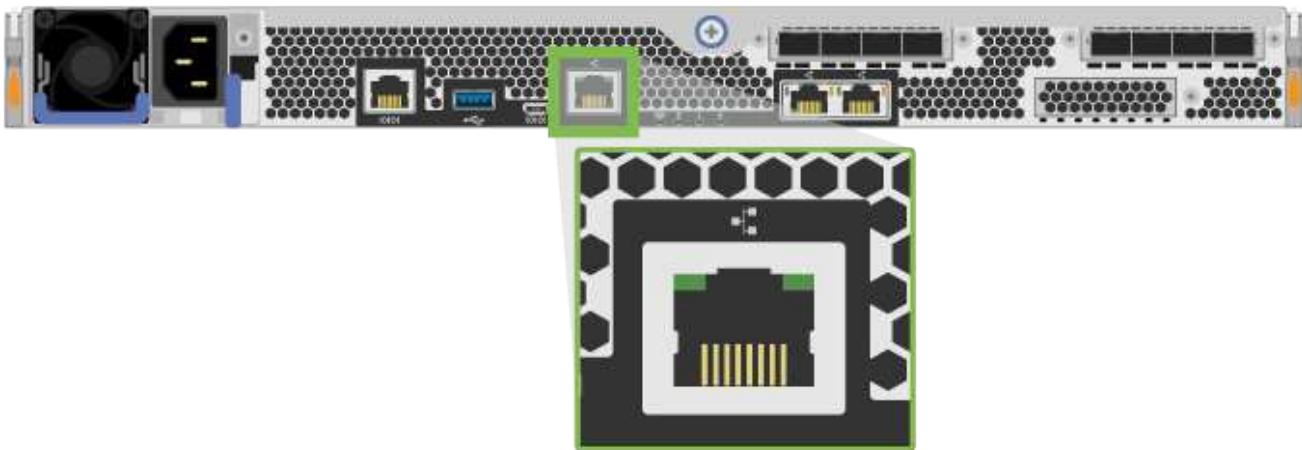
- Configure your DHCP server to associate an IP address, subnet mask, and gateway address as a permanent lease for each controller.
- Obtain the assigned IP addresses you will use to connect to the storage system from your network administrator.

Steps

- Connect an Ethernet cable to each controller's management port, and connect the other end to your network.



The following figure shows an example of the controller's management port location (EF600 shown):



2. Open a browser and connect to the storage system using one of the controller IP addresses provided to you by your network administrator.

Option 2: Static IP address

Learn how to configure the management ports manually by entering the IP address and the subnet mask.

Before you begin

- Obtain the controllers' IP address, subnet mask, gateway address, and DNS and NTP server information from your network administrator.
- Make sure that the laptop you are using is not receiving network configuration from a DHCP server.

Steps

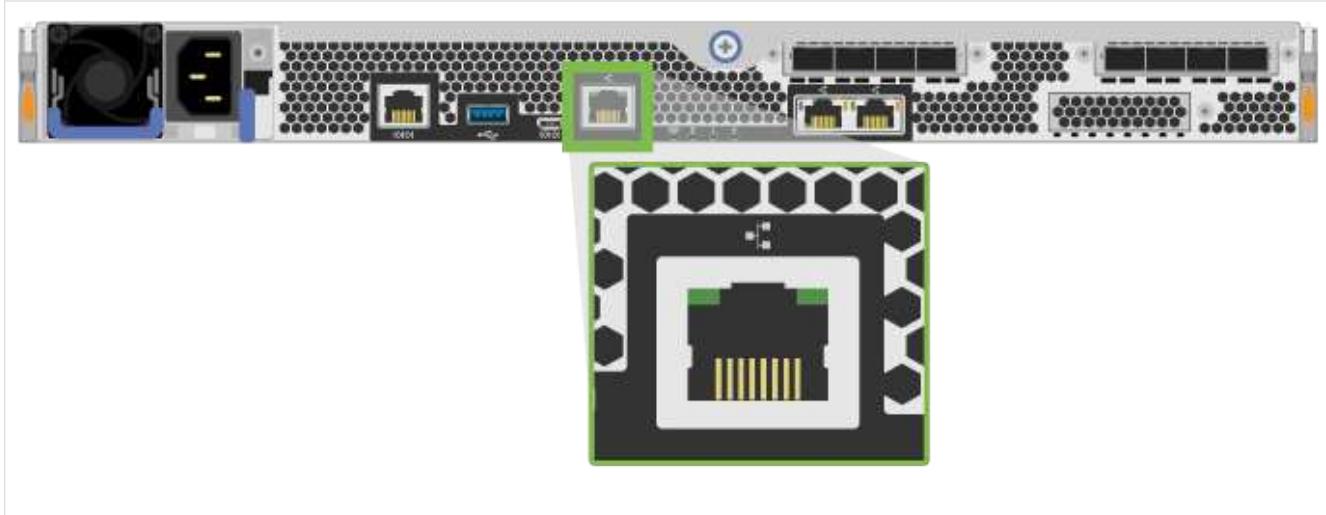
1. Using an Ethernet cable, connect controller A's management port to the Ethernet port on a laptop.



Controller A is the upper controller canister, and controller B is the lower controller canister.

| | |
|---|------------------------------------|
|  | RJ-45 Ethernet cables (if ordered) |
|---|------------------------------------|

The following figure shows an example of the controller's management port location (EF600 shown):



2. Open a browser and use the default IP address (169.254.128.101) to establish a connection to the controller. The controller sends back a self-signed certificate. The browser informs you that the connection is not secure.
3. Follow the browser's instructions to proceed and launch SANtricity System Manager.



If you are unable to establish a connection, verify that you are not receiving network configuration from a DHCP server.

4. Set the storage system's password to login.
5. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller A's network settings, and then select **Finish**.



Because you reset the IP address, System Manager loses connection to the controller.

6. Disconnect your laptop from the storage system, and connect the management port on controller A to your network.
7. Open a browser on a computer connected to your network, and enter controller A's newly configured IP address.



If you lose the connection to controller A, you can connect an ethernet cable to controller B to reestablish connection to controller A through controller B (169.254.128.102).

8. Log in using the password you set previously.

The Configure Network Settings wizard will appear.

9. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller B's network settings, and then select **Finish**.
10. Connect controller B to your network.
11. Validate controller B's network settings by entering controller B's configured IP address in a browser.



If you lose the connection to controller B, you can use your previously validated connection to controller A to reestablish connection to controller B through controller A.

Step 3: Configure storage system

After you have installed the EF300 or EF600 hardware, use the SANtricity software to configure and manage your storage system.

Before You Begin

- Configure your management ports.
- Verify and record your password and IP addresses.

Steps

1. Connect your controller to a web browser.
2. Use SANtricity System Manager to manage your EF300 or EF600 series storage system. Refer to the online help included with System Manager.

| | |
|---|---|
|  | For accessing System Manager, use the same IP addresses that you used to configure your management ports. |
|---|---|

If you are cabling your EF300 for SAS expansion, see [Maintaining EF600 Hardware](#) for SAS expansion card installation and the [Cabling E-Series hardware](#) for SAS expansion cabling.

E2800 and E5700

Install and set up E2800 and E5700 storage systems

Learn how to install and set up the E2800 or E5700 storage system.

You can choose one of the following formats to guide you through installing and setting up your new storage system.

- **PDF**

This is a printable PDF of step-by-step instructions with live links to additional content. Choose one of the following posters to get started.

- [E2860, E5760 and DE460C PDF poster](#)
- [E5724, EF570, EF280, E2812, E2824, DE212C, and DE224C PDF poster](#)

- **Online instructions**

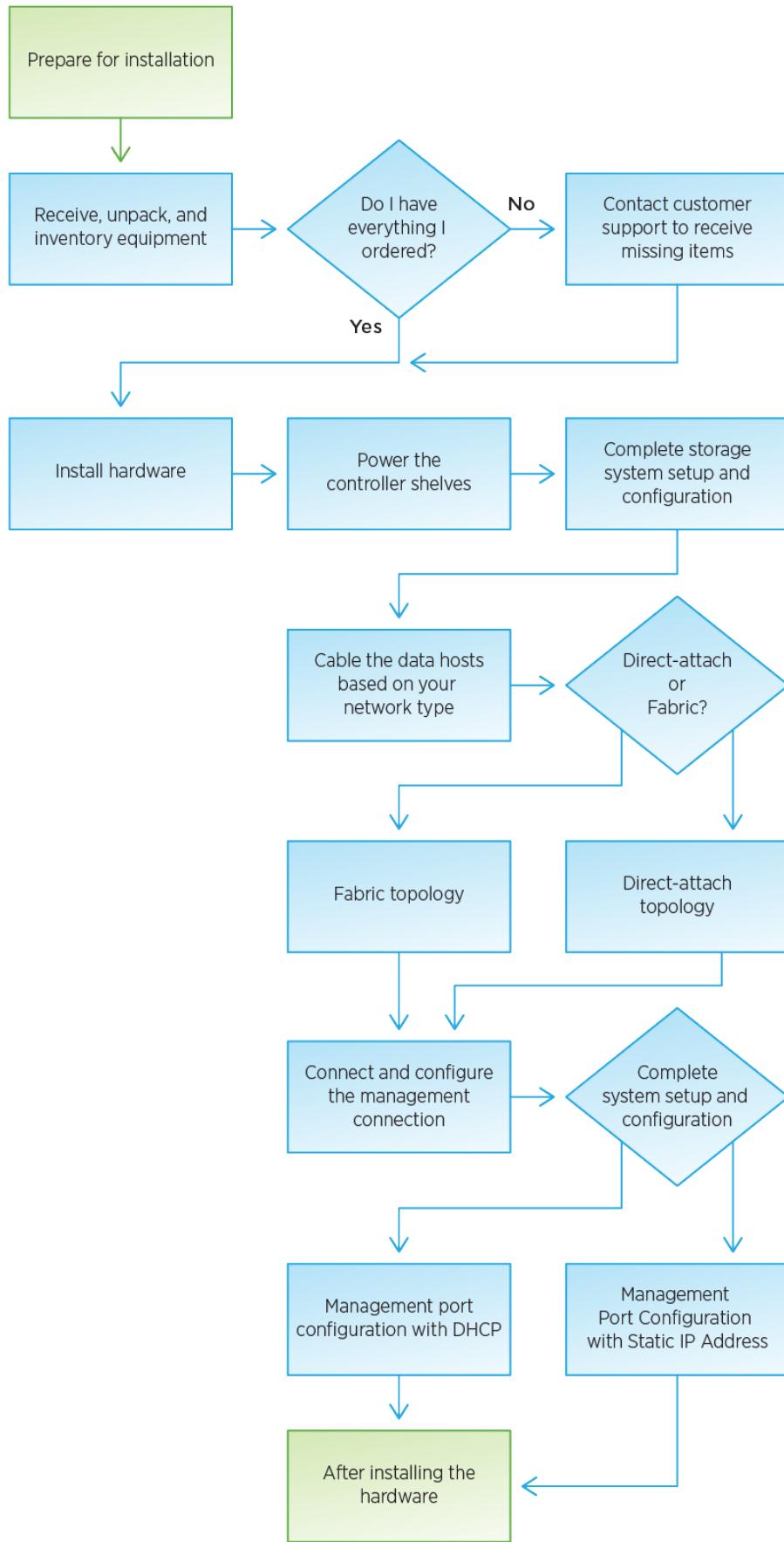
These are the setup instructions described on this site. Start with one of the following topics to get started.

- [Prepare to install E2860, E5760 and DE460C](#)

- Prepare to install E5724, EF570, EF280, E2812, E2824, DE212C, and DE224C

Overview

Before you install and set up your new storage system, familiarize yourself with the installation process:



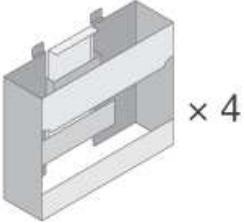
Install and set up 60-drives

Prepare for installation

Learn how to prepare to install your E2860, E5760, or DE460 series storage system.

Steps

1. Create an account and register your hardware at mysupport.netapp.com.
2. Ensure that the following items are in the box that you received.

| | |
|--|--------------------------------------|
|  | Shelf, bezel, and rackmount hardware |
|  × 4 | Shelf handles x4 |

The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see [Hardware Universe](#) to locate the cable and identify its use.

| Connector type | Cable type | Use |
|---|---------------------------------|------------------------|
|  | Ethernet cables (if ordered) | Management connection |
|  | I/O cables (if ordered) | Cabling the data hosts |

| Connector type | Cable type | Use |
|---|---|--------------------------------|
|  | Power cables x2 per shelf (if ordered) | Powering up the storage system |
|  | SAS cables (Included only with the drive shelves) | Cabling the shelves |

3. Ensure that you provide the following items.

| | |
|---|-------------------------|
|  | Phillips #2 screwdriver |
|  | Flashlight |
|  | ESD strap |

| | |
|--|--|
|  | <p>4U rack space: A standard 19 in. (48.30 cm) rack to fit 4U shelves of the following dimensions.</p> <p>Depth: 38.25 in. (97.16 cm)</p> <p>Width: 17.66 in. (44.86 cm)</p> <p>Height: 6.87 in. (17.46 cm)</p> <p>Max Weight: 250 lb (113 kg)</p> |
|  | <p>A supported browser for the management software:</p> <ul style="list-style-type: none"> • Google Chrome (version 47 and later) • Microsoft Internet Explorer (version 11 and later) • Microsoft Edge (EdgeHTML 12 and later) • Mozilla Firefox (version 31 and later) • Safari (version 9 and later) |

Install the hardware

Learn how to install a E2860, E5760, or DE460 storage system in a two-post rack or a NetApp system cabinet.

Before you begin

- Register your hardware at mysupport.netapp.com.
- Prepare a flat, static-free work area.
- Obtain an ESD wristband and take anti-static precautions.

Read through all the instructions before proceeding with the steps below.

Steps

1. Unpack the hardware contents, and then inventory the contained hardware against the packing slip.
2. Install the rails.

If instructions were included with your rack-mounting hardware, refer to them to learn how to install the rails. For additional rack-mounting instructions, see [Rack-mount hardware](#).



For square hole cabinets, you must first install the provided cage nuts to secure the front and rear of the shelf with screws.

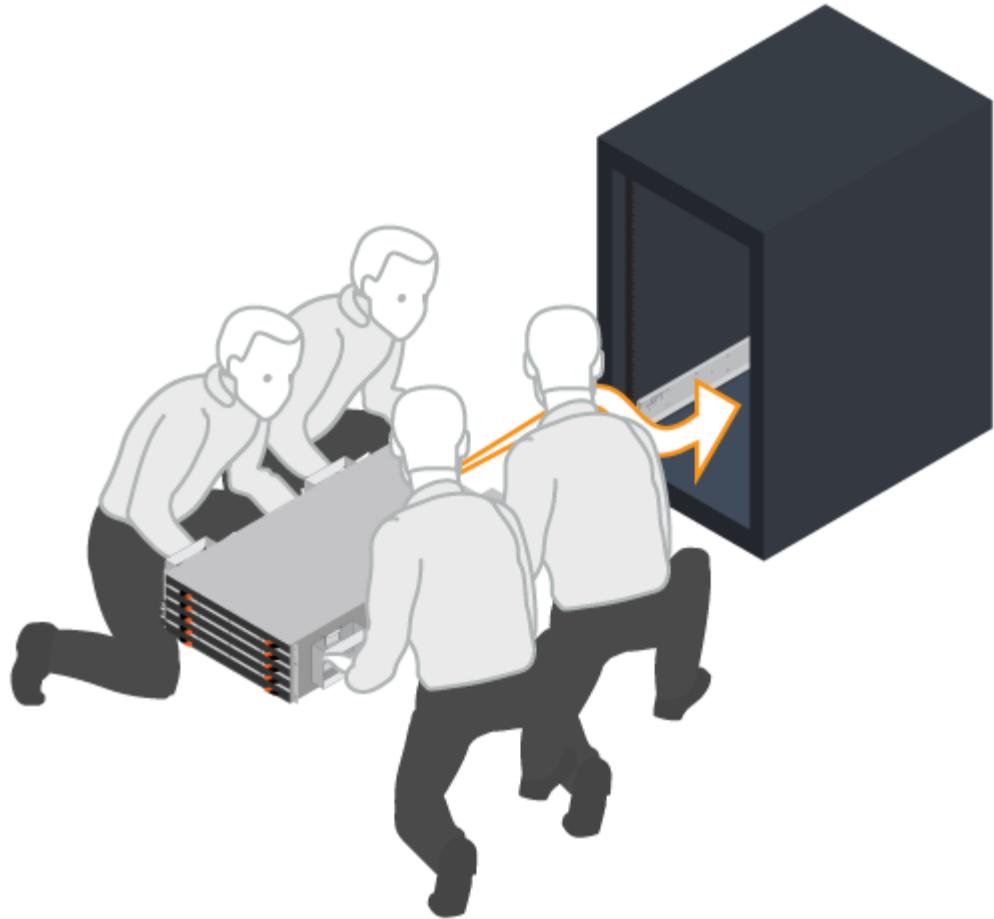


3. Install the shelf.

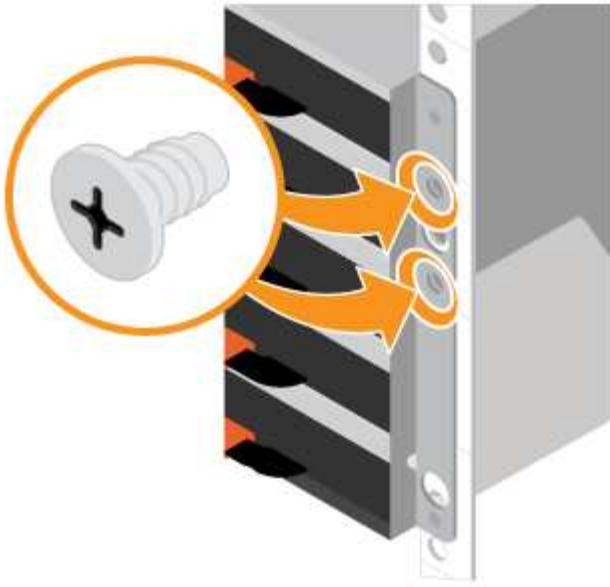


An empty shelf weighs approximately 132 lb (60 kg). A mechanized lift or four people using lift handles are required to safely move an empty shelf.

- a. If lifting the shelf by hand, attach the four lift handles. Push up on each handle until it clicks into place.
- b. Supporting the shelf from the bottom, slide it into the cabinet. If the lift handles are used, remove them one set at a time as the shelf slides into the cabinet. To remove the handles, pull back on the release latch, push down, then pull away from the shelf.



4. Secure the shelf.
 - a. Insert screws into the first and third holes from the top of the shelf on both sides to secure it to the front of the cabinet.
 - b. Place two back brackets on each side of the upper rear section of the shelf. Insert screws into the first and third holes of each bracket to secure the back of the cabinet.



5. Install the drives.

- a. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharges.
- b. Starting at the front left slot of the top drawer, install each drive by gently positioning into the drive slot and lowering the raised drive handle until it clicks into place.
 - If you are installing fewer than 60 drives, if you have solid-state drives (SSDs), or if your drives have different capacities:
 - Maintain a minimum of 20 drives per shelf. Install drives in the front four slots in each drawer first, for adequate airflow for cooling.
 - Distribute any remaining drives across the drawers. If possible, install an equal number of each type of drive in each drawer to allow for the creation of Drawer Loss Protected volume groups or disk pools.
 - Distribute any SSDs evenly across the drawers.
- c. Carefully slide the drawer back in by pushing the center and gently closing both latches.
 - Do not force the drawer into place.
 - Use the connector tool, disconnect the connector of the snake cable and reconnect it, make sure you hear a click to determine the reconnection is properly done.
 - Disconnection and reconnection should only be required during initial setup or if the tray is shipped to a different location.
- d. Attach the front bezel.



Risk of equipment damage — Stop pushing the drawer if you feel binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, carefully reinsert the drawer into the slot.

Cable the shelves

Learn how to attach the power cables and power on the drive shelves.

Before you begin

- Install your hardware.
- Take anti-static precautions.

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.)

Steps

1. Cable the shelves.

Cable the system according to your configuration. If you need more cabling options than the examples shown in this section, see [Cabling](#).

For the examples shown in this section, you need the following cables:

| | |
|---|-------------------|
|  | SAS cables |
|---|-------------------|

Example A: An E2860 controller shelf with two DE460C disk shelves in a standard SAS configuration.



- a. Cable controller A to IOM A of the first drive shelf.
- b. Cable IOM A of the first drive shelf to IOM A of the second drive shelf.
- c. Cable IOM B of the first drive shelf to IOM B of the second drive shelf.
- d. Cable controller B to IOM B of the second drive shelf.

Example B: An E2860 controller shelf with one DE460C disk shelf in a standard SAS configuration.



- a. Cable controller A to IOM A.
 - b. Cable controller B to IOM B.
2. Power the drive shelves.

You need the following cables:

|  | Power cables |
|---|--------------|
| | |



Confirm the drive shelf power switches are off.

- a. Connect the two power cables for each shelf to different power distribution units (PDUs) in the cabinet or rack.
- b. If you have drive shelves, turn on their two power switches first. Wait 2 minutes before applying power to the controller shelf.
- c. Turn on the two power switches on the controller shelf.
- d. Check the LEDs and seven-segment display on each controller.

During boot, the seven-segment display shows the repeating sequence of OS, Sd, blank to indicate the controller is performing start-of-day processing. After the controller has booted up, the shelf ID is displayed.

Example: Power connections are on the rear of the shelf.



Complete storage system setup and configuration

Learn how to cable the controllers to your network and complete storage system setup and configuration.

Step 1: Cable the data hosts

Cable the system according to your network topology.

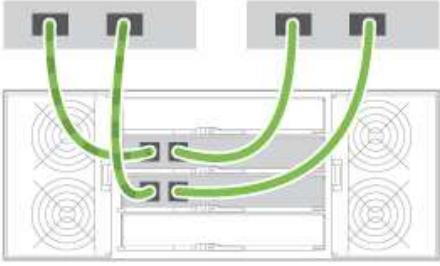


If you are using AIX®, you must install the E-Series multipath driver on the host before connecting it to the array.

Option 1: Direct-attach topology

The following example shows cabling to the data hosts using a direct-attach topology.

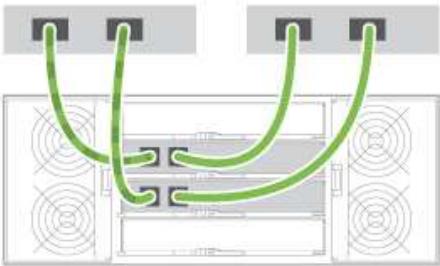
Table 3. Example A: Direct-attach topology

| | |
|---|---|
|  | <ol style="list-style-type: none"> 1. Connect each host adapter directly to the host ports on the controllers. |
|---|---|

Option 2: Fabric topology

The following example shows cabling to the data hosts using a fabric topology.

Table 4. Example B: Fabric topology

| | |
|---|---|
|  | <ol style="list-style-type: none"> 1. Connect each host adapter directly to the switch. 2. Connect each switch directly to the host ports on the controllers. |
|---|---|

Step 2: Connect and configure the management connection

You can configure the controller management ports using a DHCP server or a static IP address.

Option 1: DHCP server

Learn how to configure the management ports with a DHCP server.

Before you begin

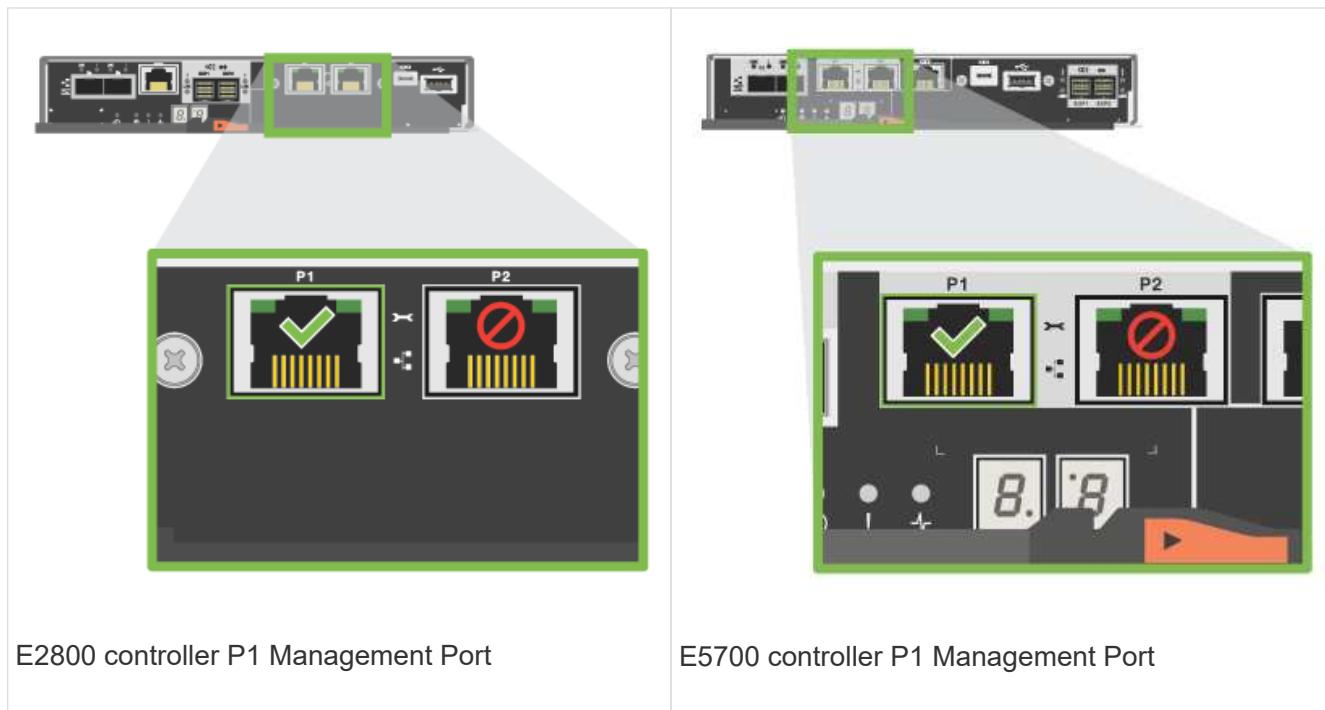
- Configure your DHCP server to associate an IP address, subnet mask, and gateway address as a permanent lease for each controller.
- Obtain the assigned IP addresses to connect to the storage system from your network administrator.

Steps

1. Connect an Ethernet cable to each controller's management port, and connect the other end to your network.

| | |
|---|------------------------------|
|  | Ethernet cables (if ordered) |
|---|------------------------------|

The following figures show examples of the controller's management port location:



- Open a browser and connect to the storage system using one of the controller IP addresses provided to you by your network administrator.

Option 2: Static IP address

Learn how to configure the management ports manually by entering the IP address and the subnet mask.

Before you begin

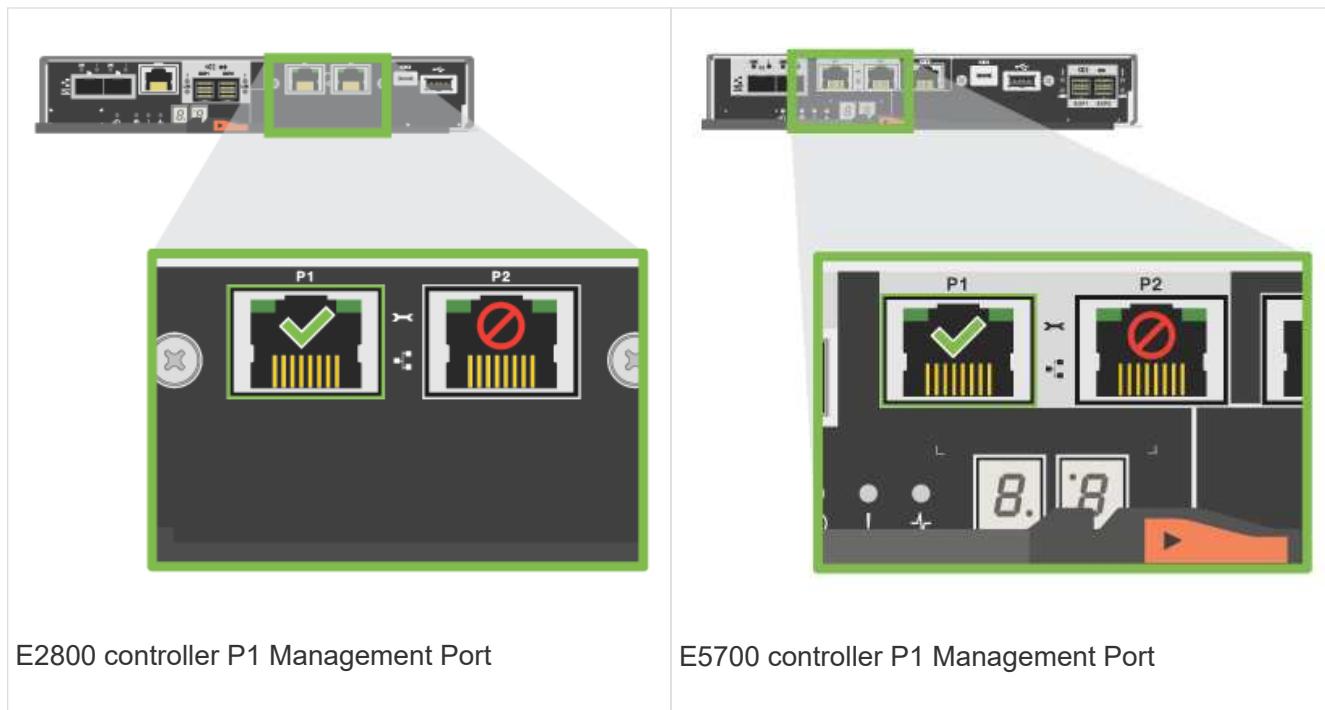
- Obtain the controllers' IP address, subnet mask, gateway address, and DNS and NTP server information from your network administrator.
- Make sure the laptop you are using is not receiving network configuration from a DHCP server.

Steps

- Using an Ethernet cable, connect controller A's management port to the Ethernet port on a laptop.

| | |
|---|------------------------------|
|  | Ethernet cables (if ordered) |
|---|------------------------------|

The following figures show examples of the controller's management port location:



2. Open a browser and use the default IP address (169.254.128.101) to establish a connection to the controller. The controller sends back a self-signed certificate. The browser informs you that the connection is not secure.
3. Follow the browser's instructions to proceed and launch SANtricity System Manager.



If you are unable to establish a connection, verify that you are not receiving network configuration from a DHCP server.

4. Set the storage system's password to login.
5. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller A's network settings, and then select **Finish**.



Because you reset the IP address, System Manager loses connection to the controller.

6. Disconnect your laptop from the storage system, and connect the management port on controller A to your network.
7. Open a browser on a computer connected to your network, and enter controller A's newly configured IP address.



If you lose the connection to controller A, you can connect an ethernet cable to controller B to reestablish connection to controller A through controller B (169.254.128.102).

8. Log in using the password you set previously.

The Configure Network Settings wizard will appear.

9. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller B's network settings, and then select **Finish**.
10. Connect controller B to your network.

11. Validate controller B's network settings by entering controller B's newly configured IP address in a browser.



If you lose the connection to controller B, you can use your previously validated connection to controller A to reestablish connection to controller B through controller A.

Step 3: Configure and manage your storage system

After you have installed your hardware, use the SANtricity software to configure and manage your storage system.

Before you begin

- Configure your management ports.
- Verify and record your password and IP addresses.

Steps

1. Use the SANtricity software to configure and manage your storage arrays.
2. In the simplest network configuration, connect your controller to a web browser and use SANtricity System Manager for managing a single E2800 or E5700 series storage array.



For accessing System Manager, use the same IP addresses that you used to configure your management ports.

Install and set up 12 and 24-drives

Prepare for installation

Learn how to prepare to install your E5724, EF570, EF280, E2812, E2824, DE212C, or DE224C series storage system.

Steps

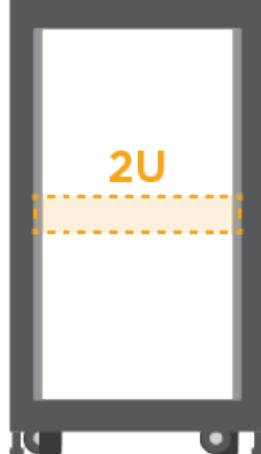
1. Create an account and register your hardware at mysupport.netapp.com.
2. Ensure that the following items are in the box that you received.

| | |
|---|---|
|  | Shelf with drives installed (bezel packaged separately) |
|  | Rack-mount hardware |

The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see [Hardware Universe](#) to locate the cable and identify its use.

| Connector type | Cable type | Use |
|---|---|--------------------------------|
|  | Ethernet cables (if ordered) | Management connection |
|  | I/O cables (if ordered) | Cabling the data hosts |
|  | Power cables (if ordered) | Powering up the storage system |
|  | SAS cables included only with the drive shelves | SAS cables |

3. Ensure that you provide the following items.

| | |
|---|--|
|  | Phillips #2 screwdriver |
|  | Flashlight |
|  | ESD strap |
|  | <p>2U rack space: A standard 19 in. (48.30 cm) rack to fit 2U shelves of the following dimensions.</p> <p>Depth: 19.0 in. (48.3 cm)</p> <p>Width: 17.6 in. (44.7 cm)</p> <p>Height: 3.34 in. (8.48 cm)</p> <p>Shelf: 24-drive</p> <p>Max Weight: 60.5 lb (27.4 kg)</p> |
|  | <p>A supported browser for the management software:</p> <ul style="list-style-type: none"> • Google Chrome (version 78 and later) • Microsoft Internet Explorer (version 11 and later) • Microsoft Edge (88 and later) • Mozilla Firefox (version 70 and later) • Safari (version 12 and later) |

Install the hardware

Learn how to install a E5724, EF570, EF280, E2812, E2824, DE212C, or DE224C storage system in a two-post rack or a NetApp system cabinet.

Before you begin

Before you install the hardware, make sure you do the following:

- Register your hardware at mysupport.netapp.com.
- Prepare a flat, static-free work area.
- Obtain an ESD wristband and take anti-static precautions.

Read through all the instructions before proceeding with the steps below.

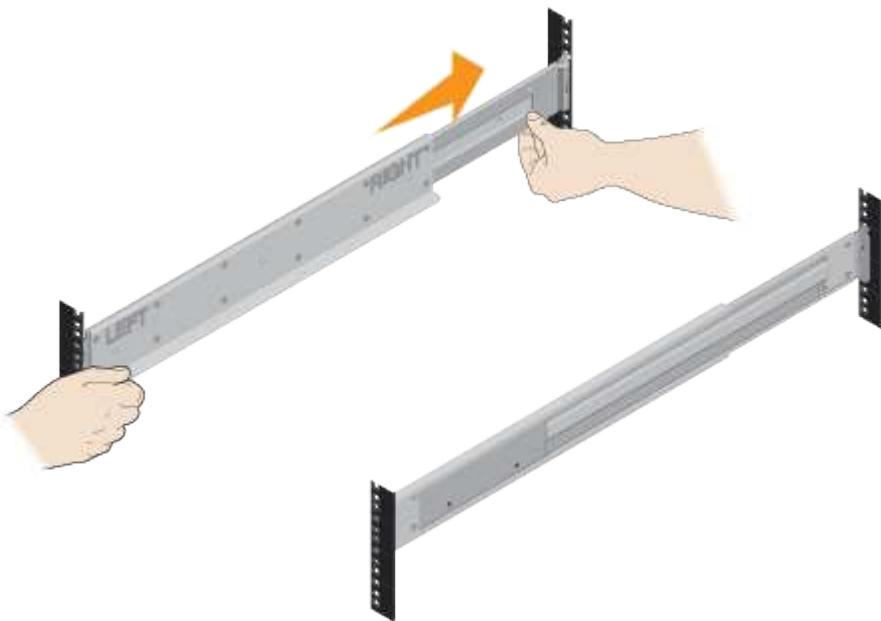
Steps

1. Unpack the hardware contents, and then inventory the contained hardware against the packing slip.
2. Install the rails.

If instructions were included with your rack-mounting hardware, refer to them for detailed information on how to install the rails. For additional rack-mounting instructions, see [Rack-mount hardware](#).



Install hardware from the bottom of the rack or cabinet up to the top to prevent the equipment from toppling over.



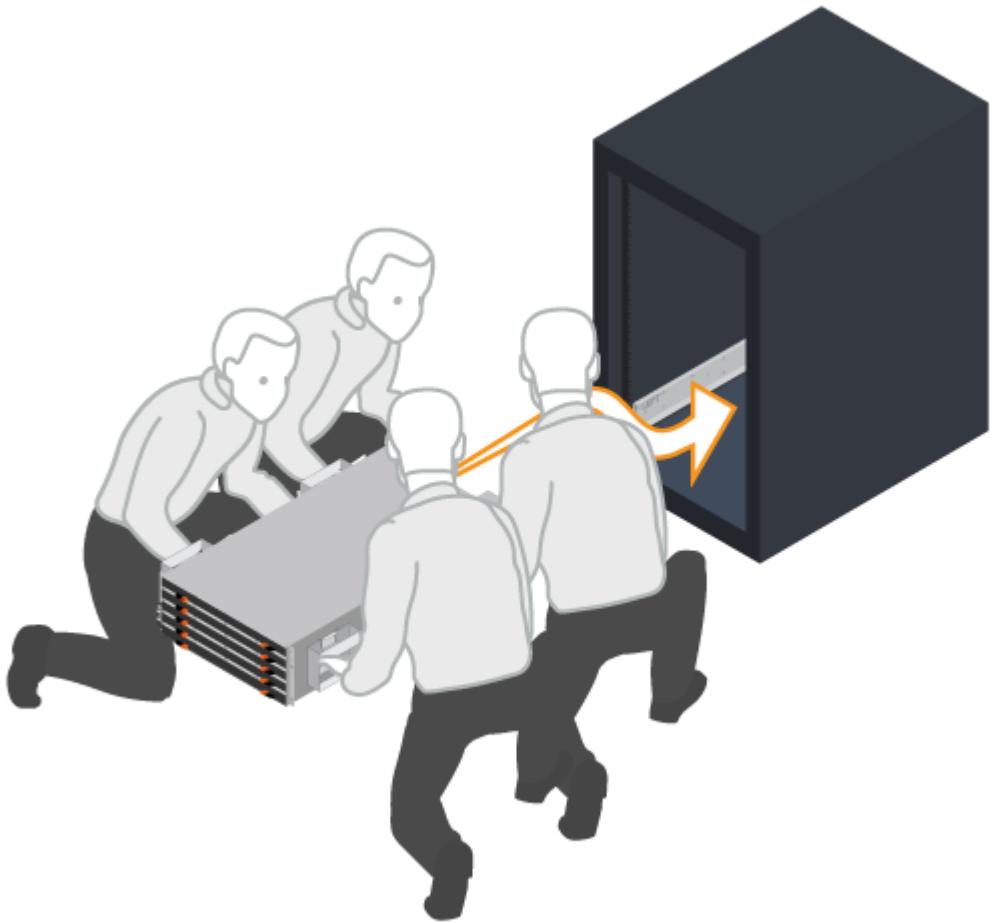
3. Install the shelf.



When fully loaded with drives, each shelf weighs approximately 64 lb (29 kg). Two persons or mechanical lift are required to safely move the shelf.

- a. Starting with the shelf you want at the bottom of the cabinet, place the back of the shelf (the end with the connectors) on the rails.

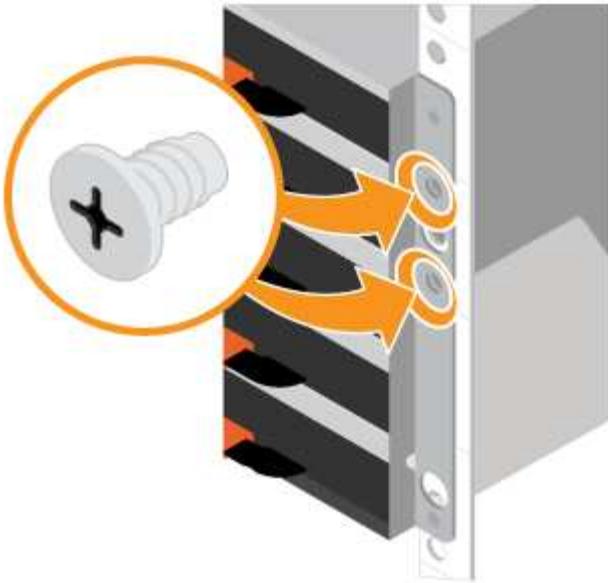
- b. Supporting the shelf from the bottom, slide it into the cabinet.



4. Secure the shelf.

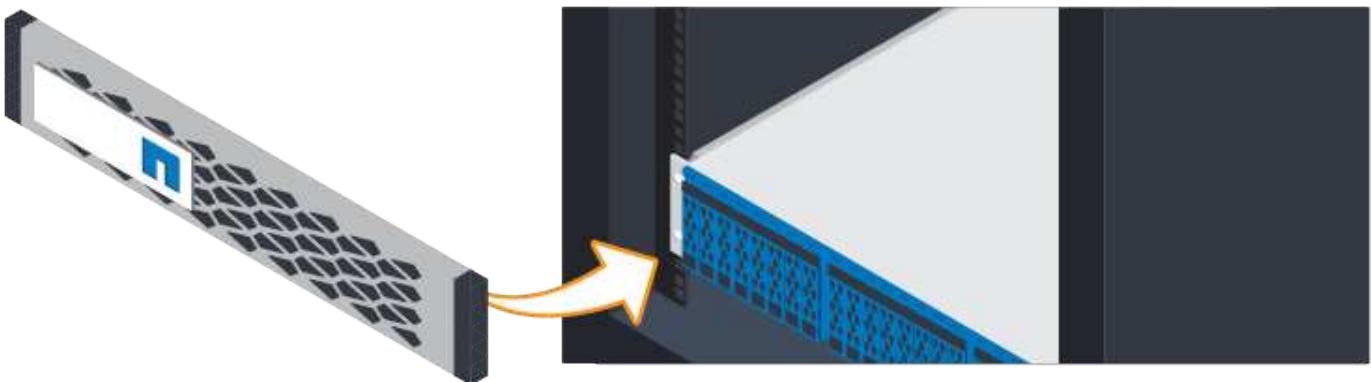
Secure the shelf to the rack as directed in [Rack-mount hardware](#).

- a. Insert screws into the first and third holes from the top of the shelf on both sides to secure it to the front of the cabinet.
- b. Place two back brackets on each side of the upper rear section of the shelf. Insert screws into the first and third holes of each bracket to secure the back of the cabinet.



5. Install the bezel or end caps.

- a. Position the front bezel in front of the controller shelf so that the holes at each end align with the fasteners on the controller shelf.
- b. Snap the bezel into place.
- c. If you have optional drive shelves, position the left end cap in front of the drive shelf so that the holes in the end cap align with the fasteners on the left side of the shelf.
- d. Snap the end cap into place.
- e. Repeat the above steps for the right end cap.



Connect the cables

Learn how to attach the power cables and power on the drive shelves.

Before you begin

- Install your hardware.
- Take anti-static precautions.

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.)

Steps

1. Cable the shelves.

Cable the system according to your configuration. If you need more cabling options than the examples shown, see [Cabling](#).

For the examples shown, you need the following cables:

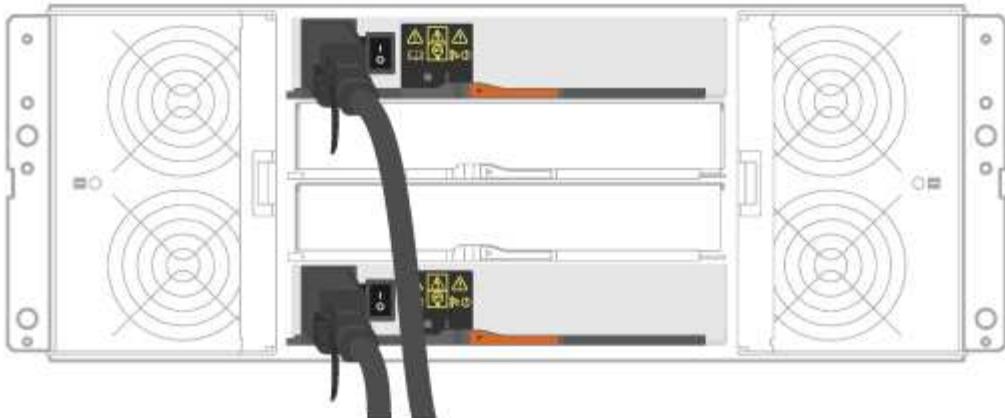
| SAS cables |
|---|
|  |

Example A: E5700 controller shelf with three DE212C/DE224 disk shelves in a standard SAS configuration.



- a. Cable controller A to IOM A of the first drive shelf.
- b. Cable IOM A of the first drive shelf to IOM A of the second drive shelf.
- c. Cable IOM A of the second drive shelf to IOM A of the third drive shelf.
- d. Cable controller B to IOM B of the third drive shelf.
- e. Cable IOM B of the second drive shelf to IOM B of the third drive shelf.
- f. Cable IOM B of the first drive shelf to IOM B of the second drive shelf.

Example B: An E5700 controller shelf with one DE212C/DE224 disk shelf in a standard SAS configuration.



- a. Cable controller A to IOM A.
 - b. Cable controller B to IOM B.
2. Power the drive shelves.

You need the following cables:

| | |
|--|---------------------|
|  | Power cables |
|--|---------------------|



Confirm the drive shelf power switches are off.

- a. Connect the two power cables for each shelf to different power distribution units (PDUs) in the cabinet or rack.
- b. If you have drive shelves, turn on their two power switches first. Wait 2 minutes before applying power to the controller shelf.
- c. Turn on the two power switches on the controller shelf.
- d. Check the LEDs and seven-segment display on each controller.

During boot, the seven-segment display shows the repeating sequence of OS, Sd, blank to indicate the controller is performing start-of-day processing. After the controller has booted up, the shelf ID is displayed.

Example: Power connections are on the rear of the shelf.



Complete storage system setup and configuration

Learn how to cable the controllers to your network and complete storage system setup and configuration.

Step 1: Cable the data hosts

Cable the system according to your network topology.



If you are using AIX®, you must install the E-Series multipath driver on the host before connecting it to the array.

Option 1: Direct-attach topology

The following example shows cabling to the data hosts using a direct-attach topology.

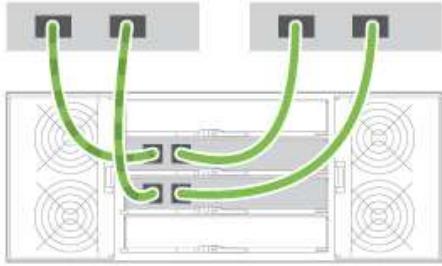
Table 5. Example A: Direct-attach topology

| | |
|--|---|
| A diagram showing two host adapters, each with two black ports, connected by green cables to two corresponding ports on a controller unit. The controller unit is shown from a rear perspective, featuring four circular fans and two black power supply units. The green cables are explicitly highlighted to show the connection path. | <ol style="list-style-type: none">1. Connect each host adapter directly to the host ports on the controllers. |
|--|---|

Option 2: Fabric topology

The following example shows cabling to the data hosts using a fabric topology.

Table 6. Example B: Fabric topology



1. Connect each host adapter directly to the switch.
2. Connect each switch directly to the host ports on the controllers.

Step 2: Connect and configure the management connection

You can configure the controller management ports using one of two options: using a DHCP server or using a static IP address.

Option 1: DHCP server

Learn how to configure the management ports with a DHCP server.

Before you begin

- Configure your DHCP server to associate an IP address, subnet mask, and gateway address as a permanent lease for each controller.
- Obtain the assigned IP addresses you will use to connect to the storage system from your network administrator.

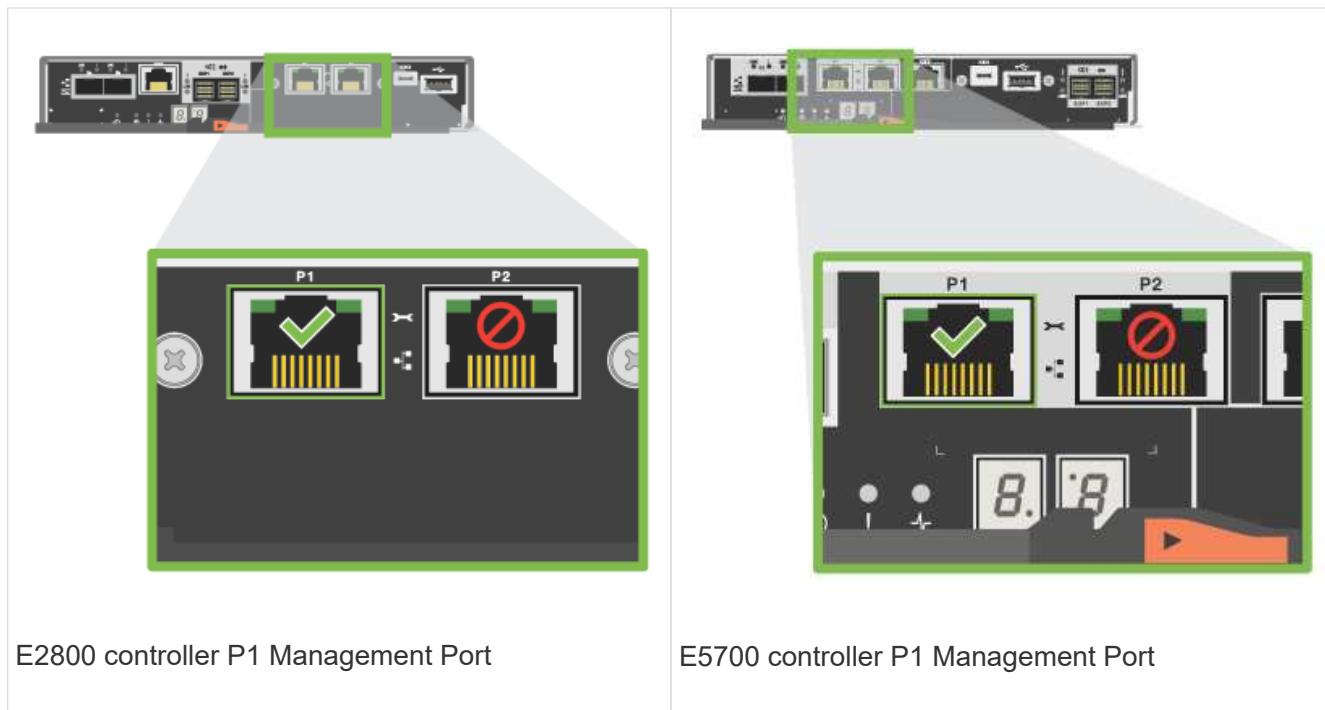
Steps

1. Connect an Ethernet cable to each controller's management port, and connect the other end to your network.



Ethernet cables (if ordered)

The following figures show examples of the controller's management port location:



2. Open a browser and connect to the storage system using one of the controller IP addresses provided to you by your network administrator.

Option 2: Static IP address

Learn how to configure the management ports manually by entering the IP address and the subnet mask.

Before you begin

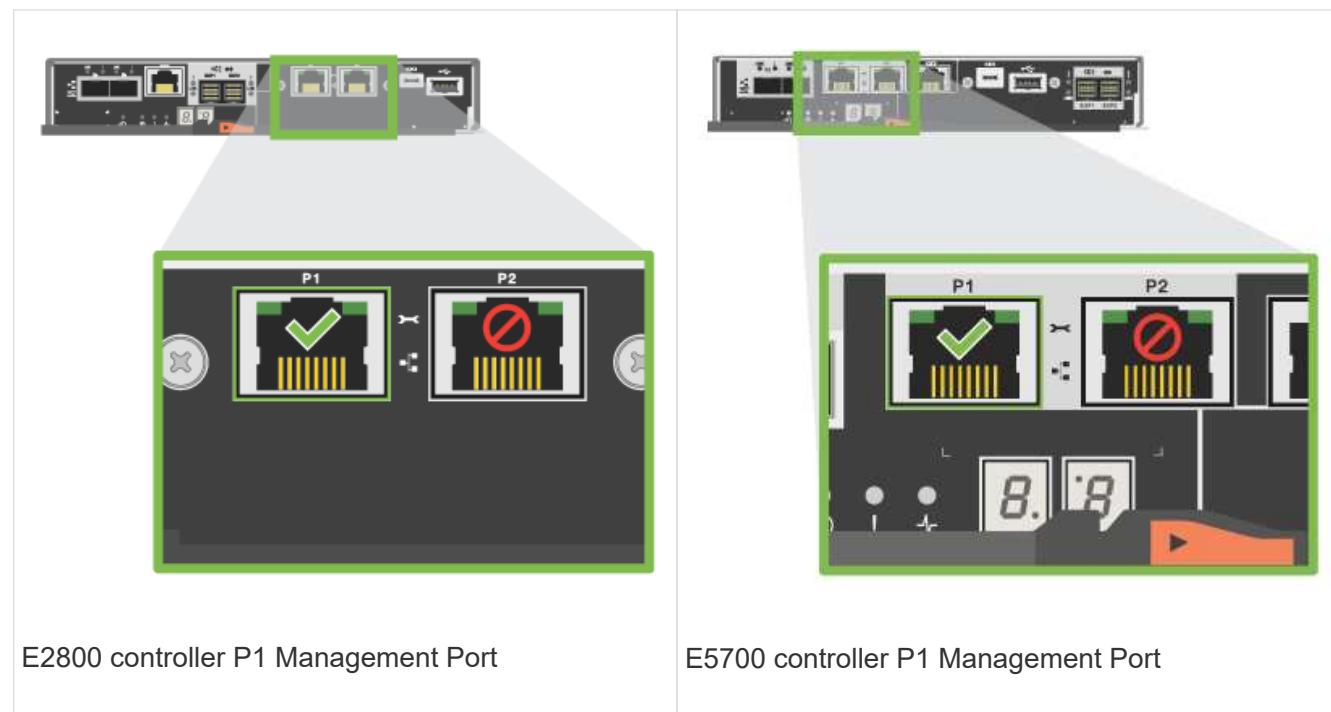
- Obtain the controllers' IP address, subnet mask, gateway address, and DNS and NTP server information from your network administrator.
- Make sure the laptop you are using is not receiving network configuration from a DHCP server.

Steps

1. Using an Ethernet cable, connect controller A's management port to the Ethernet port on a laptop.



The following figures show examples of the controller's management port location:



2. Open a browser and use the default IP address (169.254.128.101) to establish a connection to the controller. The controller sends back a self-signed certificate. The browser informs you that the connection is not secure.
3. Follow the browser's instructions to proceed and launch SANtricity System Manager.



If you are unable to establish a connection, verify that you are not receiving network configuration from a DHCP server.

4. Set the storage system's password to login.
5. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller A's network settings, and then select **Finish**.



Because you reset the IP address, System Manager loses connection to the controller.

6. Disconnect your laptop from the storage system, and connect the management port on controller A to your network.
7. Open a browser on a computer connected to your network, and enter controller A's newly configured IP address.



If you lose the connection to controller A, you can connect an ethernet cable to controller B to reestablish connection to controller A through controller B (169.254.128.102).

8. Log in using the password you set previously.

The Configure Network Settings wizard will appear.

9. Use the network settings provided by your network administrator in the **Configure Network Settings** wizard to configure controller B's network settings, and then select **Finish**.
10. Connect controller B to your network.

11. Validate controller B's network settings by entering controller B's newly configured IP address in a browser.



If you lose the connection to controller B, you can use your previously validated connection to controller A to reestablish connection to controller B through controller A.

Step 3: Configure storage system

After you have installed your hardware, use the SANtricity software to configure and manage your storage system.

Before you begin

- Configure your management ports.
- Verify and record your password and IP addresses.

Steps

1. Use the SANtricity software to configure and manage your storage arrays.
2. In the simplest network configuration, connect your controller to a web browser and use SANtricity System Manager for managing a single E2800 or E5700 series storage array.



For accessing System Manager, use the same IP addresses that you used to configure your management ports.

3040 40U cabinet

Install trays in the 3040 40U cabinet

You can install the following controller-drive trays and expansion drive trays in the E-Series 3040 40U cabinet:

- E2612, E2624, and E2660 controller-drive trays
- E2712, E2724, and E2760 controller-drive trays
- E5412, E5424, and E5460 controller-drive trays
- E5512, E5524, and E5560 controller-drive trays
- E5612, E5624, and E5660 controller-drive trays
- EF540, EF550, and EF560 flash arrays
- DE1600, DE5600, and DE6600 drive trays

You can also install the following SAS-3 controller shelves and drive shelves in the cabinet.

- E2812, E2824, and E5724 controller shelves
- DE212C and DE224C drive shelves

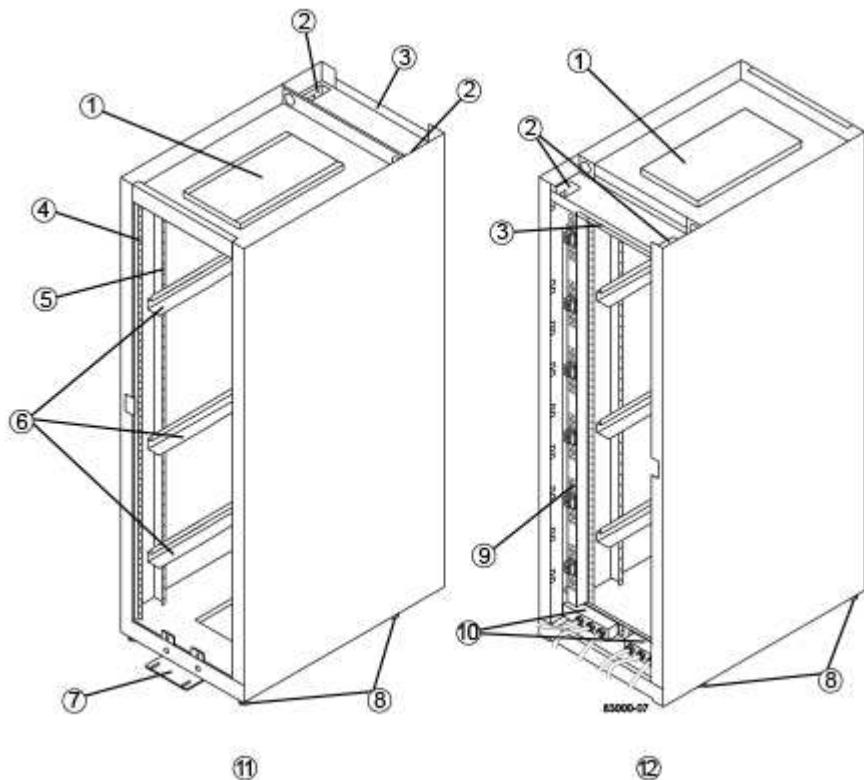
However, specifications for these shelves are not listed in these procedures. Refer to [NetApp Hardware Universe](#).

Cabinet specifications

The model 3040 40U cabinet has these standard features:

- A rear door that can be latched and locked
- Standard Electronic Industry Association (EIA) support rails that provide mounting holes for installing devices into a standard 48.3-cm (19-in.) wide cabinet
- Four roller casters and four adjustable leveling feet that are located beneath the cabinet for moving the cabinet and then leveling the cabinet in its final location
- A stability foot that stabilizes the cabinet after it is installed in its permanent location
- Access openings for interface cables
- Two AC power distribution units (PDUs) that provide integrated power connection and power handling capacity

The following figures show a front view (left) and a rear view (right) of the cabinet.



| | |
|----|---------------------------------|
| 1. | Ventilation cover |
| 2. | Interface cable access openings |

| | |
|-----|--------------------------------------|
| 3. | Rear plate |
| 4. | EIA support rails |
| 5. | Vertical support rails |
| 6. | Cabinet mounting rails |
| 7. | Stability foot |
| 8. | Adjustable leveling feet |
| 9. | Power distribution unit (one of two) |
| 10. | AC power entry boxes |
| 11. | Front of the cabinet |
| 12. | Rear of the cabinet |



Risk of bodily injury — If the bottom half of the cabinet is empty, do not install components in the top half of the cabinet. If the top half of the cabinet is too heavy for the bottom half, the cabinet might fall and cause bodily injury. Always install a component in the lowest available position in the cabinet.



Risk of bodily injury — Only move a populated cabinet with a forklift or adequate help from other persons. Always push the cabinet from the front to prevent it from falling over. A fully populated cabinet can weigh more than 2000 lb (909 kg). The cabinet is difficult to move, even on a flat surface. If you must move the cabinet along an inclined surface, remove the components from the top half of the cabinet, and make sure that you have adequate help.



You cannot install E2860 or E5760 controller shelves or a DE460C drive shelf into a 3040 40U cabinet.



If a 3040 cabinet is fully populated with DE6600 trays, it weighs more than 2756 lb (1250.1 kg).

Power requirements and heat dissipation

The cabinet includes the following specifications for power and heat dissipation.

Power rating

The 3040 40U cabinet is rated at 200 VAC to 240 VAC at 50 Hz to 60 Hz, and operates to ± 10 percent of that range.

Power distribution units (PDUs)

The cabinet includes two identical AC power distribution units (PDUs), with each PDU providing up to 72A of usable power. The PDUs are mounted vertically at the back of the cabinet, and each PDU includes six 12A power banks. Each power bank contains four IEC 60320-C19 power outlets and a 15A circuit breaker. Each PDU has a total of 24 outlets and 6 circuit breakers.

Each of the two PDUs has three power entry boxes, which are located at the bottom of the cabinet. Each power entry box provides power to eight of the power outlets, as follows:

- Power entry box 1, which has power cord C1, supplies power to the bottom eight outlets
- Power entry box 2, which has power cord C2, supplies power to the middle eight outlets
- Power entry box 3, which has power cord C3, supplies power to the top eight outlets

The power entry boxes are labeled C1, C2, and C3 where the power cords connect to the modules.

Power calculations and heat calculations for the cabinet

| Component | kVA | Watts | BTU/Hr |
|---|------------|--------------|---------------|
| Cabinet PDU (72A PDUs) | 14.4 | 14400 | 49176 |
| Cabinet PDU/12A bank (72A PDUs) | 2.40* | 2400* | 8196* |
| E2612 controller-drive tray | 0.437 | 433 | 1476 |
| E2624 controller-drive tray | 0.487 | 482 | 1644 |
| E2660 controller-drive tray | 1.128 | 1117 | 3810 |
| E2712 controller-drive tray | 0.516 | 511 | 1744 |
| E2724 controller-drive tray | 0.561 | 555 | 1894 |
| E2760 controller-drive tray | 1.205 | 1193 | 4072 |
| E5412 controller-drive tray | 0.558 | 552 | 1883 |
| E5424 controller-drive tray and the EF540 flash array | 0.607 | 601 | 2051 |

| Component | kVA | Watts | BTU/Hr |
|---|------------|--------------|---------------|
| E5460 controller-drive tray | 1.254 | 1242 | 4237 |
| E5512 controller-drive tray | 0.587 | 581 | 1982 |
| E5524 controller-drive tray and the EF550 flash array | 0.637 | 630 | 2150 |
| E5560 controller-drive tray | 1.285 | 1272 | 4342 |
| E5612 controller-drive tray | 0.625 | 619 | 2111 |
| E5624 controller-drive tray and the EF560 flash array | 0.675 | 668 | 2279 |
| E5660 controller-drive tray | 1.325 | 1312 | 4477 |
| DE1600 drive tray | 0.325 | 322 | 1099 |
| DE5600 drive tray | 0.375 | 371 | 1267 |
| DE6600 drive tray | 0.1.011 | 1001 | 3415 |

Maximum number of trays

The maximum number of trays that you can install in a 3040 40U cabinet depends on the height of each tray in rack units (U).

Tray heights in rack units (U)

Each rack unit is 1.75 inches (4.45 cm). For example, you can install up to ten 4U trays, up to twenty 2U trays, or a combination of 2U and 4U trays, up to 40U.

| Tray | Rack units (U) |
|--------------------------------------|-----------------------|
| E2x12 or E2x24 controller-drive tray | 2U |
| E2x60 controller-drive tray | 4U |
| E5x12 or E5x24 controller-drive tray | 2U |

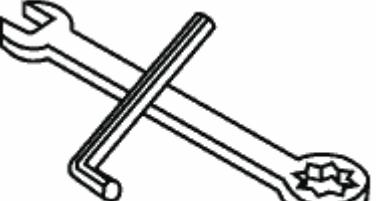
| Tray | Rack units (U) |
|-----------------------------|----------------|
| E5x60 controller-drive tray | 4U |
| EF5x0 Flash Array | 2U |
| DE1600 drive tray | 2U |
| DE5600 drive tray | 2U |
| DE6600 drive tray | 4U |

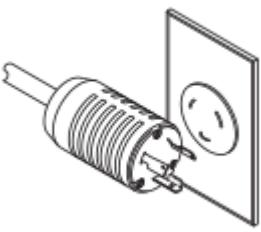
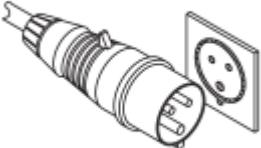
Gather required tools and equipment

Before installing the 3040 40U cabinet, make sure you have required tools and equipment.

Step

1. Gather all items listed in the following table.

| | Item | Included with the cabinet |
|--|---|--|
|  83009-02 | <p>3/4-in. wrench (supplied in the shipping crate) — To raise and lower the leveling feet under the cabinet.</p> <p>1/4-in. Allen wrench — To raise and lower the stability foot in the front of the cabinet.</p> |  |

| Item | Included with the cabinet |
|--|--|
| NEMA L6-30  | <p>AC power cords — To connect the cabinet to external power sources (wall plugs).</p> <ul style="list-style-type: none"> The NEMA L6-30 connectors are for use in the USA and Canada. The IEC-60309 connectors are for use worldwide, except for USA and Canada. |
| IEC-60309  | <p>Each PDU must be connected to an independent power source.</p> |
|  | <p>SAS cables (optional) – Two cables are included with each drive tray, while host side cables must be purchased separately.</p> <p>Communication cables (optional) – To attach the tray to the host.</p> <p>Refer to the appropriate controller-drive tray installation guide for additional required items.</p> |
|  | <p>Mountable cable spools – Installed along both sides of the vertical power distribution outlets to accommodate excess cable length and cable routing. Two cable spools are included with each controller-drive tray. Cable spools are also shipped with standalone drive trays.</p> |
| | <p>Shears – To cut the metal bands on the shipping crate.</p> |

| | Item | Included with the cabinet |
|--|---|---------------------------|
| | Forklift (optional) – To remove the cabinet from the shipping pallet. | |
| | Front panel kits (optional) – To cover the empty bays at the front of the cabinet. | |
| | Antistatic bags (optional) – To protect components that are removed during the installation procedure for the cabinet. | |

Prepare to move cabinet

Prepare to move the cabinet from its location in your receiving area by estimating its total weight, acclimating the cabinet, removing the packing materials, and checking the shipping contents.

Step 1: Estimate cabinet weight

The cabinet reliably and safely transports up to 909.1 kg (2000 lb) of capacity. You need to know the approximate weight of the cabinet so that you can safely move it.

Steps

1. Use the following table to calculate the approximate total weight of your cabinet.

The total weight of the cabinet depends on the number and type of trays that are installed in the cabinet.

| Component | Weight | Notes |
|--|----------------------|------------------------------------|
| Cabinet | 138.80 kg (306.0 lb) | Empty with the rear door installed |
| Power distribution units (PDUs) [pair] | 19.96 kg (44.0 lb) | |
| Mounting rails (pair) | 1.59 kg (3.50 lb) | |
| E2612 controller-drive tray | 27 kg (59.52 lb) | Maximum configuration |
| E2624 controller-drive tray | 26.12 kg (57.32 lb) | Maximum configuration |
| E2660 controller-drive tray | 105.2 kg (232 lb) | Maximum configuration |
| E2712 controller-drive tray | 27.12 kg (59.8 lb) | Maximum configuration |

| Component | Weight | Notes |
|-----------------------------|----------------------|-----------------------|
| E2724 controller-drive tray | 26 kg (57.32 lb) | Maximum configuration |
| E2760 controller-drive tray | 105.2 kg (232 lb) | Maximum configuration |
| E5412 controller-drive tray | 27.92 (61.52 lb) | Maximum configuration |
| E5424 controller-drive tray | 26.92 kg (59.32 lb) | Maximum configuration |
| E5460 controller-drive tray | 105.2 kg (232 lb) | Maximum configuration |
| E5512 controller-drive tray | 28.89 kg (63.7 lb) | Maximum configuration |
| E5524 controller-drive tray | 27.9 kg (61.52 lb) | Maximum configuration |
| E5560 controller-drive tray | 107.13 kg (236.2 lb) | Maximum configuration |
| E5612 controller-drive tray | 28.89 kg (63.7 lb) | Maximum configuration |
| E5624 controller-drive tray | 27.9 kg (61.52 lb) | Maximum configuration |
| E5660 controller-drive tray | 107.13 kg (236.2 lb) | Maximum configuration |
| EF540 flash array | 23.64 kg (52.12 lb) | Maximum configuration |
| EF550 flash array | 24.63 kg (54.32 lb) | Maximum configuration |
| EF560 flash array | 24.63 kg (54.32 lb) | Maximum configuration |
| DE1600 drive tray | 26.3 kg (58 lb) | Maximum configuration |
| DE5600 drive tray | 25.31 kg (55.8 lb) | Maximum configuration |
| DE6600 drive tray | 104.1 kg (229.6 lb) | Maximum configuration |

2. Review the following notes.



Remove all drives from the DE6600 drive tray before moving the cabinet to its final position.



Possible equipment damage — Cabinets with DE6600 drive trays ship without drives to reduce shipping weight. Because a fully-populated cabinet with DE6600 drive trays can weigh more than 1247.3 kg (2750 lb), make sure that you move the cabinet into place before you load the drives, and make sure that the floor load capability of the cabinet's destination supports that much weight.



Possible damage to tray components — Do not place a DE6600 drive tray on a flat surface. Install the DE6600 drive tray in the cabinet before operating or moving drawers.

Step 2: Acclimate cabinet

Make sure that the cabinet and the trays are acclimated to the indoor environment before removing the packing materials.

Steps

1. If the outdoor temperature is below 0°C (32°F), leave the cabinet and trays inside of their crates indoors for at least 24 hours to prevent condensation.
2. Increase or decrease the 24-hour stabilization period depending on the outside temperature upon arrival.



Possible damage to tray components — If the outdoor temperature is below 0°C (32°F) when you receive your cabinet and trays, do not immediately unpack them or uncrate them. Exposing cold components to warm indoor temperatures can cause condensation, which results in component damage or failures.

Step 3: Remove packing materials

Remove the packing materials only after the cabinet has acclimated to the indoor temperature.

Steps

1. Refer to the unpacking instructions included on the front of the shipping crate.
2. Remove the packing materials according to the enclosed instructions.

Step 4: Check shipping contents

Check the shipping contents to make sure that all equipment arrived at the site.

Steps

1. Compare the packing list with the equipment that you received.
2. Make sure that all equipment arrived at the site.
3. If any items are missing, contact your sales representative.

Step 5: Remove heavy components from cabinet

Remove some of the heavier components that are located in the top of the cabinet to ensure maximum stability.

Before you begin

- Make sure the maximum weight does not exceed 2000 lbs before you move the cabinet.
- Note the location of each tray, component, and cable before removing it, so that you can reinstall each item in its original location.

Steps

1. Record the cable configuration for future reassembly if any cables must be disconnected.
2. Remove the drive trays and controller-drive trays in the top half of the cabinet. Keep all of the components

from the same tray together.



You do not need to remove the power supplies or other components from the rear of each tray.

3. Place each component in a separate antistatic bag. If the original shipping boxes are available, use them to transport the components.

Move cabinet to its permanent location

The 3040 40U cabinet has heavy-duty casters that enable you to move the cabinet to its permanent location.

Before you begin

- Review the instructions for rolling the cabinet off the pallet without the use of a forklift.

Shipping crates provide built-in ramps and instructions. Refer to the unpacking instructions included on the front of the shipping crate.

- Evaluate all of the ramps between the loading dock and the cabinet's final destination.

You must evaluate all ramps to make sure that the cabinet's center of gravity (when the cabinet is on a ramp and sitting at an angle) does not extend beyond the cabinet's footprint.

About this task

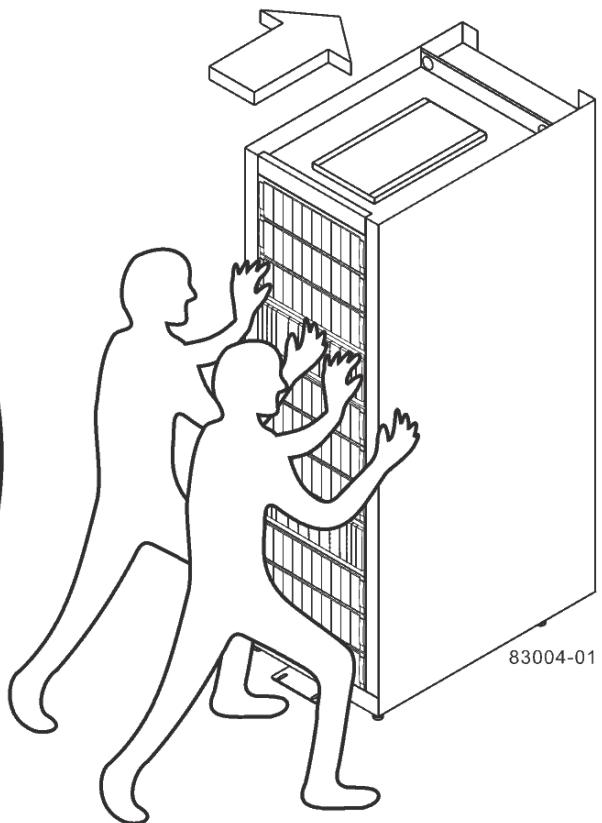
Many of the cabinets are populated with drive trays. This situation results in most of the weight in the front portion of the cabinet, making the center of gravity closer to the front.

Steps

1. Remove the top-most devices in your cabinet to make sure that the cabinet is safely transported to its final location. This is especially important if any ramp has an incline or a decline greater than 10 degrees.
2. Move the cabinet to its permanent location using the correct method shown in the following figure. Make sure that you push on the front of the cabinet, not the rear.



Rear of Cabinet



Front of Cabinet

83004-01

Complete cabinet installation

After you move the cabinet, lower the leveling feet and the stability foot, reinstall the components you removed, install other required components, and connect the cabinet to power.

Step 1: Lower leveling feet and stability foot

You stabilize the cabinet by adjusting its feet. The leveling feet support the cabinet off the casters. The stability foot prevents the cabinet from falling over after it is placed in its permanent location.

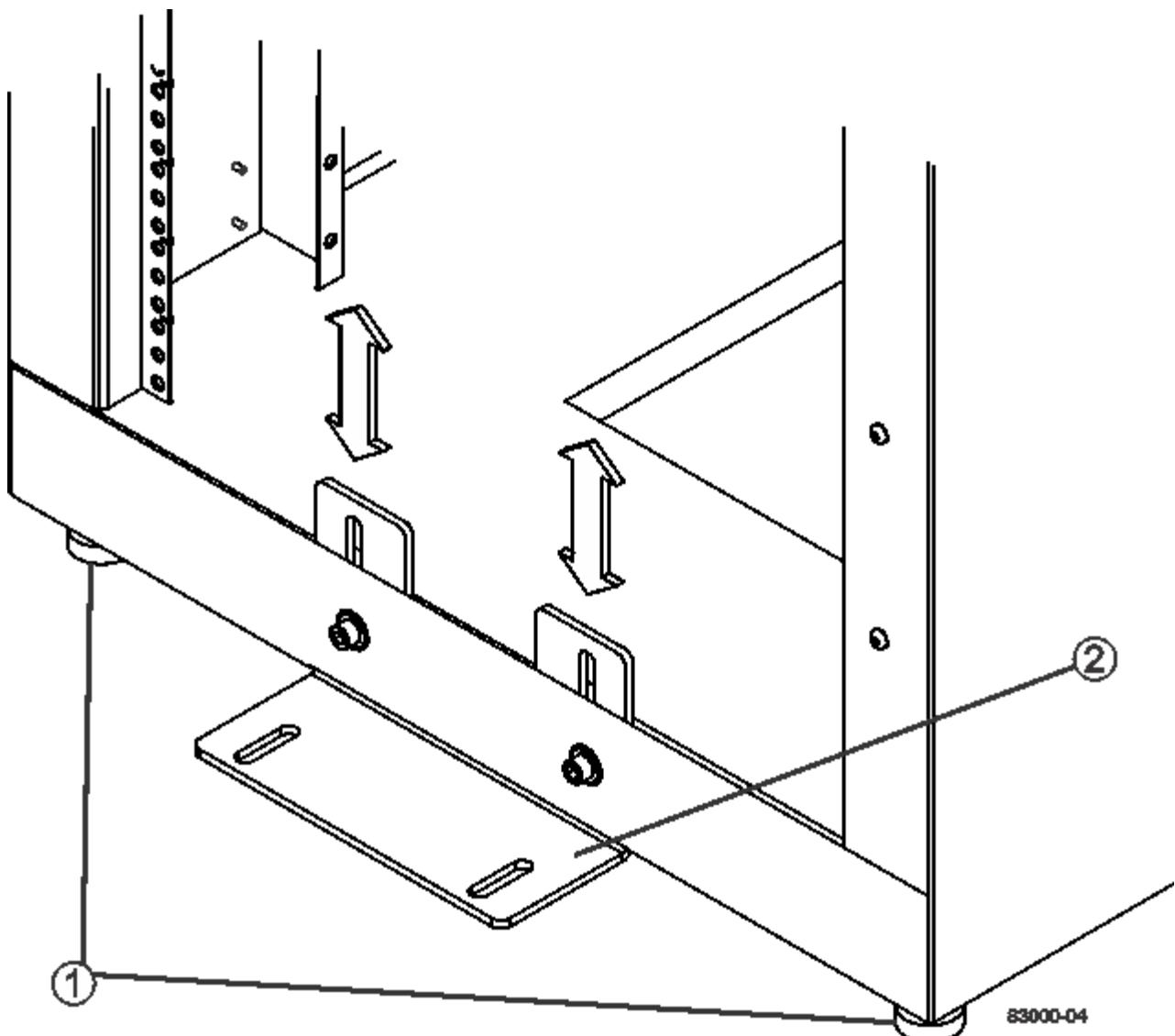
Steps

1. Lower the leveling feet to support the cabinet off the casters.

The leveling feet are located near each bottom corner of the cabinet.

2. Make sure that the cabinet is as level as possible.

The following figure provides a close-up view of the stability foot and the leveling feet.



| | |
|----|----------------|
| 1. | Leveling feet |
| 2. | Stability foot |

Step 2: Reinstall trays

After you move the cabinet, you can reinstall the trays in their original locations.

! *Do not install the following trays in the top of the cabinet over your head. When fully-populated, each of these trays weighs over 100 kg (220 lb). If installed in the top of the cabinet, these trays create a top-heavy cabinet that can become easily unbalanced: E2660, E2660, E2760, E5460, E5560, and E5660 controller-drive trays, as well as the DE6600 drive tray.*

Steps

1. Reinstall all of the trays in their original locations in the cabinet.



Risk of bodily injury—An empty tray weighs approximately 56.7 kg (125 lb). Three persons are required to safely move an empty tray. If the tray is populated with components, a mechanized lift is required to safely move the tray.

2. Reinstall all of the components in their original locations in the trays.

To prevent address conflicts and loss of data access, replace all components in the same tray and in the same location in the tray.

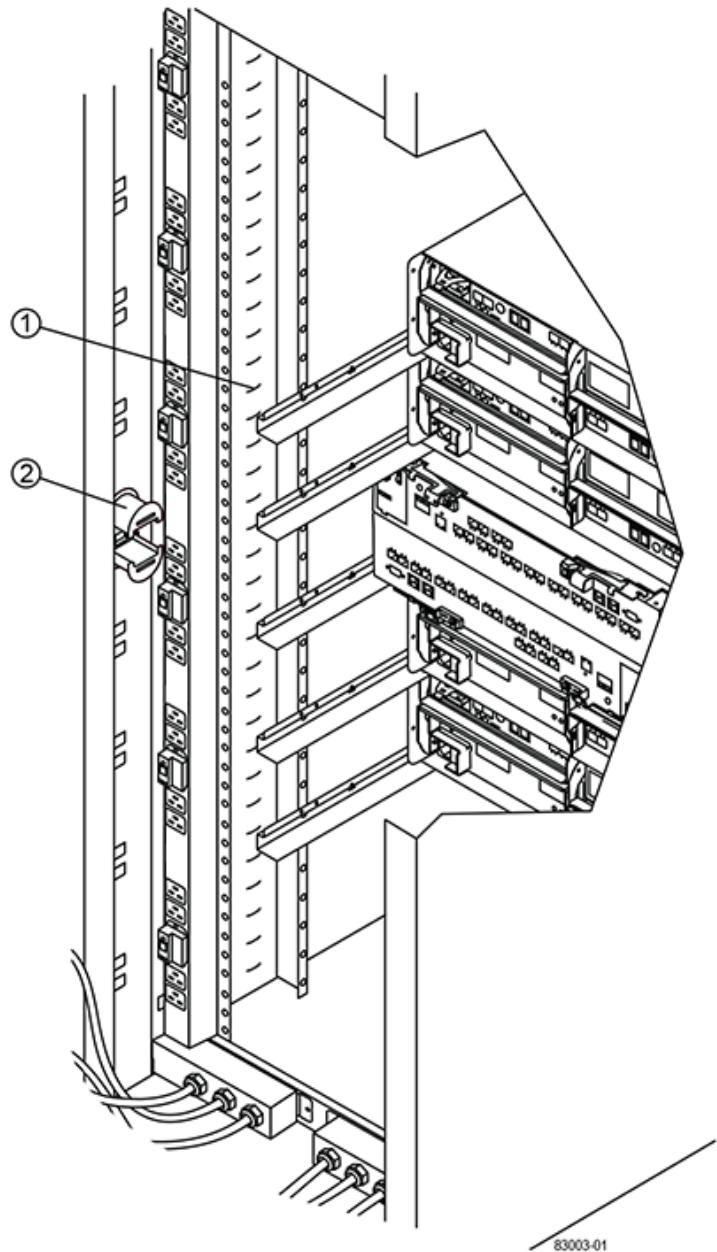
3. Reinstall all cables to their original locations in the trays.
4. Route the interface cables to the cabinet.
5. Route the main power cords from the cabinet to the two external power sources. *Do not* plug in the power cords at this time.

Step 3: Install cable spools and tie wraps

After you reinstall the trays, install the cable spools and tie wraps. The cable spools and tie wraps accommodate excess cable length and cable routing for the controllers and the trays.

Step

1. Install the cable spools and the tie wraps along both sides of the vertical power distribution outlets.



83003-01

| | |
|----|-------------------|
| 1. | Tie wrap location |
| 2. | Cable spool |

Step 4: Install additional trays

If needed, you can install additional trays. You must cover unused positions for trays to assure correct air flow.

Steps

1. If you have additional trays that must be installed, install the mounting hardware for these trays.
2. If the front of the cabinet is not completely filled with trays, use front panel kits to cover the empty spaces above or below the installed trays.

Covering the empty spaces is necessary so that the correct airflow through the cabinet is maintained.

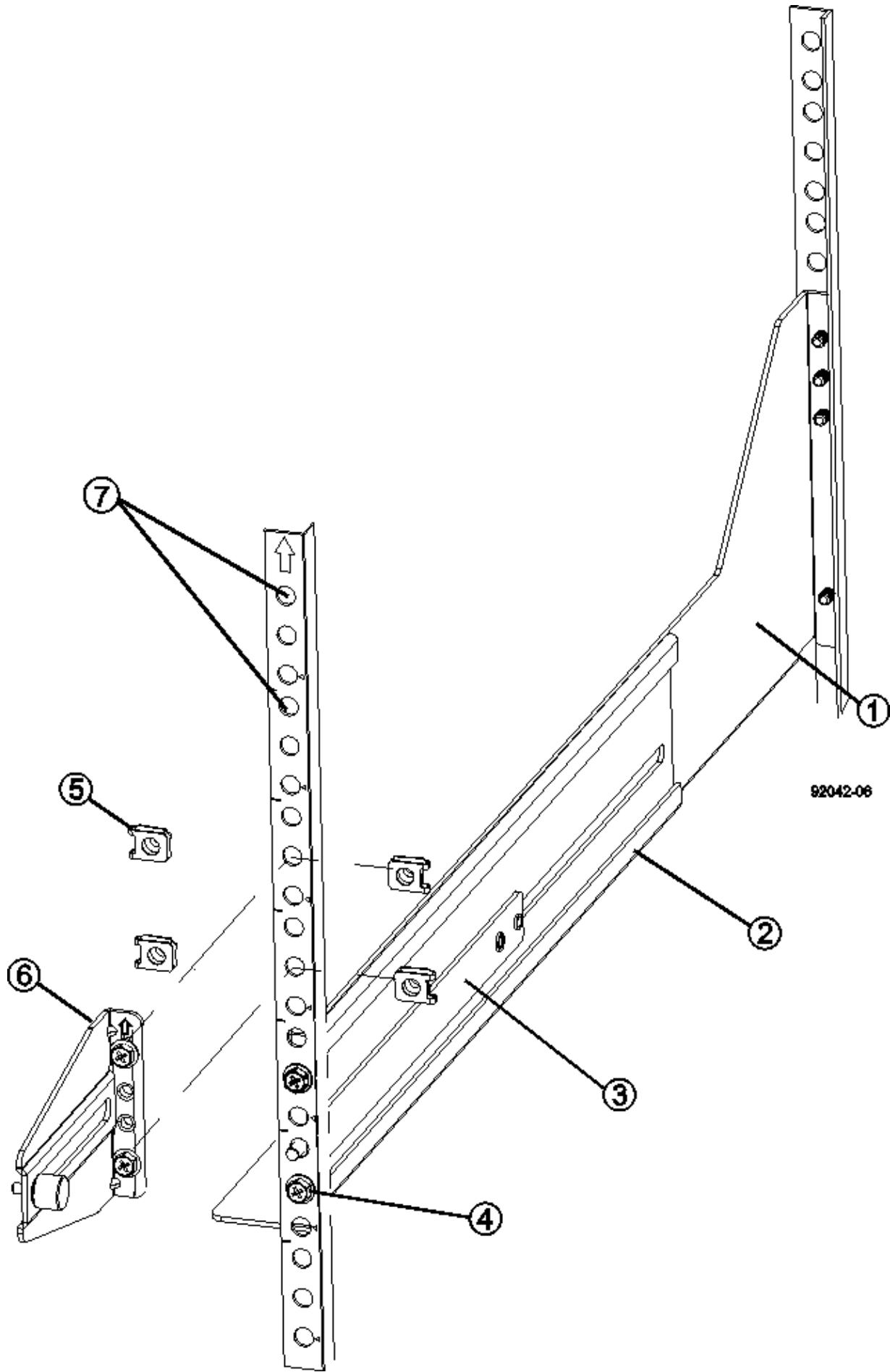
3. Power on the trays.

Step 5: Install additional mounting rails

If you are installing controller-drive trays, or drive trays that were shipped separately (not already installed in the cabinet), you might need to install additional mounting rails in the cabinet.

Steps

1. Determine the location for the mounting rails.
 - **Above an existing tray** — Position the mounting rails immediately above the top tray in the cabinet.
 - **Beneath an existing tray** — Position the mounting rails with enough clearance to hold the tray being installed:
 - 8.9 cm (3.5 in.) for 2U controller-drive trays or drive trays
 - 17.8 cm (7 in.) for 4U controller-drive trays or drive trays
2. Use the measurement markers on the right-front and left-front vertical supports to attach the mounting rails to the same position on each side of the cabinet.



| | |
|----|------------------------------|
| 1. | Front adjustable rail |
| 2. | Rear adjustable rail |
| 3. | Adjustment plate and screws |
| 4. | Rail mounting M5×10mm screws |
| 5. | Clip nuts |
| 6. | Rear hold down bracket |
| 7. | Vertical support |



The clip nuts and the rear hold down bracket are not used when the rails are installed in a 3040 cabinet.

3. Place the rear adjustable rail on the vertical support.
 4. On the rear adjustable rail, align the adjustable rail holes in front of the holes in the vertical support.
 5. Attach two M5×10mm screws.
 - a. Attach the screws through the vertical support rail and the rear adjustable rail.
 - b. Tighten the screws.
 6. Place the front adjustable rail on the vertical support.
 7. On the front adjustable rail, align the adjustable rail holes in front of the holes in the vertical support.
 8. Attach two M5×10mm screws.
 - a. Attach one screw through the vertical support rail and the bottom hole of the front adjustable rail.
 - b. Attach one screw through the vertical support rail and the middle of the top three holes in the front adjustable rail.
 - c. Tighten the screws.
- The remaining two screw holes are used to mount the tray.
9. Repeat step 3 through step 8 to attach the second rail on the other side of the cabinet.
 10. Install each tray using the applicable tray installation instructions.
 11. Choose one of the following options:
 - If all positions for trays are full, power-on the trays.
 - If not all positions for trays are full, use front panel kits to cover the empty spaces above or below the installed trays.

Step 6: Connect the cabinet to power

To complete the cabinet installation, power on the cabinet components.

About this task

While the trays perform the power-on procedure, the LEDs on the front and the rear of the trays blink. Depending on your configuration, it can take several minutes to complete the power-on procedure.

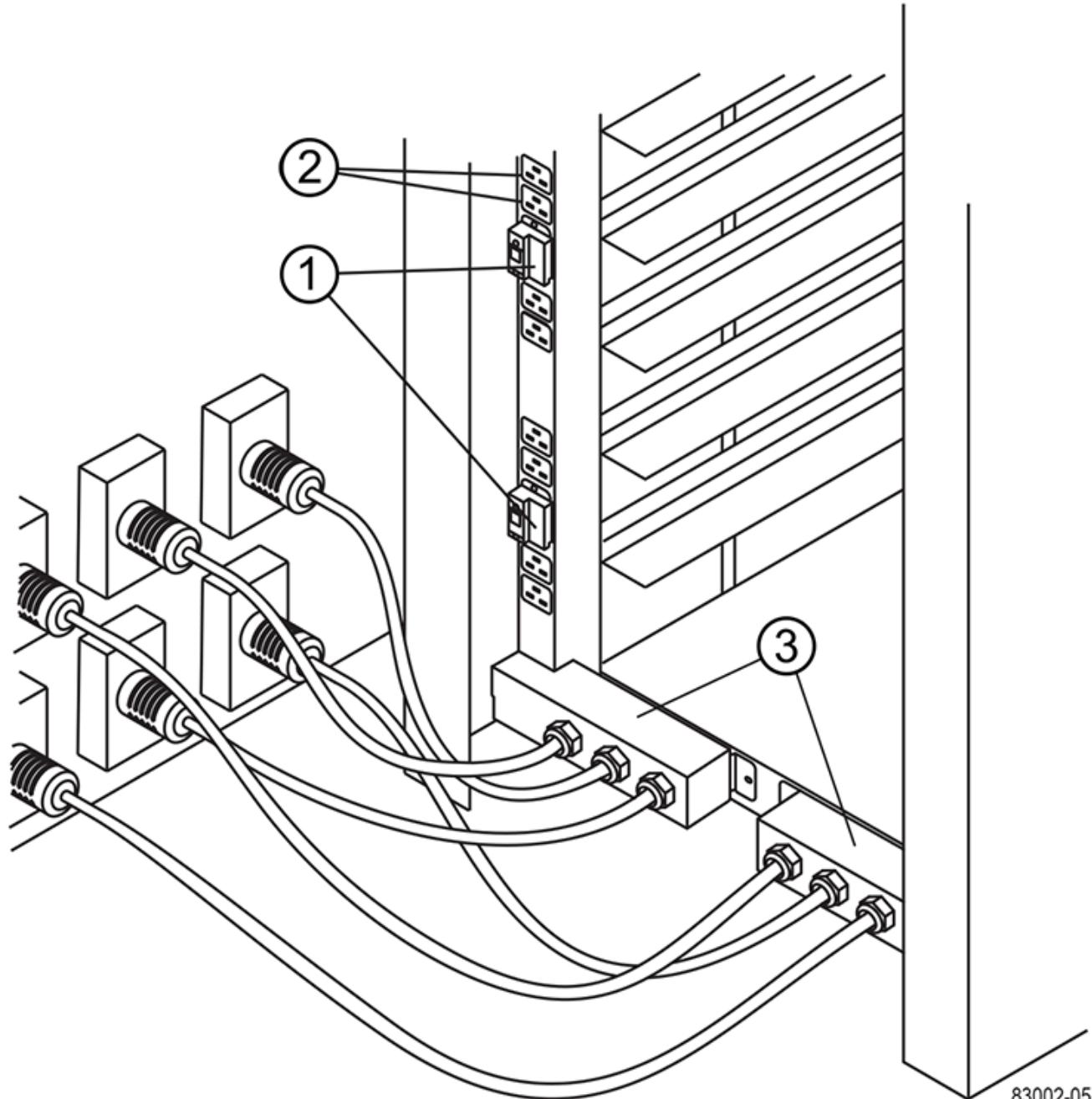
Steps

1. Turn off the power to all components in the cabinet.
2. Turn all 12 circuit breakers to their off (down) position.
3. Plug each of the six NEMA L6-30 connectors (USA and Canada) or the six IEC 60309 connectors (worldwide, except for USA and Canada) into an available electrical outlet.



You must connect each PDU to an independent power source outside of the cabinet.

4. Turn all 12 circuit breakers to their on (up) position.



| | |
|----|--------------------|
| 1. | Circuit breakers |
| 2. | Electrical outlets |
| 3. | Power entry boxes |

5. Turn on the power to all drive trays in the cabinet.



Wait 30 seconds after turning on the drive trays before you turn on the power to the controller-drive trays.

6. Wait 30 seconds after turning on the drive trays, and then turn on the power to all controller-drive trays in the cabinet.

Result

The cabinet installation is complete. You can resume normal operations.

Rack-mount hardware

Use the links below to access documentation that describes how to install rack-mounting hardware.

Adjustable support rails

Access [Installing adjustable support rails](#) for installing a controller-drive tray or a drive tray that was shipped separately (not already installed in the cabinet). This procedure is applicable for the following 2U (9 cm or 3.5 inch) trays:

- DE1600 or DE5600
- E2612 or E2624
- E5412, E5424, E5512, or E5524

Two-post rack — 2U

Access [Installing 2U equipment into a two-post rack](#).

Four-post rack or cabinet — 2U

Access [Installing a 2U 12-drive enclosure in a four-post rack or cabinet](#).

Four-post rack — SuperRail

Access [Install SuperRail into a four-post rack \(DE224C/DE460C shelves\)](#).

Cabling

Cabling overview

You can cable a host directly to a controller or use switches to connect a host to a controller.

If your storage system includes one or more drive shelves, you must cable them to your controller shelf. You can add a new drive shelf while power is still applied to other components of the storage system. In addition, you can connect your storage system to a network for out-of-band management.

The cabling information is intended for a hardware installer or system administrator who is installing or expanding a storage system. It is assumed that you have installed the storage system as described in the *Installation and Setup Instructions* for your hardware.

Applicable hardware model

Cabling information applies to the following hardware models.

| Controller Shelf | Drive Shelf |
|-----------------------------------|-----------------|
| EF600 | Not applicable. |
| E5724, EF570, E2812, E2824, EF280 | DE212C, DE224C |
| E2860, E5760 | DE460C |

Additional cabling information

If you are cabling for the following configuration, see [Adding IOM Drive Shelves to an Existing E27XX, E56XX, or EF560 Controller Shelf](#).

| Controller Shelf | Drive Shelf |
|-----------------------------------|----------------|
| E2712, E2724, E5612, E5624, EF560 | DE212C, DE224C |
| E2760, E5660 | DE460C |

For information about other cabling options, see the [E-Series Hardware Cabling Guide](#) for older systems.

For information about cabling to support mirroring features, see the [Synchronous and Asynchronous Mirroring Feature Descriptions and Deployment Guide](#).

Requirements

In addition to controller shelves and drive shelves, you might need some or all of the following components when cabling your storage system:

- Cables: SAS, Fibre Channel (FC), Ethernet, InfiniBand
- Small form-factor pluggable (SFP) or Quad SFP (QSFP) transceivers
- Switches

- Host bus adapters (HBAs)
- Host channel adapters (HCAs)
- Network interface cards (NICs)

Host cabling

You can cable a host directly to a controller (direct-attached topology) or use switches (switch topology) to connect a host to a controller.

Cabling for a direct-attached topology

A direct-attached topology connects host adapters directly to controllers in your storage system.

The following figure shows an example connection. To help ensure maximum performance, use all available host adapter ports.

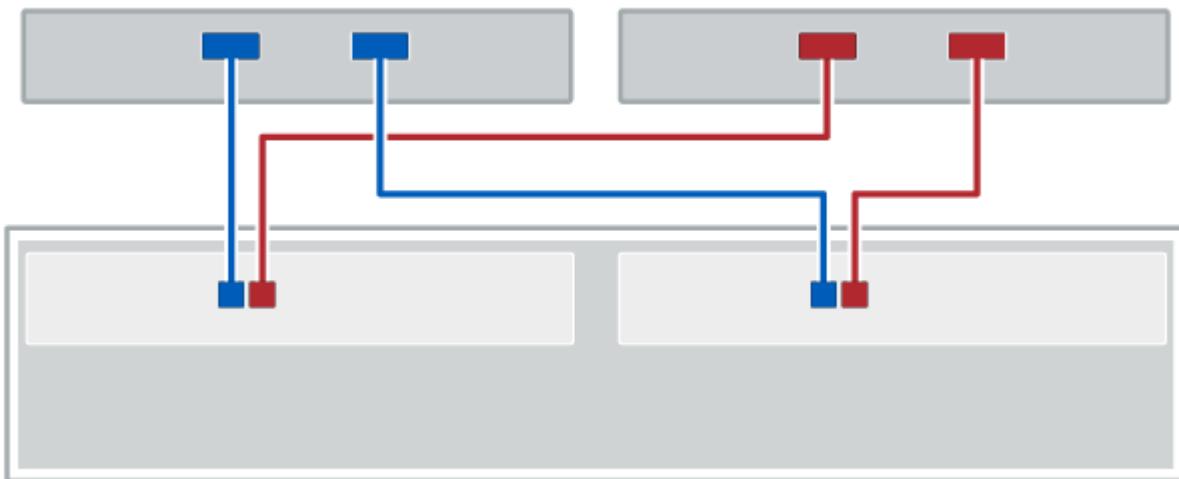


Figure 1. Two hosts and two controllers

(1) Connect each host adapter port directly to the host ports on the controllers.

Cabling for a switch topology

A switch topology uses switches to connect hosts to the controllers in your storage system. The switch must support the connection type used between the host and the controller.

The following figure shows an example connection. For switches that provide provisioning capability, you should isolate each initiator and target pair.

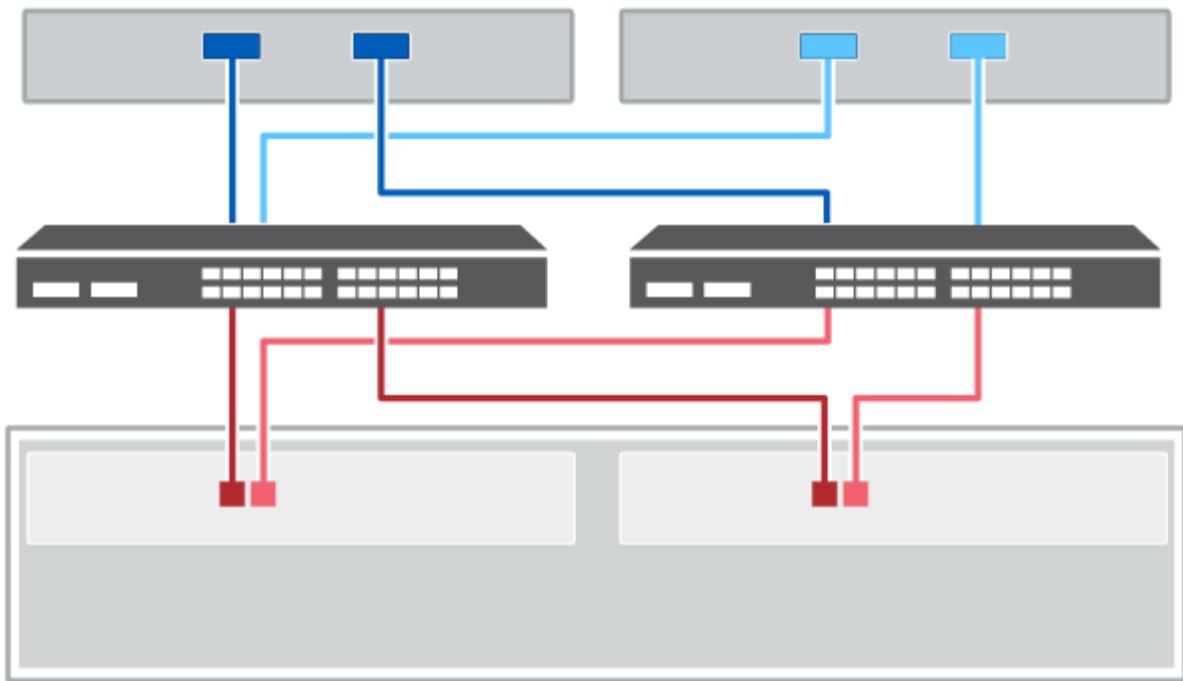


Figure 2. Two hosts and two switches

(1) Connect each host adapter directly to the switch.

(2) Connect each switch directly to the host ports on the controllers. To help ensure maximum performance, use all available host adapter ports.

Drive shelf cabling

You must connect each controller in the controller shelf to an I/O module (IOM) in a drive shelf.

This procedure applies to IOM12 and IOM12B drive shelves.

i 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.)

If you are cabling an older controller shelf to a DE212C, DE224C, or DE460, see [Adding IOM Drive Shelves to an Existing E27XX, E56XX, or EF560 Controller Shelf](#).

Cabling E2800 and E5700

The following information applies to cabling an E5700, EF570, E2800, or EF280 controller shelf to a DE212C, DE224C, or DE460 drive shelf.

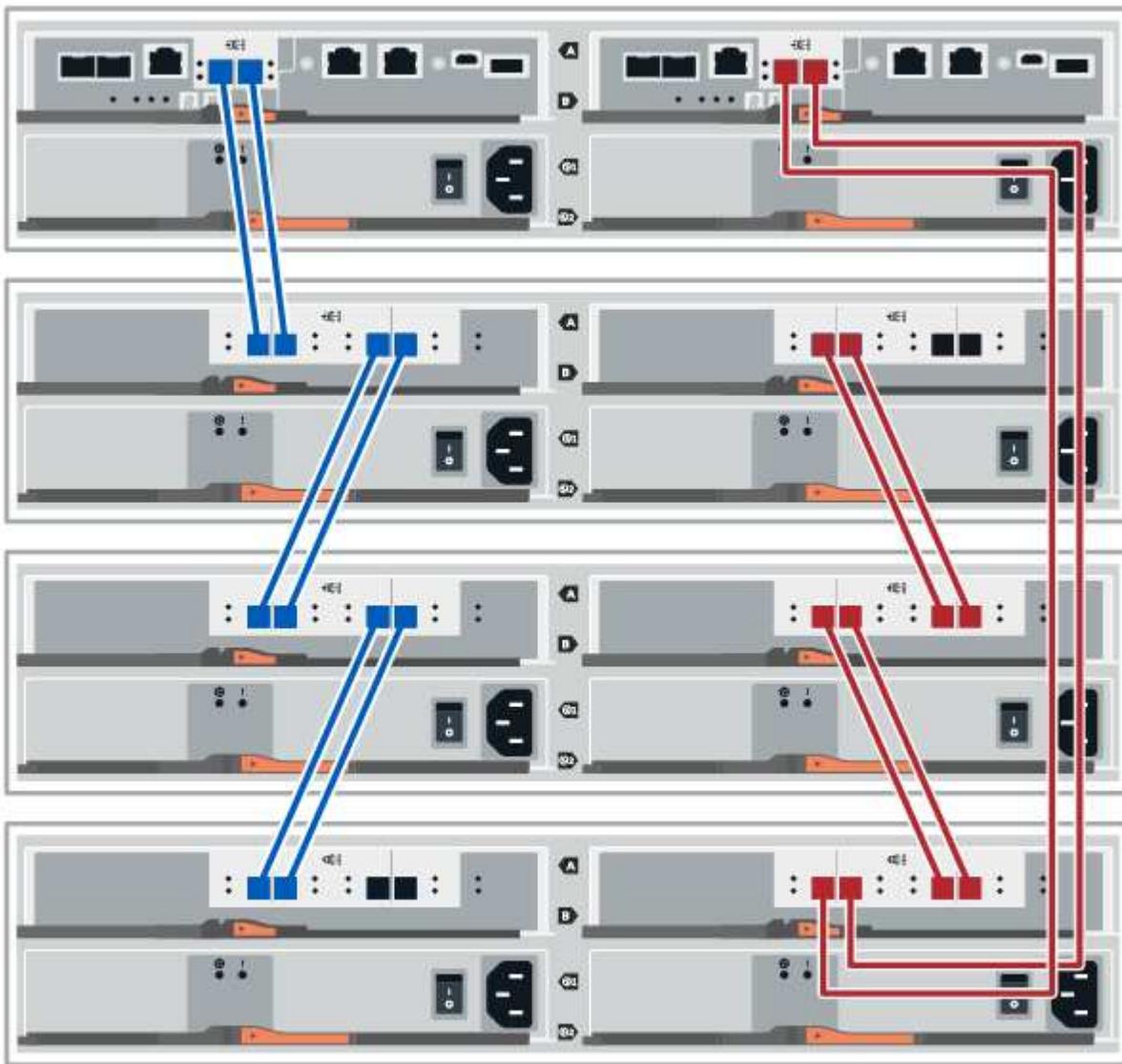
Cabling a 12-drive or 24-drive shelf

You can cable your controller shelf to one or more 12-drive or 24-drive shelves.

The following image shows a representation of the controller shelf and the drive shelves. To locate the ports on

your model, see [Hardware Universe](#).

A controller shelf and 12-drive or 24-drive shelves

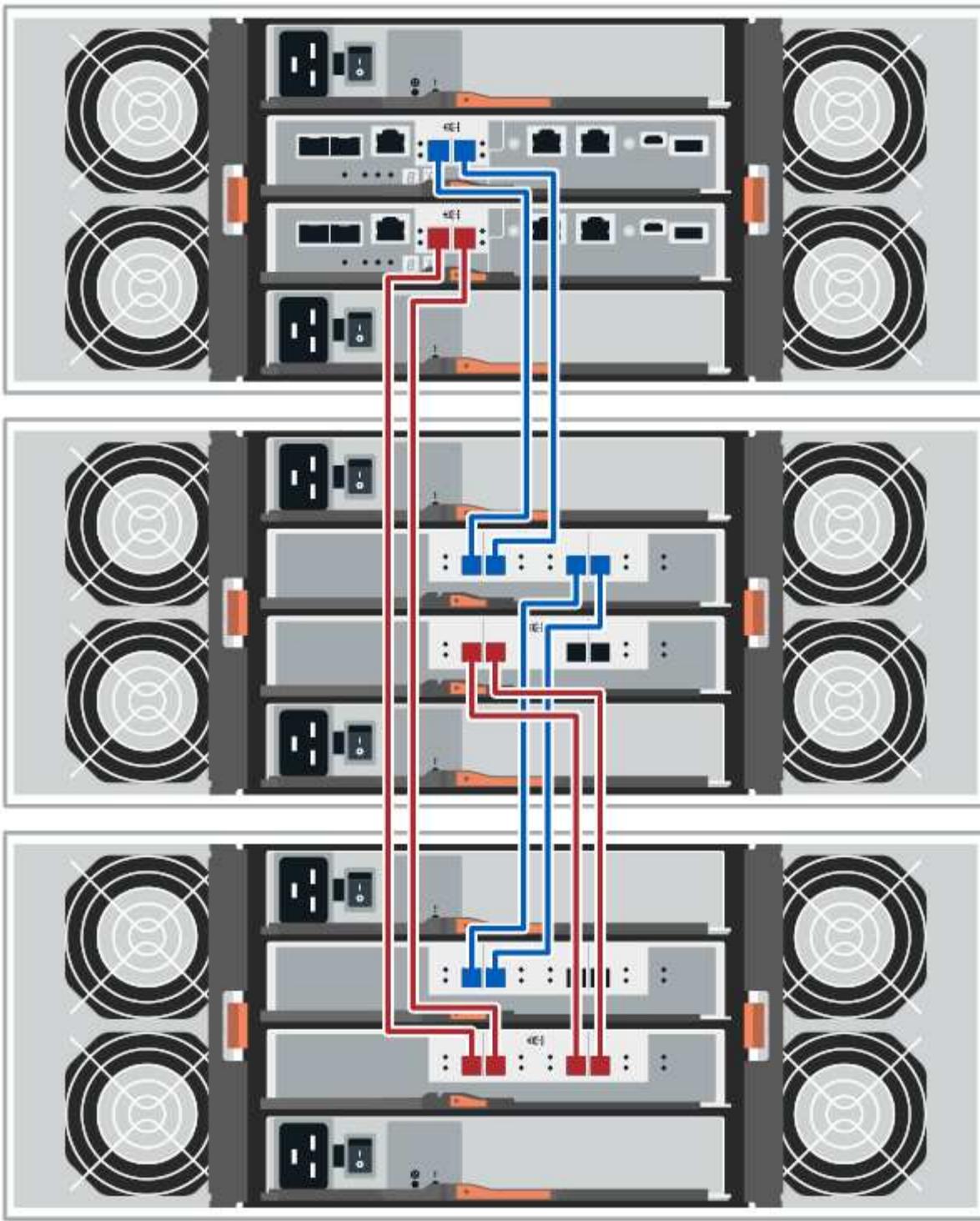


Cabling a 60-drive shelf

You can cable your controller shelf to one or more 60-drive shelves.

The following image shows a representation of the controller shelf and the drive shelves. To locate the ports on your model, see [Hardware Universe](#).

A controller shelf and 60-drive shelves



Cabling EF300

The following information applies to cabling an EF300 controller shelf to a DE212C, DE224C, or DE460 drive shelf.

Before you begin

Before cabling the EF300, make sure the firmware is updated to the latest version. To update the firmware,

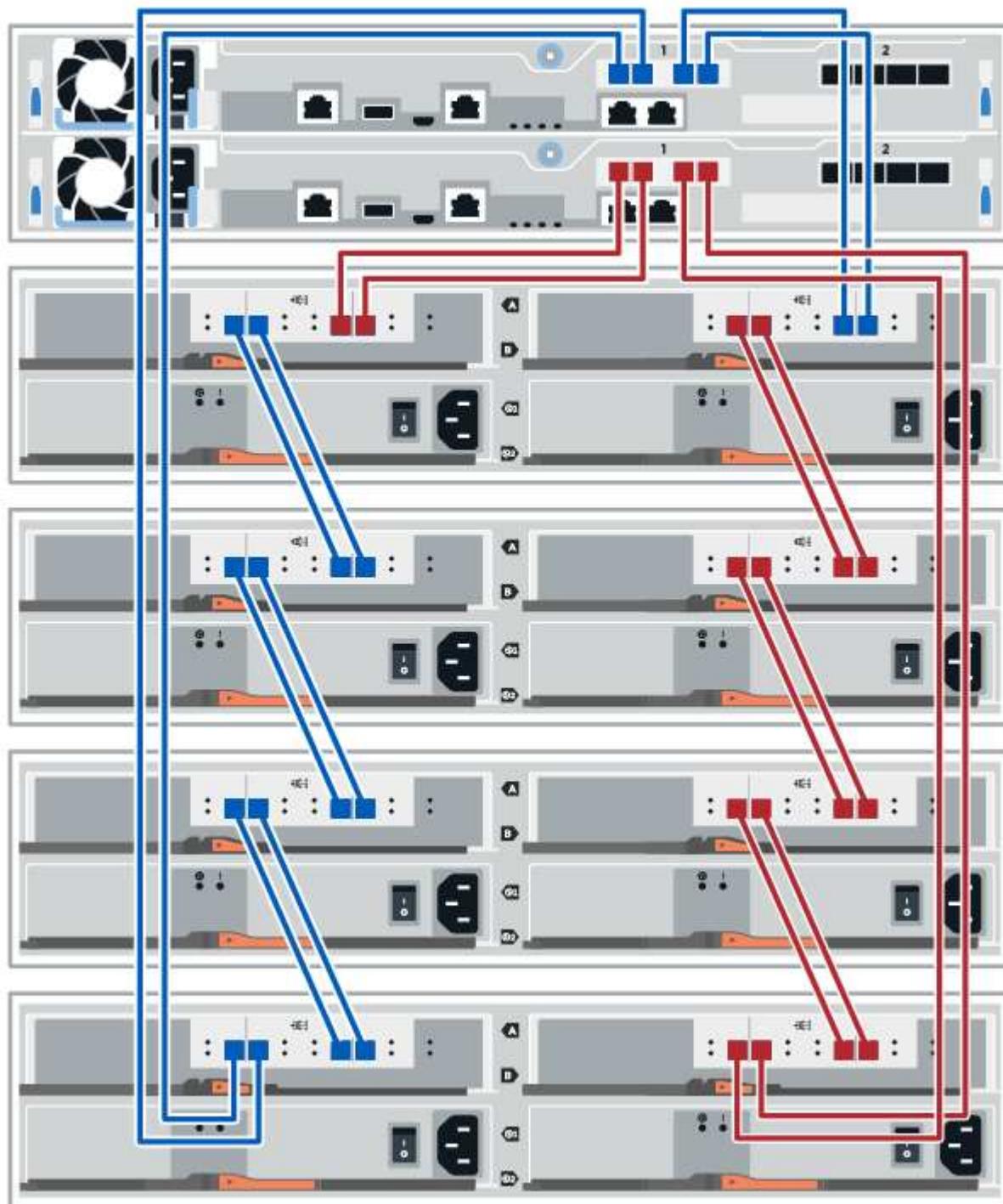
follow the instructions in [Upgrading SANtricity OS](#).

Cabling a 12-drive or 24-drive shelf

You can cable your controller shelf to one or more 12-drive or 24-drive shelves.

The following image shows a representation of the controller shelf and the drive shelves. To locate the ports on your model, see [Hardware Universe](#).

A controller shelf and 12-drive or 24-drive shelves

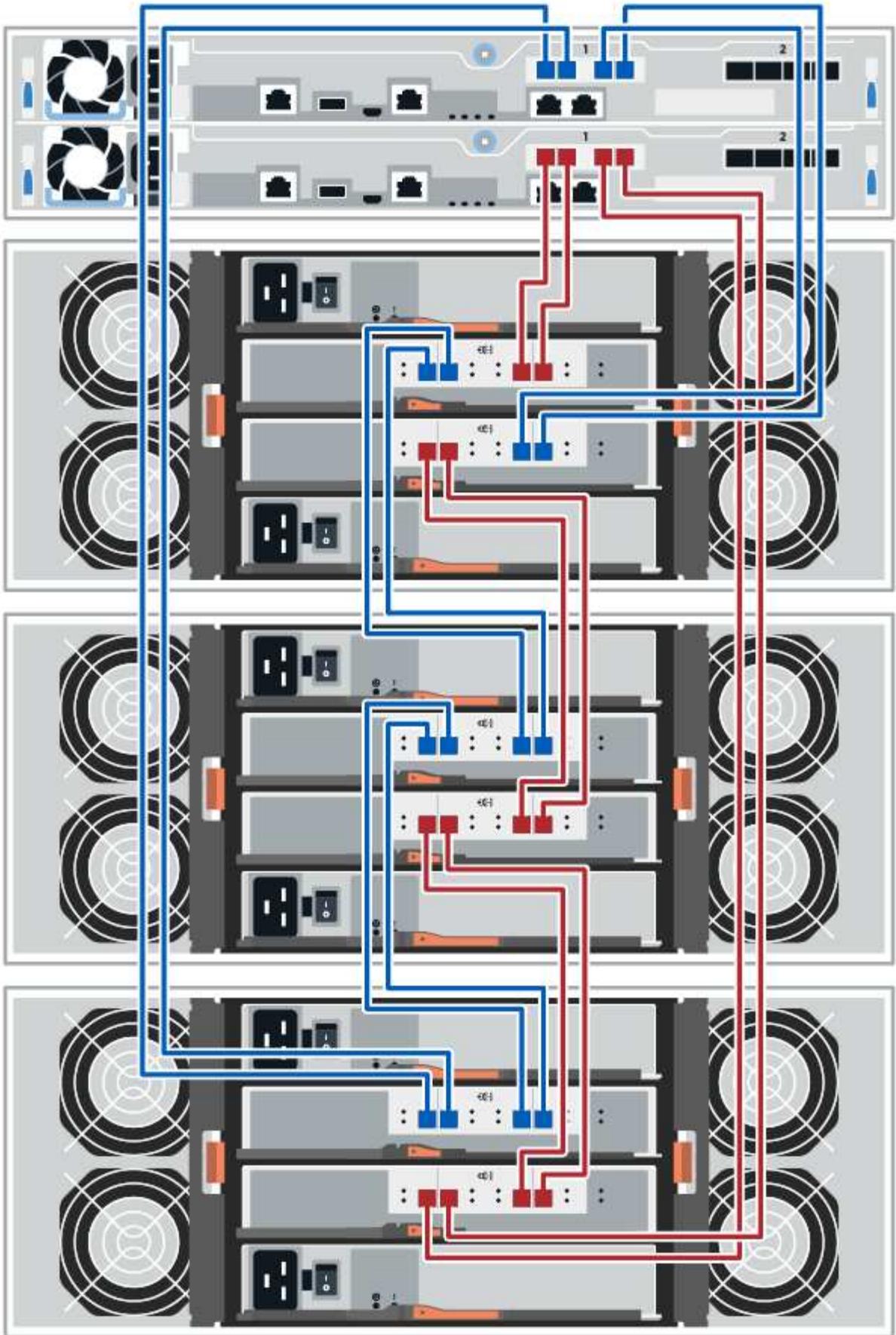


Cabling a 60-drive shelf

You can cable your controller shelf to one or more 60-drive shelves.

The following image shows a representation of the controller shelf and the drive shelves. To locate the ports on your model, see [Hardware Universe](#).

A controller shelf and 60-drive shelves



Power cabling

You must connect each component's power supplies to separate power circuits.

Before you begin

- You have confirmed that your location provides the necessary power.
- The two power switches on the two shelf power supplies must be turned off.

About this task

The power source for your storage system must be able to accommodate the power requirements of the new drive shelf. For information about the power consumption for your storage system, see the [Hardware Universe](#).

Step

1. Connect the two power cables for each shelf to different power distribution units (PDUs) in the cabinet or rack.

Hot adding a drive shelf

You can add a new drive shelf while power is still applied to the other components of the storage system. You can configure, reconfigure, add, or relocate storage system capacity without interrupting user access to data.

Before you begin

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

- Read all steps before beginning the procedure.
- Ensure hot adding a drive shelf is the procedure you need.

About this task

This procedure applies to hot adding a DE212C, DE224C, or DE460C drive shelf to an E5700, EF570, E2800, EF280, or EF300 controller shelf.

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.)

If you are cabling an older controller shelf to a DE212C, DE224C, or DE460, see [Adding IOM Drive Shelves to an Existing E27XX, E56XX, or EF560 Controller Shelf](#).

 To maintain system integrity, you must follow the procedure exactly in the order presented.

Step 1: Prepare to add the drive shelf

To prepare to hot add a drive shelf, you must check for critical events and check the status of the IOMs.

Before you begin

- The power source for your storage system must be able to accommodate the power requirements of the

new drive shelf. For the power specification for your drive shelf, see the [Hardware Universe](#).

- The cabling pattern for the existing storage system must match one of the applicable schemes shown in this procedure.

Steps

1. In SANtricity System Manager, select **Support > Support Center > Diagnostics**.
2. Select **Collect Support Data**.

The Collect Support Data dialog box appears.

3. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name support-data.7z. The data is not automatically sent to technical support.

4. Select **Support > Event Log**.

The Event Log page displays the event data.

5. Select the heading of the **Priority** column to sort critical events to the top of the list.
6. Review the system critical events for events that have occurred in the last two to three weeks, and verify that any recent critical events have been resolved or otherwise addressed.



If unresolved critical events have occurred within the previous two to three weeks, stop the procedure and contact technical support. Continue the procedure only when the issue is resolved.

7. Select **Hardware**.

8. Select the **IOMs (ESMs)** icon.



The Shelf Component Settings dialog box appears with the **IOMs (ESMs)** tab selected.

9. Make sure that the status shown for each IOM/ESM is *Optimal*.
10. Click **Show more settings**.
11. Confirm that the following conditions exist:
 - The number of ESMs/IOMs detected matches the number of ESMs/IOMs installed in the system and that for each drive shelf.
 - Both of the ESMs/IOMs show that communication is OK.
 - The data rate is 12Gb/s for DE212C, DE224C, and DE460C drive shelves or 6 Gb/s for other drive trays.

Step 2: Install the drive shelf and apply power

You install a new drive shelf or a previously installed drive shelf, turn on the power, and check for any LEDs that require attention.

Steps

1. If you are installing a drive shelf that has previously been installed in a storage system, remove the drives.

The drives must be installed one at a time later in this procedure.

If the installation history of the drive shelf that you are installing is unknown, you should assume that it has been previously installed in a storage system.

2. Install the drive shelf in the rack that holds the storage system components.



See the installation instructions for your model for the full procedure for physical installation and power cabling. The installation instructions for your model includes notes and warnings that you must take into account to safely install a drive shelf.

3. Power on the new drive shelf, and confirm that no amber attention LEDs are illuminated on the drive shelf. If possible, resolve any fault conditions before you continue with this procedure.

Step 3: Cable your system

Select one of the following options, depending on whether you are cabling an E2800 and E5700 storage system or an EF300 storage system.

- [Option 1: Connect the drive shelf for E2800 and E5700](#)
- [Option 2: Connect the drive shelf for EF300](#)

If you are cabling an older controller shelf to a DE212C, DE224C, or DE460, see [Adding IOM Drive Shelves to an Existing E27XX, E56XX, or EF560 Controller Shelf](#).

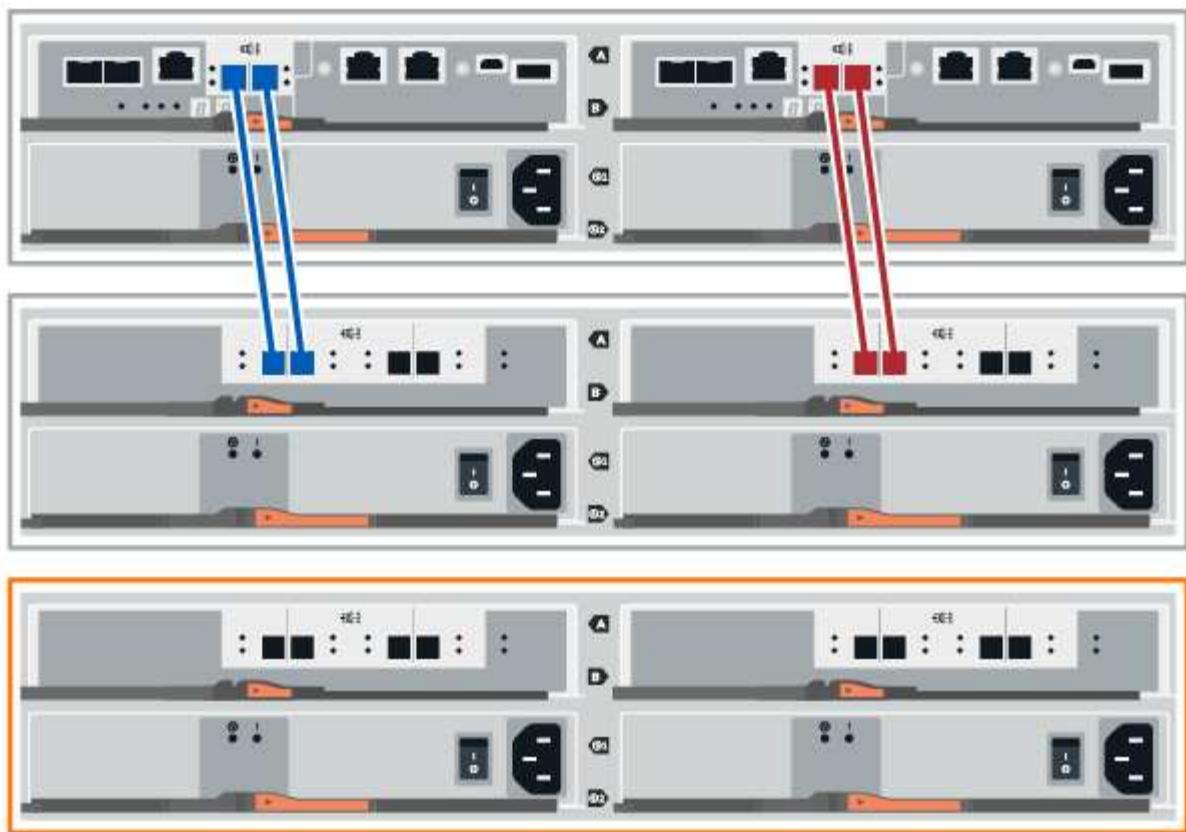
Option 1: Connect the drive shelf for E2800 and E5700

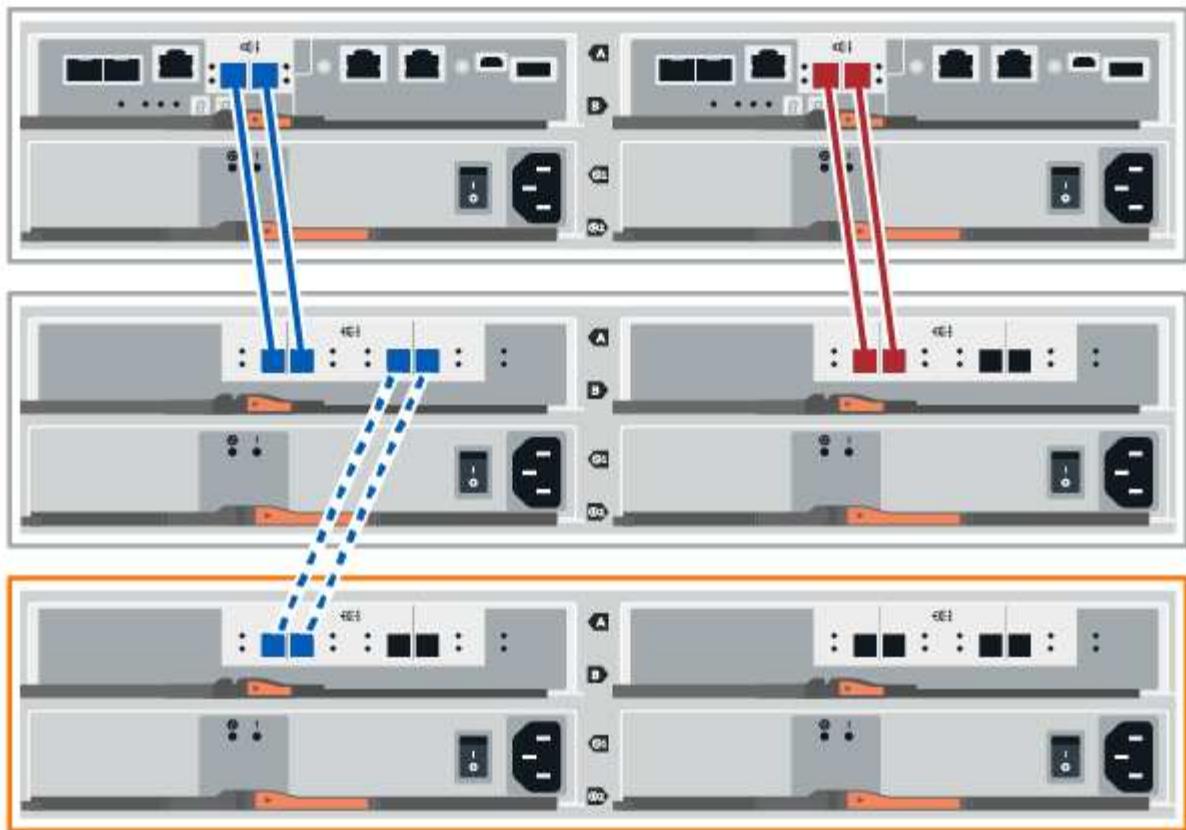
You connect the drive shelf to controller A, confirm IOM status, and then connect the drive shelf to controller B.

Steps

1. Connect the drive shelf to controller A.

The following figure shows an example connection between an additional drive shelf and controller A. To locate the ports on your model, see the [Hardware Universe](#).





2. In SANtricity System Manager, click **Hardware**.



At this point in the procedure, you have only one active path to the controller shelf.

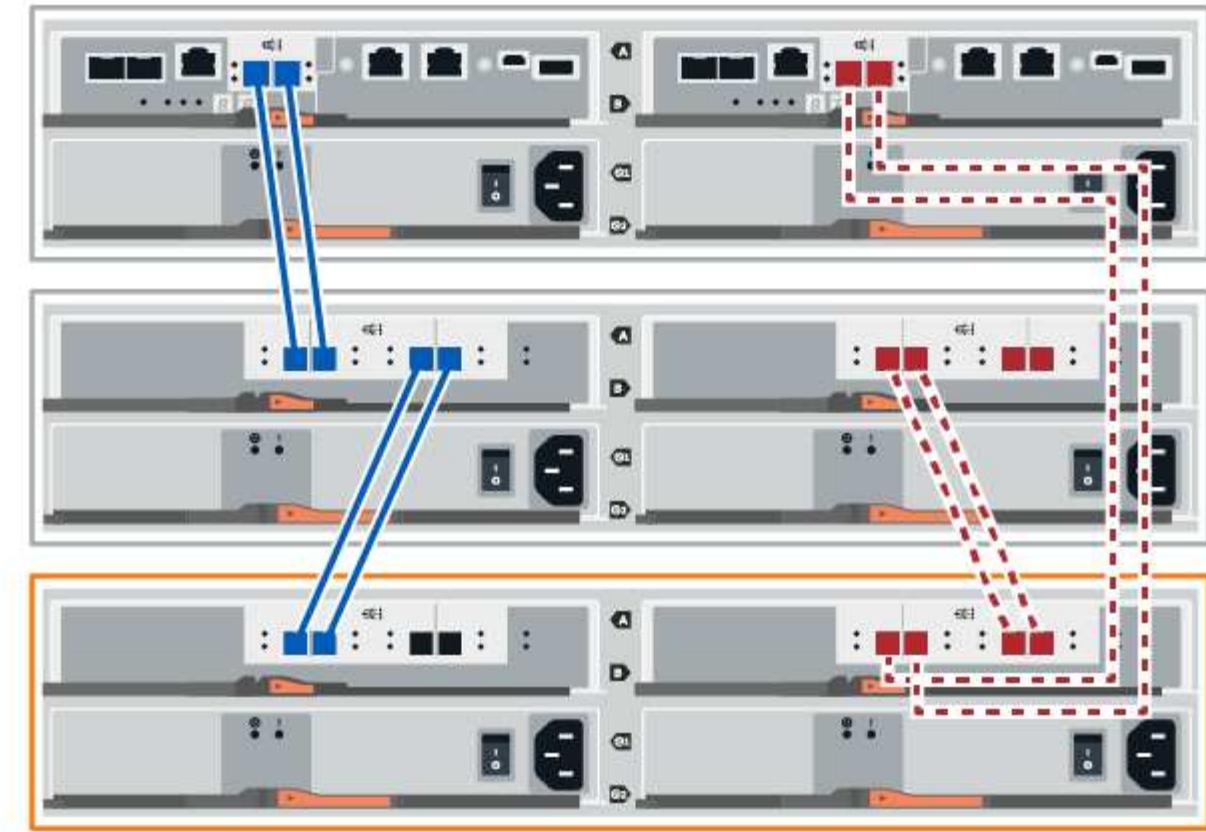
3. Scroll down, as necessary, to see all the drive shelves in the new storage system. If the new drive shelf is not displayed, resolve the connection issue.
4. Select the **ESMs/IOMs** icon for the new drive shelf.



The **Shelf Component Settings** dialog box appears.

5. Select the **ESMs/IOMs** tab in the **Shelf Component Settings** dialog box.
6. Select **Show more options**, and verify the following:
 - IOM/ESM A is listed.
 - Current data rate is 12 Gbps for a SAS-3 drive shelf.
 - Card communications is OK.
7. Disconnect all expansion cables from controller B.
8. Connect the drive shelf to controller B.

The following figure shows an example connection between an additional drive shelf and controller B. To locate the ports on your model, see the [Hardware Universe](#).



- If it is not already selected, select the **ESMs/IOMs** tab in the **Shelf Component Settings** dialog box, and then select **Show more options**. Verify that Card communications is **YES**.



Optimal status indicates that the loss of redundancy error associated with the new drive shelf has been resolved and the storage system is stabilized.

Option 2: Connect the drive shelf for EF300

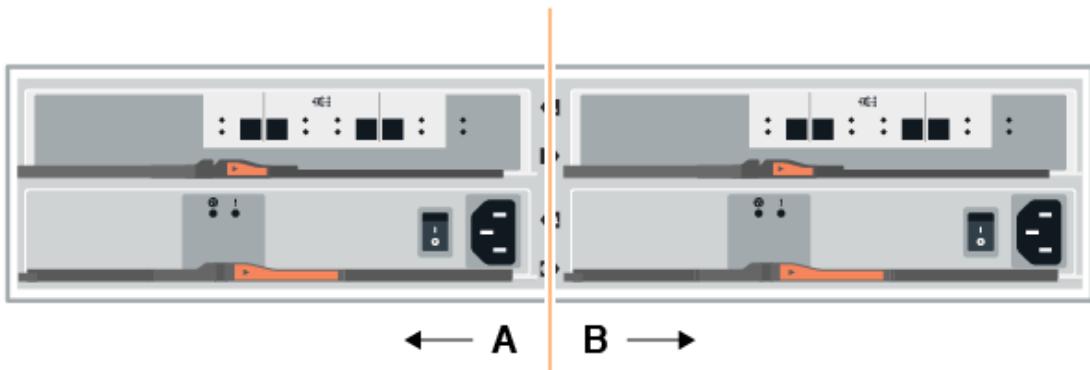
You connect the drive shelf to controller A, confirm IOM status, and then connect the drive shelf to controller B.

Before you begin

- You have updated your firmware to the latest version. To update your firmware, follow the instructions in the [Upgrading SANtricity OS](#).

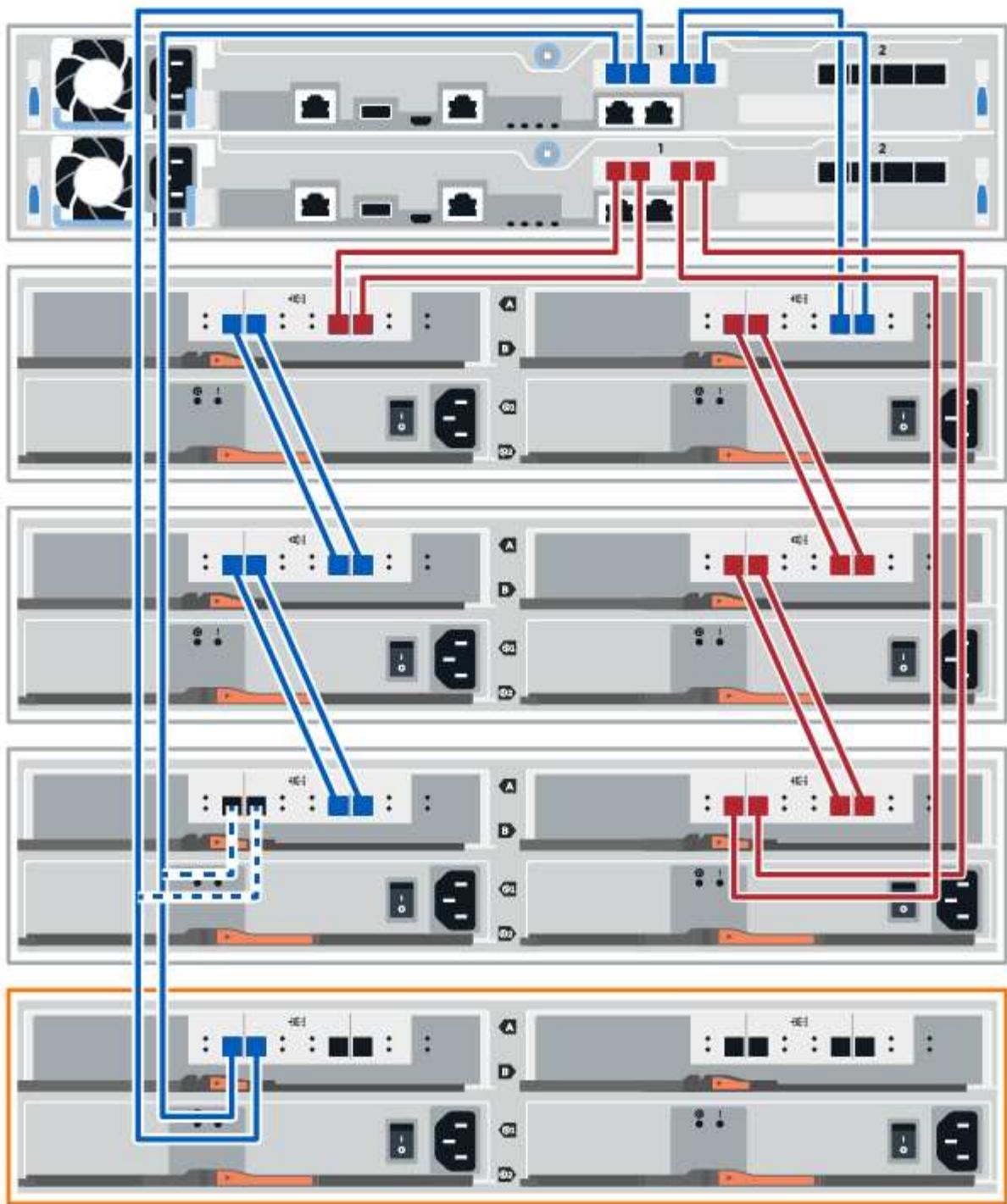
Steps

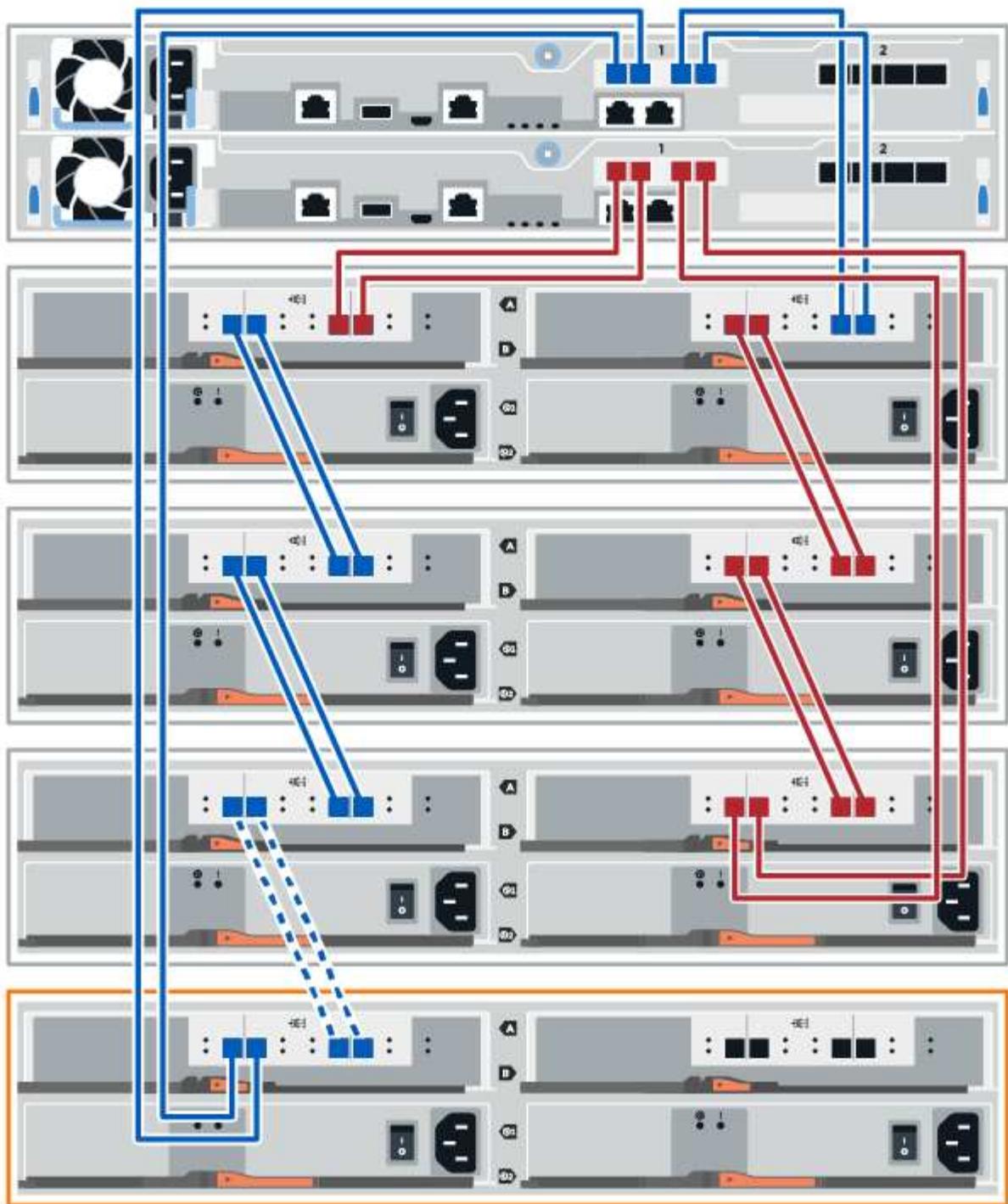
- Disconnect both of the A-side controller cables from IOM12 ports one and two from previous last shelf in the stack and then connect them to the new shelf IOM12 ports one and two.



2. Connect the cables to A-side IOM12 ports three and four from the new shelf to previous last shelf IOM12 ports one and two.

The following figure shows an example connection for A side between an additional drive shelf and the previous last shelf. To locate the ports on your model, see the [Hardware Universe](#).





3. In SANtricity System Manager, click **Hardware**.



At this point in the procedure, you have only one active path to the controller shelf.

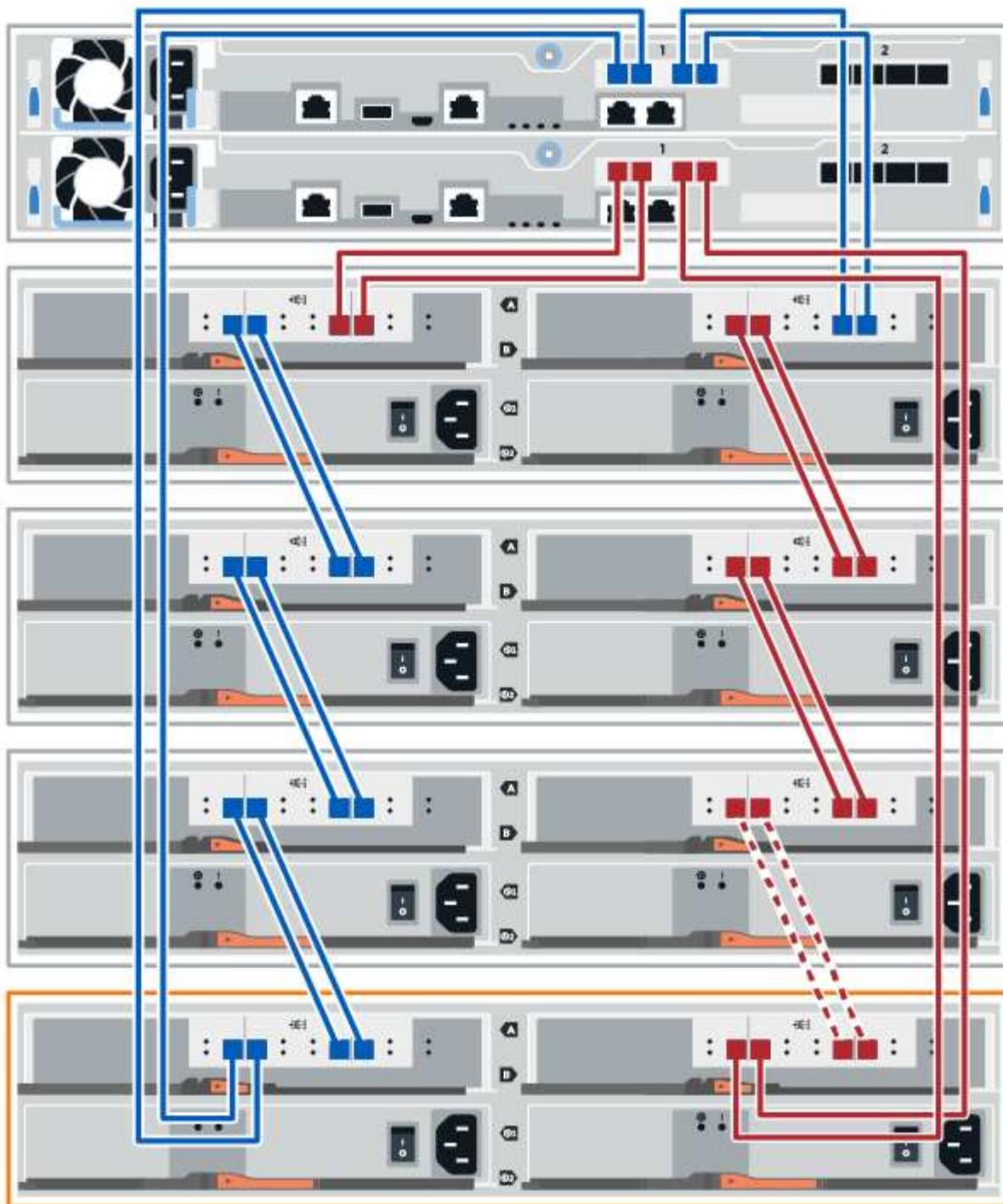
4. Scroll down, as necessary, to see all the drive shelves in the new storage system. If the new drive shelf is not displayed, resolve the connection issue.
5. Select the **ESMs/IOMs** icon for the new drive shelf.



The **Shelf Component Settings** dialog box appears.

6. Select the **ESMs/IOMs** tab in the **Shelf Component Settings** dialog box.
7. Select **Show more options**, and verify the following:
 - IOM/ESM A is listed.
 - Current data rate is 12 Gbps for a SAS-3 drive shelf.
 - Card communications is OK.
8. Disconnect both the B-side controller cables from IOM12 ports one and two from the previous last shelf in the stack then connect them to the new shelf IOM12 ports one and two.
9. Connect the cables to B-side IOM12 ports three and four from the new shelf to the previous last shelf IOM12 ports one and two.

The following figure shows an example connection for B side between an additional drive shelf and the previous last shelf. To locate the ports on your model, see the [Hardware Universe](#).



10. If it is not already selected, select the **ESMs/IOMs** tab in the **Shelf Component Settings** dialog box, and then select **Show more options**. Verify that Card communications is **YES**.



Optimal status indicates that the loss of redundancy error associated with the new drive shelf has been resolved and the storage system is stabilized.

Step 4: Complete hot add

You complete the hot add by checking for any errors and confirming that the newly added drive shelf uses the latest firmware.

Steps

1. In SANtricity System Manager, click **Home**.
2. If the link labeled **Recover from problems** appears at the center top of the page, click the link, and resolve any issues indicated in the Recovery Guru.
3. In SANtricity System Manager, click **Hardware**, and scroll down, as necessary, to see the newly added drive shelf.
4. For drives that were previously installed in a different storage system, add one drive at time to the newly installed drive shelf. Wait for each drive to be recognized before you insert the next drive.

When a drive is recognized by the storage system, the representation of the drive slot in the **Hardware** page displays as a blue rectangle.

5. Select **Support > Support Center > Support Resources** tab.
6. Click the **Software and Firmware Inventory** link, and check which versions of the IOM/ESM firmware and the drive firmware are installed on the new drive shelf.



You might need to scroll down the page to locate this link.

7. If necessary, upgrade the drive firmware.

IOM/ESM firmware automatically upgrades to the latest version unless you have disabled the upgrade feature.

The hot add procedure is complete. You can resume normal operations.

Ethernet cabling for a management station

You can connect your storage system to an Ethernet network for out-of-band storage array management. You must use Ethernet cables for all storage array management connections.

Direct topology

A direct topology connects your controller directly to an Ethernet network.

You must connect management port 1 on each controller for out-of-band management and leave port 2 available for access to the storage array by technical support.

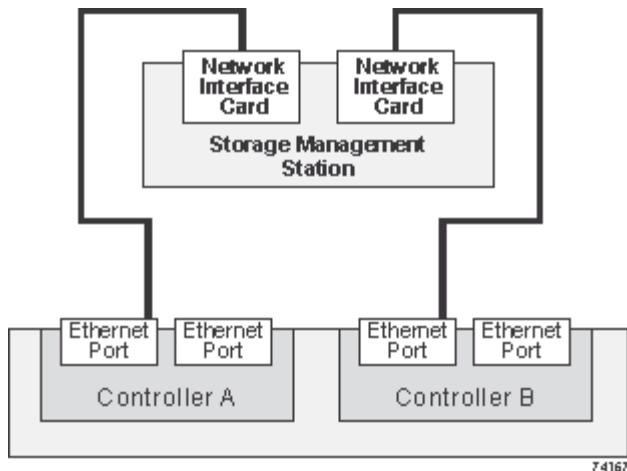


Figure 3. Direct storage management connections

Fabric topology

A fabric topology uses a switch to connect your controller to an Ethernet network.

You must connect management port 1 on each controller for out-of-band management and leave port 2 available for access to the storage array by technical support.

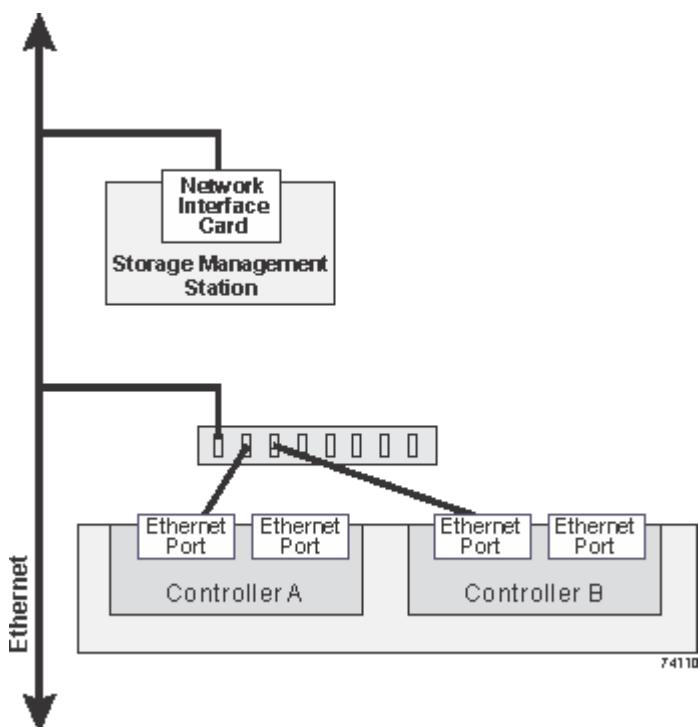


Figure 4. Fabric storage management connections

Deploy software

Linux express configuration

Linux express configuration overview

The Linux express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone Linux host to an E-Series storage system. It is designed to get the storage system up and running as quickly as possible with minimal decision points.

Procedure overview

The Linux express method includes the following steps.

1. Set up one of the following communication environments:
 - Fibre Channel (FC)
 - iSCSI
 - SAS
 - iSER over Infiniband
 - SRP over Infiniband
 - NVMe over Infiniband
 - NVMe over RoCE
 - NVMe over Fibre Channel
2. Create logical volumes on the storage array.
3. Make the volumes available to the data host.

Find more information

- Online help — Describes how to use SANtricity System Manager to complete configuration and storage management tasks. It is available within the product.
- [NetApp Knowledgebase](#) (a database of articles) — Provides troubleshooting information, FAQs, and instructions for a wide range of NetApp products and technologies.
- [NetApp Interoperability Matrix Tool](#) — Enables you to search for configurations of NetApp products and components that meet the standards and requirements specified by NetApp.
- [Linux Unified Host Utilities 7.1 Installation Guide](#) — Describes how to use the Linux Unified Host Utilities 7.1.

Assumptions

The Linux express method is based on the following assumptions:

| Component | Assumptions |
|----------------------------|--|
| Hardware | <ul style="list-style-type: none"> • You have used the Installation and Setup Instructions included with the controller shelves to install the hardware. • You have connected cables between the optional drive shelves and the controllers. • You have applied power to the storage system. • You have installed all other hardware (for example, management station, switches) and made the necessary connections. • If you are using NVMe over Infiniband, NVMe over RoCE, or NVMe over Fibre Channel, each EF300, EF600, EF570, or E5700 controller contains at least 32 GB of RAM. |
| Host | <ul style="list-style-type: none"> • You have made a connection between the storage system and the data host. • You have installed the host operating system. • You are not using Linux as a virtualized guest. • You are not configuring the data (I/O attached) host to boot from SAN. • You have installed any OS updates as listed under the NetApp Interoperability Matrix Tool. |
| Storage management station | <ul style="list-style-type: none"> • You are using a 1 Gbps or faster management network. • You are using a separate station for management rather than the data (I/O attached) host. • You are using out-of-band management, in which a storage management station sends commands to the storage system through the Ethernet connections to the controller. • You have attached the management station to the same subnet as the storage management ports. |
| IP addressing | <ul style="list-style-type: none"> • You have installed and configured a DHCP server. • You have not yet made an Ethernet connection between the management station and the storage system. |
| Storage provisioning | <ul style="list-style-type: none"> • You will not use shared volumes. • You will create pools rather than volume groups. |

| Component | Assumptions |
|--------------------------------|---|
| Protocol: FC | <ul style="list-style-type: none"> • You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: iSCSI | <ul style="list-style-type: none"> • You are using Ethernet switches capable of transporting iSCSI traffic. • You have configured the Ethernet switches according to the vendor's recommendation for iSCSI. |
| Protocol: SAS | <ul style="list-style-type: none"> • You are using NetApp-supported SAS HBAs. • You are using SAS HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: iSER over InfiniBand | <ul style="list-style-type: none"> • You are using an InfiniBand fabric. • You are using IB-iSER HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: SRP over InfiniBand | <ul style="list-style-type: none"> • You are using an InfiniBand fabric. • You are using IB-SRP driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: NVMe over InfiniBand | <ul style="list-style-type: none"> • You have received the 100G or 200G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over InfiniBand protocol or the controllers were ordered with standard IB ports and need to be converted to NVMe-oF ports. • You are using an InfiniBand fabric. • You are using NVMe/IB driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |

| Component | Assumptions |
|-----------------------------------|--|
| Protocol: NVMe over RoCE | <ul style="list-style-type: none"> • You have received the 100G or 200G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over RoCE protocol or the controllers were ordered with standard IB ports and need to be converted to NVMe-oF ports. • You are using NVMe/RoCE driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: NVMe over Fibre Channel | <ul style="list-style-type: none"> • You have received the 32G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over Fibre Channel protocol or the controllers were ordered with standard FC ports and need to be converted to NVMe-oF ports. • You are using NVMe/FC driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |



These express method instructions include examples for SUSE Linux Enterprise Server (SLES) and for Red Hat Enterprise Linux (RHEL).

Fibre Channel Express Setup

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.

The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from [NetApp Support](#).



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|---|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> Go to the directory where the SMIA*.bin installation package is located. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin Run the chmod +x SMIA*.bin command to grant execute permission to the file. Run the ./SMIA*.bin command to start the installer. |

- Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.

- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is

disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r  
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

5. Do one of the following to enable the multipathd daemon on boot.

| If you are using.... | Do this... |
|-----------------------------|--|
| RHEL 7.x and 8.x systems: | <code>systemctl enable multipathd</code> |
| SLES 12.x and 15.x systems: | <code>systemctl enable multipathd</code> |

6. Rebuild the initramfs image or the initrd image under /boot directory:

| If you are using.... | Do this... |
|-----------------------------|---|
| RHEL 7.x and 8.x systems: | <code>dracut --force --add multipath</code> |
| SLES 12.x and 15.x systems: | <code>dracut --force --add multipath</code> |

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

For example, for grub it is /boot/grub/menu.lst and for grub2 it is /boot/grub2/menu.cfg.

8. Use the "Create host manually" procedure in the online help to check whether the hosts are defined. Verify that each host type is either **Linux DM-MP (Kernel 3.10 or later)** if you enable the Automatic Load Balancing feature, or **Linux DM-MP (Kernel 3.9 or earlier)** if you disable the Automatic Load Balancing feature. If necessary, change the selected host type to the appropriate setting.

9. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd. Any line in the file with a first non-white-space character of # is considered a comment line. Empty lines are ignored.



For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

The multipath.conf files are available in the following locations:

- For SLES:

```
/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic
```

- For RHEL:

```
/usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf
```

Configure the FC switches

Configuring (zoning) the Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)

About this task

Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Determine host WWPNs and make the recommended settings

You install an FC HBA utility so you can view the worldwide port name (WWPN) of each host port.

Additionally, you can use the HBA utility to change any settings recommended in the Notes column of the

NetApp Interoperability Matrix Tool for the supported configuration.

About this task

Review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. You will need the correct version of HBA for your host operating system and CPU. Examples of FC HBA utilities include:
 - Emulex OneCommand Manager for Emulex HBAs
 - QLogic QConverge Console for QLogic HBAs
- Host I/O ports might automatically register if the host context agent is installed.

Steps

1. Download the appropriate utility from your HBA vendor's web site.
2. Install the utility.
3. Select the appropriate settings in the HBA utility.

Appropriate settings for your configuration are listed in the Notes column of the [NetApp Interoperability Matrix Tool](#).

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the `/dev/mapper` folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```

# sanlun lun show -p

        E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
        Volume Name:
        Preferred Owner: Controller in Slot B
        Current Owner: Controller in Slot B
        Mode: RDAC (Active/Active)
        UTM LUN: None
        LUN: 116
        LUN Size:
        Product: E-Series
        Host Device:
mpathr(360080e50004300ac000007575568851d)
        Multipath Policy: round-robin 0
        Multipath Provider: Native
-----
-----
host      controller                  controller
path      path          /dev/       host      target
state     type          node        adapter   port
-----
-----
up        secondary    sdcx       host14    A1
up        secondary    sdat       host10    A2
up        secondary    sdbv       host13    B1

```

2. Create a new partition according to the method appropriate for your Linux OS release.

Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```

# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%

```

3. Create a file system on the partition.

The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

Before using the volume, verify that the host can write data to the volume and read it back.

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

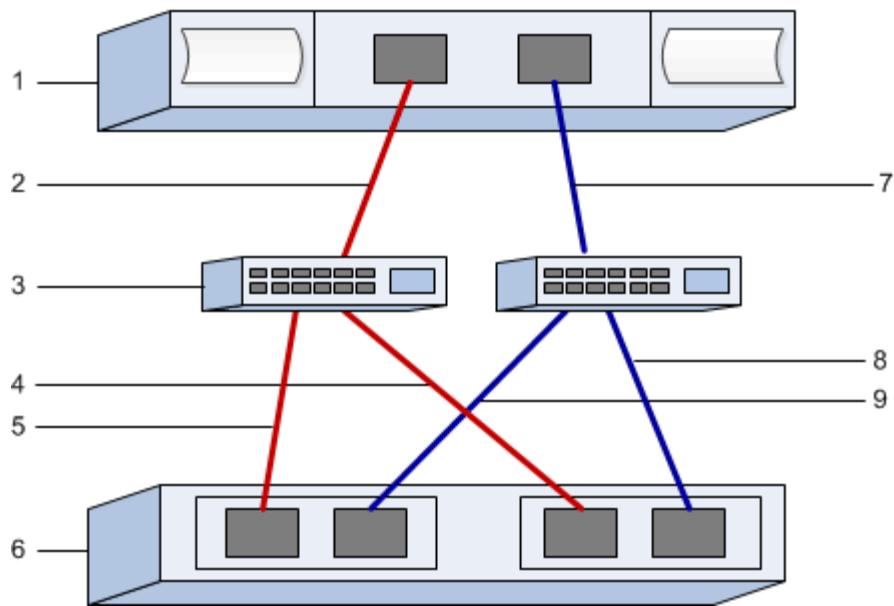
After you finish

Remove the file and folder that you copied.

Record your FC configuration

You can generate and print a PDF of this page, and then use the following worksheet to record FC storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Any single port has two paths to the storage (one to each controller).



Host identifiers

| Callout No. | Host (initiator) port connections | WWPN |
|-------------|-----------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host port 0 to FC switch zone 0 | |
| 7 | Host port 1 to FC switch zone 1 | |

Target identifiers

| Callout No. | Array controller (target) port connections | WWPN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 6 | Array controller (target) | <i>not applicable</i> |
| 5 | Controller A, port 1 to FC switch 1 | |
| 9 | Controller A, port 2 to FC switch 2 | |
| 4 | Controller B, port 1 to FC switch 1 | |
| 8 | Controller B, port 2 to FC switch 2 | |

Mapping host

| | |
|-------------------|--|
| Mapping host name | |
|-------------------|--|

| | |
|--------------|--|
| Host OS type | |
|--------------|--|

SAS Setup

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply. As necessary, make the updates for your operating system and protocol that are prescribed in the tool. Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
- Controller B, port 1: 169.254.128.102
- Subnet mask: 255.255.0.0

2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.

The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from [NetApp Support](#).



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|--|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none">a. Go to the directory where the SMIA*.bin installation package is located.b. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.binc. Run the chmod +x SMIA*.bin command to grant execute permission to the file.d. Run the ./SMIA*.bin command to start the installer. |

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following

browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.

- **Enable AutoSupport**— Automatically monitor the health of your storage array and have dispatches sent to technical support.
4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

5. Do one of the following to enable the `multipathd` daemon on boot.

| If you are using.... | Do this... |
|-----------------------------|-----------------------------|
| RHEL 7.x and 8.x systems: | systemctl enable multipathd |
| SLES 12.x and 15.x systems: | systemctl enable multipathd |

6. Rebuild the `initramfs` image or the `initrd` image under `/boot` directory:

| If you are using.... | Do this... |
|-----------------------------|---|
| RHEL 7.x and 8.x systems: | <code>dracut --force --add multipath</code> |
| SLES 12.x and 15.x systems: | <code>dracut --force --add multipath</code> |

7. Make sure that the newly created `/boot/initrams-*` image or `/boot/initrd-*` image is selected in the boot configuration file.

For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

8. Use the "Create host manually" procedure in the online help to check whether the hosts are defined. Verify that each host type is either **Linux DM-MP (Kernel 3.10 or later)** if you enable the Automatic Load Balancing feature, or **Linux DM-MP (Kernel 3.9 or earlier)** if you disable the Automatic Load Balancing feature. If necessary, change the selected host type to the appropriate setting.

9. Reboot the host.

Set up the multipath.conf file

The `multipath.conf` file is the configuration file for the multipath daemon, `multipathd`.

The `multipath.conf` file overrides the built-in configuration table for `multipathd`. Any line in the file with a first non-white-space character of `#` is considered a comment line. Empty lines are ignored.



For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

The `multipath.conf` files are available in the following locations:

- For SLES:

`/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic`

- For RHEL:

`/usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf`

Determine SAS host identifiers - Linux

For the SAS protocol, you find the SAS addresses using the HBA utility, then use the HBA BIOS to make the appropriate configuration settings.

Before you begin this procedure, review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. Depending on your host operating system and CPU, use either the LSI-sas2flash(6G) or sas3flash(12G) utility.
- Host I/O ports might automatically register if the host context agent is installed.

Steps

1. Download the HBA utility from your HBA vendor's web site.
2. Install the utility.
3. Use the HBA BIOS to select the appropriate settings for your configuration.

See the Notes column of the [NetApp Interoperability Matrix Tool](#) for recommendations.

Create partitions and filesystems

A new LUN has no partition or file system when the Linux host first discovers it. You must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the `/dev/mapper` folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```

# sanlun lun show -p

        E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
        Volume Name:
        Preferred Owner: Controller in Slot B
        Current Owner: Controller in Slot B
        Mode: RDAC (Active/Active)
        UTM LUN: None
        LUN: 116
        LUN Size:
        Product: E-Series
        Host Device:
mpathr(360080e50004300ac000007575568851d)
        Multipath Policy: round-robin 0
        Multipath Provider: Native
-----
-----
host      controller                  controller
path      path          /dev/       host      target
state     type          node        adapter   port
-----
-----
up        secondary    sdcx        host14    A1
up        secondary    sdat        host10    A2
up        secondary    sdbv        host13    B1

```

2. Create a new partition according to the method appropriate for your Linux OS release.

Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```

# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%

```

3. Create a file system on the partition.

The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

Before using the volume, you verify that the host can write data to the volume and read it back.

What you'll need

An initialized volume that is formatted with a file system.

Steps

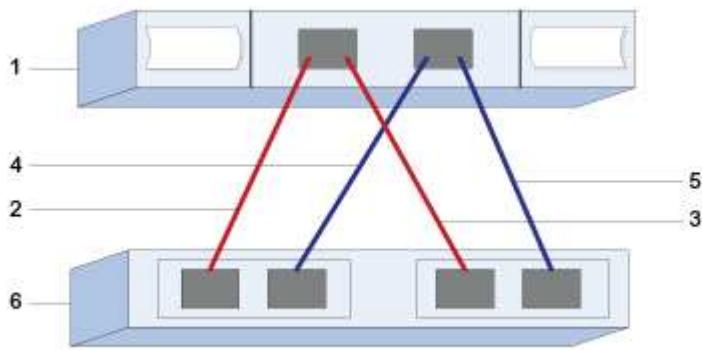
1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your SAS configuration

You can generate and print a PDF of this page, and then use the following worksheet to record SAS storage configuration information. You need this information to perform provisioning tasks.



Host identifiers

| Callout No. | Host (initiator) port connections | SAS address |
|-------------|-----------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |

| Callout No. | Host (initiator) port connections | SAS address |
|-------------|---|-------------|
| 2 | Host (initiator) port 1 connected to Controller A, port 1 | |
| 3 | Host (initiator) port 1 connected to Controller B, port 1 | |
| 4 | Host (initiator) port 2 connected to Controller A, port 1 | |
| 5 | Host (initiator) port 2 connected to Controller B, port 1 | |

Target identifiers

Recommended configurations consist of two target ports.

Mapping host

| | |
|-------------------|--|
| Mapping Host Name | |
| Host OS Type | |

iSCSI Setup

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.

The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from [NetApp Support](#).



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|---|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> Go to the directory where the SMIA*.bin installation package is located. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin Run the chmod +x SMIA*.bin command to grant execute permission to the file. Run the ./SMIA*.bin command to start the installer. |

- Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

If you are an iSCSI user, you closed the Setup wizard while configuring iSCSI.

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

5. Do one of the following to enable the multipathd daemon on boot.

| If you are using.... | Do this... |
|-----------------------------|--|
| RHEL 7.x and 8.x systems: | <code>systemctl enable multipathd</code> |
| SLES 12.x and 15.x systems: | <code>systemctl enable multipathd</code> |

6. Rebuild the `initramfs` image or the `initrd` image under `/boot` directory:

| If you are using.... | Do this... |
|-----------------------------|---|
| RHEL 7.x and 8.x systems: | <code>dracut --force --add multipath</code> |
| SLES 12.x and 15.x systems: | <code>dracut --force --add multipath</code> |

7. Use the "Create host manually" procedure in the online help to check whether the hosts are defined. Verify that each host type is either **Linux DM-MP (Kernel 3.10 or later)** if you enable the Automatic Load Balancing feature, or **Linux DM-MP (Kernel 3.9 or earlier)** if you disable the Automatic Load Balancing feature. If necessary, change the selected host type to the appropriate setting.
8. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd. Any line in the file with a first non-white-space character of # is considered a comment line.



For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

The multipath.conf files are available in the following locations:

- For SLES:

```
/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic
```

- For RHEL:

```
/usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf
```

Configure the switches

You configure the switches according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as code updates.

You must ensure the following:

- You have two separate networks for high availability. Make sure that you isolate your iSCSI traffic to separate network segments.
- You must enable flow control **end to end**.
- If appropriate, you have enabled jumbo frames.



Port channels/LACP is not supported on the controller's switch ports. Host-side LACP is not recommended; multipathing provides the same benefits, and in some cases, better benefits.

Configure networking

You can set up your iSCSI network in many ways, depending on your data storage requirements.

Consult your network administrator for tips on selecting the best configuration for your environment.

To configure an iSCSI network with basic redundancy, connect each host port and one port from each controller to separate switches, and partition each set of host ports and controller ports on separate network segments or VLANs.

You must enable send and receive hardware flow control **end to end**. You must disable priority flow control.

If you are using jumbo frames within the IP SAN for performance reasons, make sure to configure the array, switches, and hosts to use jumbo frames. Consult your operating system and switch documentation for information on how to enable jumbo frames on the hosts and on the switches. To enable jumbo frames on the

array, complete the steps in [Configure array-side networking](#).



Many network switches must be configured above 9,000 bytes for IP overhead. Consult your switch documentation for more information.

Configure array-side networking

You use the SANtricity System Manager GUI to configure iSCSI networking on the array side.

What you'll need

- The IP address or domain name for one of the storage array controllers.
- A password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service configured for the appropriate security access to the storage array. See the SANtricity System Manager online help for more information about Access Management.

About this task

This task describes how to access the iSCSI port configuration from System Manager's Hardware page. You can also access the configuration from **System > Settings > Configure iSCSI ports**.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Close the Setup wizard.

You will use the wizard later to complete additional setup tasks.

4. Select **Hardware**.

5. If the graphic shows the drives, click **Show back of shelf**.

The graphic changes to show the controllers instead of the drives.

6. Click the controller with the iSCSI ports you want to configure.

The controller's context menu appears.

7. Select **Configure iSCSI ports**.

The Configure iSCSI Ports dialog box opens.

8. In the drop-down list, select the port you want to configure, and then click **Next**.
9. Select the configuration port settings, and then click **Next**.

To see all port settings, click the **Show more port settings** link on the right of the dialog box.

| Port Setting | Description |
|---|---|
| Configured ethernet port speed | <p>Select the desired speed. The options that appear in the drop-down list depend on the maximum speed that your network can support (for example, 10 Gbps).</p> <p> The optional 25Gb iSCSI host interface cards available on the controllers do not auto-negotiate speeds. You must set the speed for each port to either 10 Gb or 25 Gb. All ports must be set to the same speed.</p> |
| Enable IPv4 / Enable IPv6 | Select one or both options to enable support for IPv4 and IPv6 networks. |
| TCP listening port (Available by clicking Show more port settings .) | <p>If necessary, enter a new port number.</p> <p>The listening port is the TCP port number that the controller uses to listen for iSCSI logins from host iSCSI initiators. The default listening port is 3260. You must enter 3260 or a value between 49152 and 65535.</p> |
| MTU size (Available by clicking Show more port settings .) | <p>If necessary, enter a new size in bytes for the Maximum Transmission Unit (MTU).</p> <p>The default Maximum Transmission Unit (MTU) size is 1500 bytes per frame. You must enter a value between 1500 and 9000.</p> |
| Enable ICMP PING responses | Select this option to enable the Internet Control Message Protocol (ICMP). The operating systems of networked computers use this protocol to send messages. These ICMP messages determine whether a host is reachable and how long it takes to get packets to and from that host. |

If you selected **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you selected **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you selected both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

10. Configure the IPv4 and/or IPv6 settings, either automatically or manually. To see all port settings, click the **Show more settings** link on the right of the dialog box.

| Port setting | Description |
|---------------------------------------|--|
| Automatically obtain configuration | Select this option to obtain the configuration automatically. |
| Manually specify static configuration | Select this option, and then enter a static address in the fields. For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address. |

11. Click **Finish**.

12. Close System Manager.

Configure host-side networking

To configure host-side networking, you must perform several steps.

About this task

You configure iSCSI networking on the host side by setting the number of node sessions per physical path, turning on the appropriate iSCSI services, configuring the network for the iSCSI ports, creating iSCSI face bindings, and establishing the iSCSI sessions between initiators and targets.

In most cases, you can use the inbox software-initiator for iSCSI CNA/NIC. You do not need to download the latest driver, firmware, and BIOS. Refer to the [NetApp Interoperability Matrix Tool](#) to determine code requirements.

Steps

1. Check the `node.session.nr_sessions` variable in the `/etc/iscsi/iscsid.conf` file to see the default number of sessions per physical path. If necessary, change the default number of sessions to one session.

```
node.session.nr_sessions = 1
```

2. Change the `node.session.timeo.replacement_timeout` variable in the `/etc/iscsi/iscsid.conf` file to 20, from a default value of 120.

```
node.session.timeo.replacement_timeout=20
```

3. Make sure `iscsid` and `(open-)iscsi` services are on and enabled for boot.

Red Hat Enterprise Linux 7 and 8 (RHEL 7 and RHEL 8)

```
# systemctl start iscsi  
# systemctl start iscsid  
# systemctl enable iscsi  
# systemctl enable iscsid
```

SUSE Linux Enterprise Server 12 and 15 (SLES 12 and SLES 15)

```
# systemctl start iscsid.service  
# systemctl enable iscsid.service
```

Optionally, you set `node.startup = automatic` in `/etc/iscsi/iscsid.conf` before running any `iscsiadm` commands to have sessions persist after reboot.

4. Get the host IQN initiator name, which will be used to configure the host to an array.

```
# cat /etc/iscsi/initiatorname.iscsi
```

5. Configure the network for iSCSI ports:



In addition to the public network port, iSCSI initiators should use two or more NICs on separate private segments or VLANs.

- Determine the iSCSI port names using the `# ifconfig -a` command.
- Set the IP address for the iSCSI initiator ports. The initiator ports should be present on the same subnet as the iSCSI target ports.

```
# vim /etc/sysconfig/network-scripts/ifcfg-<NIC port>  
Edit:  
BOOTPROTO=none  
ONBOOT=yes  
NM_CONTROLLED=no  
Add:  
IPADDR=192.168.xxx.xxx  
NETMASK=255.255.255.0
```



Be sure to set the address for both iSCSI initiator ports.

- Restart network services.

```
# systemctl restart network
```

- Make sure the Linux server can ping *all* of the iSCSI target ports.

6. Configure the iSCSI interfaces by creating two iSCSI iface bindings.

```
iscsiadm -m iface -I iface0 -o new  
iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v <NIC  
port1>
```

```
iscsiadm -m iface -I ifacel -o new  
iscsiadm -m iface -I ifacel -o update -n iface.net_ifacename -v <NIC  
port2>
```



To list the interfaces, use `iscsiadm -m iface`.

7. Establish the iSCSI sessions between initiators and targets (four total).

- Discover iSCSI targets. Save the IQN (it will be the same with each discovery) in the worksheet for the next step.

```
iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I iface0 -P  
1
```



The IQN looks like the following:

```
iqn.1992-01.com.netapp:2365.60080e50001bf160000000531d7be3
```

- Create the connection between the iSCSI initiators and iSCSI targets, using ifaces.

```
iscsiadm -m node -T iqn.1992-  
01.com.netapp:2365.60080e50001bf160000000531d7be3  
-p 192.168.0.1:3260 -I iface0 -l
```

- List the iSCSI sessions established on the host.

```
# iscsiadm -m session
```

Verify IP network connections

You verify Internet Protocol (IP) network connections by using ping tests to ensure the host and array are able to communicate.

Steps

1. On the host, run one of the following commands, depending on whether jumbo frames are enabled:

- If jumbo frames are not enabled, run this command:

```
ping -I <hostIP\> <targetIP\>
```

- If jumbo frames are enabled, run the ping command with a payload size of 8,972 bytes. The IP and ICMP combined headers are 28 bytes, which when added to the payload, equals 9,000 bytes. The -s switch sets the packet size bit. The -d switch sets the debug option. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

```
ping -I <hostIP\> -s 8972 -d <targetIP\>
```

In this example, the iSCSI target IP address is 192.0.2.8.

```
#ping -I 192.0.2.100 -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Issue a ping command from each host's initiator address (the IP address of the host Ethernet port used for iSCSI) to each controller iSCSI port. Perform this action from each host server in the configuration, changing the IP addresses as necessary.



If the command fails (for example, returns Packet needs to be fragmented but DF set), verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the ls command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

          E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
          Volume Name:
          Preferred Owner: Controller in Slot B
          Current Owner: Controller in Slot B
          Mode: RDAC (Active/Active)
          UTM LUN: None
          LUN: 116
          LUN Size:
          Product: E-Series
          Host Device:
mpathr(360080e50004300ac000007575568851d)
          Multipath Policy: round-robin 0
          Multipath Provider: Native
-----
-----
host      controller                      controller
path      path        /dev/    host      target
state     type       node     adapter   port
-----
-----
up        secondary    sdcx    host14    A1
up        secondary    sdat    host10    A2
up        secondary    sdbv    host13    B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

Before using the volume, you verify that the host can write data to the volume and read it back.

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

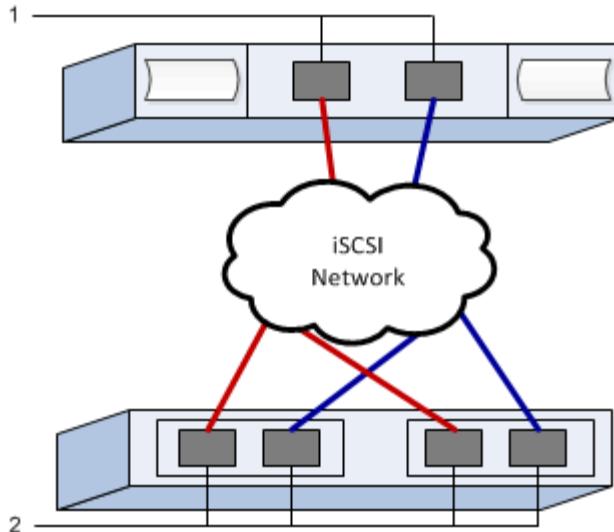
Remove the file and folder that you copied.

Record your iSCSI configuration

You can generate and print a PDF of this page, and then use the following worksheet to record iSCSI storage configuration information. You need this information to perform provisioning tasks.

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports with one or more VLANs.



Target IQN

| Callout No. | Target port connection | IQN |
|-------------|------------------------|-----|
| 2 | Target port | |

Mapping host name

| Callout No. | Host information | Name and type |
|-------------|-------------------|---------------|
| 1 | Mapping host name | |
| | Host OS type | |

iSER over InfiniBand Setup

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.

6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HBA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Enable Subnet Manager on each port of the connected HCA on the host:

SLES example

- ° Add the following two lines to `/etc/rc.d/rc.after`. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

RHEL example

- ° Add the following two lines to `/etc/rc.d/rc.local`. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.

The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from [NetApp Support](#).



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|---|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> Go to the directory where the SMIA*.bin installation package is located. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin Run the chmod +x SMIA*.bin command to grant execute permission to the file. Run the ./SMIA*.bin command to start the installer. |

- Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.

- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is

disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r  
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

5. Do one of the following to enable the multipathd daemon on boot.

| If you are using.... | Do this... |
|-----------------------------|--|
| RHEL 7.x and 8.x systems: | <code>systemctl enable multipathd</code> |
| SLES 12.x and 15.x systems: | <code>systemctl enable multipathd</code> |

6. Rebuild the initramfs image or the initrd image under /boot directory:

| If you are using.... | Do this... |
|-----------------------------|---|
| RHEL 7.x and 8.x systems: | <code>dracut --force --add multipath</code> |
| SLES 12.x and 15.x systems: | <code>dracut --force --add multipath</code> |

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

For example, for grub it is /boot/grub/menu.lst and for grub2 it is /boot/grub2/menu.cfg.

8. Use the "Create host manually" procedure in the online help to check whether the hosts are defined. Verify that each host type is either **Linux DM-MP (Kernel 3.10 or later)** if you enable the Automatic Load Balancing feature, or **Linux DM-MP (Kernel 3.9 or earlier)** if you disable the Automatic Load Balancing feature. If necessary, change the selected host type to the appropriate setting.

9. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd. Any line in the file with a first non-white-space character of # is considered a comment line.



For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

The multipath.conf files are available in the following locations:

- For SLES:

```
/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic
```

- For RHEL:

```
/usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf
```

Configure network connections

If your configuration uses the iSER over InfiniBand protocol, perform the steps in this section to configure network connections.

Steps

1. From System Manager, go to **Settings > System > Configure iSER over Infiniband Ports**. Refer to the System Manager online help for further instructions.

Put the array iSCSI addresses on the same subnet as the host port(s) you will use to create iSCSI sessions. For addresses, see your [iSER worksheet](#).

2. Record the IQN.

This information might be necessary when you create iSER sessions from operating systems that do not support send targets discovery. Enter this information in the [iSER worksheet](#).

Configure networking for storage attached hosts

If your configuration uses the iSER over InfiniBand protocol, perform the steps in this section.

The InfiniBand OFED driver stack supports running both iSER and SRP simultaneously on the same ports, so no additional hardware is required.

What you'll need

A NetApp recommended OFED installed on the system. For more information, see the [NetApp Interoperability Matrix Tool](#).

Steps

1. Enable and start iSCSI services on the host(s):

Red Hat Enterprise Linux 7 and 8 (RHEL 7 and RHEL 8)

```
# systemctl start iscsi  
# systemctl start iscsid  
# systemctl enable iscsi  
# systemctl enable iscsid
```

SUSE Linux Enterprise Server 12 and 15 (SLES 12 and SLES 15)

```
# systemctl start iscsid.service  
# systemctl enable iscsid.service
```

2. Configure IPoIB network interfaces:

- a. Identify the InfiniBand ports that will be used. Document the HW Address (MAC address) of each port.
- b. Configure persistent names for the InfiniBand network interface devices.
- c. Configure the IP address and network information for the IPoIB interfaces identified.

The specific interface configuration required might vary depending on the operating system used. Consult your vendor's operating system documentation for specific information on implementation.

- d. Start the IB network interfaces by restarting the networking service or by manually restarting each interface. For example:

```
systemctl restart network
```

- e. Verify connectivity to the target ports. From the host, ping the IP addresses you configured when you configured network connections.

3. Restart services to load the iSER module.

4. Edit the iSCSI settings in /etc/iscsi/iscsid.conf.

```
node.startup = automatic  
replacement_timeout = 20
```

5. Create iSCSI session configurations:

- a. Create iface configuration files for each InfiniBand interface.



The directory location for the iSCSI iface files is operating system dependent. This example is for using Red Hat Enterprise Linux:

```
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces iface-ib0  
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces iface-ib1
```

- b. Edit each iface file to set the interface name and initiator IQN. Set the following parameters appropriately for each iface file:

| Option | Value |
|---------------------|---|
| iface.net_ifacename | The interface device name (ex. ib0). |
| iface.initiatorname | The host initiator IQN documented in the worksheet. |

- c. Create iSCSI sessions to the target.

The preferred method to create the sessions is to use the SendTargets discovery method. However, this method does not work on some operating system releases.



Use **Method 2** for RHEL 6.x or SLES 11.3 or later.

- **Method 1 - SendTargets discovery:** Use the SendTargets discovery mechanism to one of the target portal IP addresses. This will create sessions for each of the target portals.

```
iscsiadm -m discovery -t st -p 192.168.130.101 -I iser
```

- **Method 2 - Manual creation:** For each target portal IP address, create a session using the appropriate host interface iface configuration. In this example, interface ib0 is on subnet A and interface ib1 is on subnet B. For these variables, substitute the appropriate value from the worksheet:
 - <Target IQN> = storage array Target IQN
 - <Target Port IP> = IP address configured on the specified target port

```
# Controller A Port 1  
iscsiadm -m node --target <Target IQN\> -I iface-ib0 -p <Target Port IP\> -l -o new  
# Controller B Port 1  
iscsiadm -m node --target <Target IQN\> -I iface-ib0 -p <Target Port IP\> -l -o new  
# Controller A Port 2  
iscsiadm -m node --target <Target IQN\> -I iface-ib1 -p <Target Port IP\> -l -o new  
# Controller B Port 2  
iscsiadm -m node --target <Target IQN\> -I iface-ib1 -p <Target Port IP\> -l -o new
```

6. Log in to iSCSI sessions.

For each session, run the iscsiadadm command to log in to the session.

```
# Controller A Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port
IP> -l
# Controller B Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port
IP> -l
# Controller A Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port
IP> -l
# Controller B Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port
IP> -l
```

7. Verify the iSER/iSCSI sessions.

- Check the iscsi session status from the host:

```
iscsiadm -m session
```

- Check the iscsi session status from the array. From SANtricity System Manager, navigate to **Storage Array > iSER > View/End Sessions**.

When the OFED/RDMA service starts, the iSER kernel module(s) loads by default when the iSCSI services are running. To complete the iSER connection setup, the iSER module(s) should be loaded. Currently this requires a host reboot.

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the ls command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

- Retrieve the SCSI ID of the mapped disk by issuing the sanlun lun show -p command.

The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

        E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
        Volume Name:
        Preferred Owner: Controller in Slot B
        Current Owner: Controller in Slot B
        Mode: RDAC (Active/Active)
        UTM LUN: None
        LUN: 116
        LUN Size:
        Product: E-Series
        Host Device:
mpathr(360080e50004300ac000007575568851d)
        Multipath Policy: round-robin 0
        Multipath Provider: Native
-----
-----
host      controller          controller
path      path        /dev/    host      target
state     type       node     adapter   port
-----
-----
up        secondary  sdcx    host14    A1
up        secondary  sdat    host10    A2
up        secondary  sdbv    host13    B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e500321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

Before using the volume, you verify that the host can write data to the volume and read it back.

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your iSER over IB configuration

You can generate and print a PDF of this page, and then use the following worksheet to record iSER over Infiniband storage configuration information. You need this information to perform provisioning tasks.

Host identifiers



The software initiator IQN is determined during the task, [Configure networking for storage attached hosts](#).

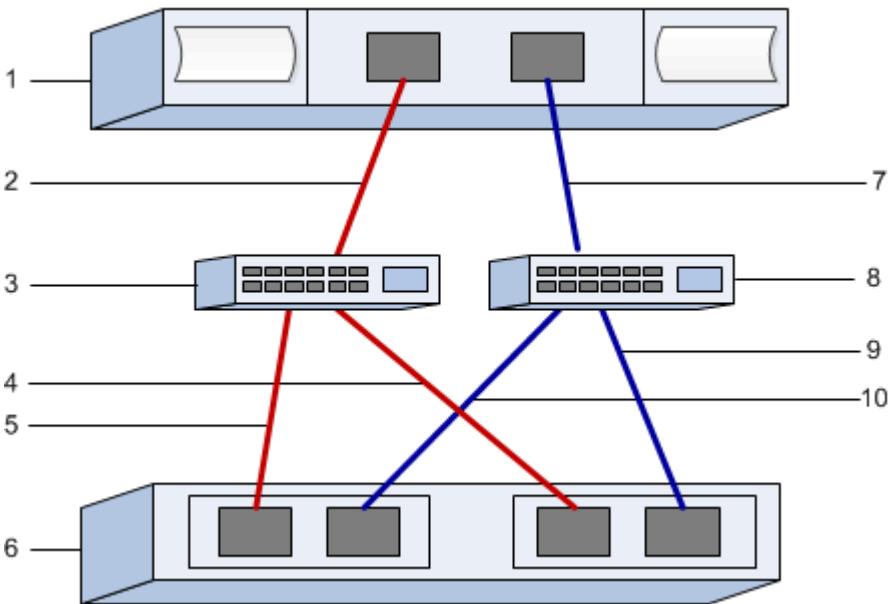
Locate and document the initiator IQN from each host. For software initiators, the IQN is typically found in the `/etc/iscsi/initiatorname.iscsi` file.

| Callout No. | Host port connections | Software initiator IQN |
|-------------|-----------------------|------------------------|
| 1 | Host (initiator) 1 | |
| n/a | | |
| n/a | | |

| Callout No. | Host port connections | Software initiator IQN |
|-------------|-----------------------|------------------------|
| n/a | | |
| n/a | | |

Recommended configuration

Recommended configurations consist of two host (initiator) ports and four target ports.



Target IQN

Document the target IQN for the storage array. You will use this information in [Configure networking for storage attached hosts](#).

Find the Storage Array IQN name using SANtricity: **Storage Array > iSER > Manage Settings**. This information might be necessary when you create iSER sessions from operating systems that do not support send targets discovery.

| Callout No. | Array name | Target IQN |
|-------------|---------------------------|------------|
| 6 | Array controller (target) | |

Network configuration

Document the network configuration that will be used for the hosts and storage on the InfiniBand fabric. These instructions assume that two subnets will be used for full redundancy.

Your network administrator can provide the following information. You use this information in the topic, [Configure networking for storage attached hosts](#).

Subnet A

Define the subnet to be used.

| Network Address | Netmask |
|-----------------|---------|
|-----------------|---------|

Document the IQNs to be used by the array ports and each host port.

| Callout No. | Array controller (target) port connections | IQN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 5 | Controller A, port 1 | |
| 4 | Controller B, port 1 | |
| 2 | Host 1, port 1 | |
| | (Optional) Host 2, port 1 | |

Subnet B

Define the subnet to be used.

| Network Address | Netmask |
|-----------------|---------|
|-----------------|---------|

Document the IQNs to be used by the array ports and each host port.

| Callout No. | Array controller (target) port connections | IQN |
|-------------|--|-----------------------|
| 8 | Switch | <i>not applicable</i> |
| 10 | Controller A, port 2 | |
| 9 | Controller B, port 2 | |
| 7 | Host 1, port 2 | |
| | (Optional) Host 2, port 2 | |

Mapping host name



The mapping host name is created during the workflow.

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

SRP over InfiniBand Setup

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
- Controller B, port 1: 169.254.128.102
- Subnet mask: 255.255.0.0

2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HBA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Enable Subnet Manager on each port of the connected HCA on the host:

SLES example

- Add the following two lines to `/etc/rc.d/rc.after`. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

RHEL example

- ° Add the following two lines to /etc/rc.d/rc.local. Substitute the values you found in step 2 for GUID0 and GUID1. For P0 and P1, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

Install and configure Linux Host Utilities

The Linux Unified Host Utilities package includes tools to manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.
The versions are listed in a column within each supported configuration.
2. Download the Unified Host Utilities from [NetApp Support](#).



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|--|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none">a. Go to the directory where the SMIA*.bin installation package is located.b. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.binc. Run the chmod +x SMIA*.bin command to grant execute permission to the file.d. Run the ./SMIA*.bin command to start the installer. |

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user

interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage

array can access.

- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

- Do one of the following to enable the `multipathd` daemon on boot.

| If you are using.... | Do this... |
|-----------------------------|--|
| RHEL 7.x and 8.x systems: | <code>systemctl enable multipathd</code> |
| SLES 12.x and 15.x systems: | <code>systemctl enable multipathd</code> |

- Rebuild the `initramfs` image or the `initrd` image under `/boot` directory:

| If you are using.... | Do this... |
|-----------------------------|---|
| RHEL 7.x and 8.x systems: | <code>dracut --force --add multipath</code> |
| SLES 12.x and 15.x systems: | <code>dracut --force --add multipath</code> |

- Make sure that the newly created `/boot/initrams-*` image or `/boot/initrd-*` image is selected in the boot configuration file.

For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

- Use the "Create host manually" procedure in the online help to check whether the hosts are defined. Verify that each host type is either **Linux DM-MP (Kernel 3.10 or later)** if you enable the Automatic Load Balancing feature, or **Linux DM-MP (Kernel 3.9 or earlier)** if you disable the Automatic Load Balancing feature. If necessary, change the selected host type to the appropriate setting.

- Reboot the host.

Set up the `multipath.conf` file

The `multipath.conf` file is the configuration file for the multipath daemon, `multipathd`.

The `multipath.conf` file overrides the built-in configuration table for `multipathd`. Any line in the file with a first non-white-space character of # is considered a comment line.



For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

The `multipath.conf` files are available in the following locations:

- For SLES:

`/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic`

- For RHEL:

`/usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf`

Determine host port GUIDs and make the recommended settings

The InfiniBand-diags package includes commands to display the globally unique ID (GUID) of each InfiniBand (IB) port. Most Linux distributions with OFED/RDMA supported through the included packages also have the InfiniBand-diags package, which includes commands to display information about the HCA.

Steps

1. Install the InfiniBand-diags package using the operating system's package management commands.
2. Run the `ibstat` command to display the port information.
3. Record the initiator's GUIDs on the [SRP worksheet](#).
4. Select the appropriate settings in the HBA utility.

Appropriate settings for your configuration are listed in the Notes column of the [NetApp Interoperability Matrix Tool](#).

Configure network connections—SRP over Infiniband

If your configuration uses the SRP over Infiniband protocol, follow the steps in this section.

What you'll need

To connect the Linux host to the storage array, you must enable the InfiniBand driver stack with the appropriate options. Specific settings might vary between Linux distributions. Check the [NetApp Interoperability Matrix Tool](#) for specific instructions and additional recommended settings specific to your solution.

Steps

1. Install the OFED/RDMA driver stack for your OS.

SLES

```
zypper install rdma-core
```

RHEL

```
yum install rdma-core
```

2. Configure OFED/RDMA to load the SRP module.

SLES

```
zypper install srp_daemon
```

RHEL

```
yum install srp_daemon
```

3. In the OFED/RDMA configuration file, set SRP_LOAD=yes and SRP_DAEMON_ENABLE=yes.

The RDMA configuration file is located at the following location:

```
/etc/rdma/rdma.conf
```

4. Enable and start the OFED/RDMA service.

RHEL 7.x and SLES 12.x or greater

- To enable the InfiniBand modules to load on boot:

```
systemctl enable rdma
```

- To load the InfiniBand modules immediately:

```
systemctl start rdma
```

5. Enable the SRP daemon.

RHEL 7.x and SLES 12 or greater

- To enable the SRP daemon to start on boot:

```
systemctl enable srp_daemon
```

- To start the SRP daemon immediately:

```
systemctl start srp_daemon
```

6. If you need to modify the SRP configuration, enter the following command to create /etc/modprobe.d/ib_srp.conf .

```
options ib_srp cmd_sg_entries=255 allow_ext_sg=y  
indirect_sg_entries=2048
```

- a. Under the /etc/srp_daemon.conf , add the following line.

```
a      max_sect=4096
```

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the `/dev/mapper` folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```

# sanlun lun show -p

        E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
        Volume Name:
        Preferred Owner: Controller in Slot B
        Current Owner: Controller in Slot B
        Mode: RDAC (Active/Active)
        UTM LUN: None
        LUN: 116
        LUN Size:
        Product: E-Series
        Host Device:
mpathr(360080e50004300ac000007575568851d)
        Multipath Policy: round-robin 0
        Multipath Provider: Native
-----
-----
host      controller                  controller
path      path          /dev/       host      target
state     type          node        adapter   port
-----
-----
up        secondary    sdcx        host14    A1
up        secondary    sdat        host10    A2
up        secondary    sdbv        host13    B1

```

2. Create a new partition according to the method appropriate for your Linux OS release.

Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```

# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%

```

3. Create a file system on the partition.

The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

Before using the volume, you verify that the host can write data to the volume and read it back.

What you'll need

An initialized volume that is formatted with a file system.

Steps

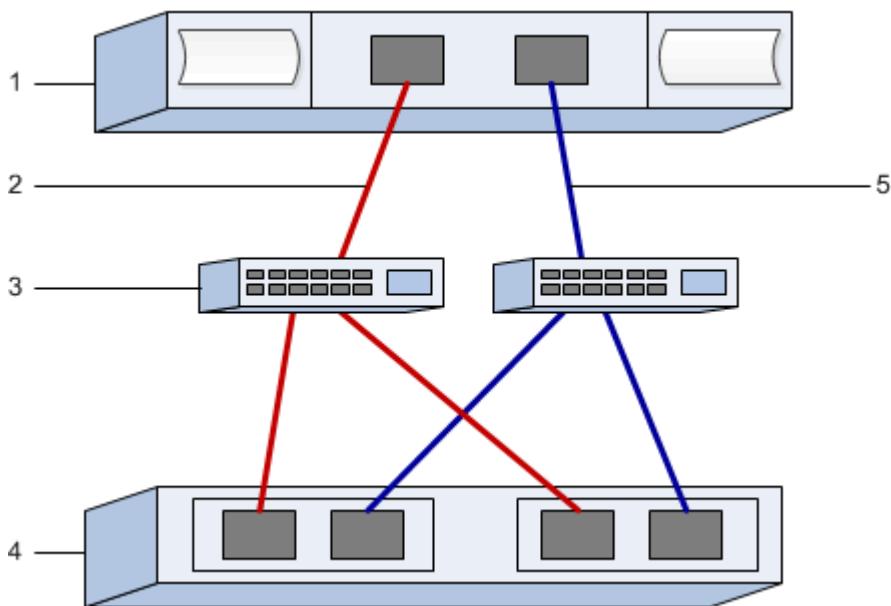
1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your SRP over IB configuration

You can generate and print a PDF of this page, and then use the following worksheet to record SRP over InfiniBand storage configuration information. You need this information to perform provisioning tasks.



Host identifiers



The initiator GUIDs are determined in the task, [Determine host port GUIDs and make the recommended settings](#).

| Callout No. | Host (initiator) port connections | GUID |
|-------------|---------------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 3 | Switch | <i>not applicable</i> |
| 4 | Target (storage array) | <i>not applicable</i> |
| 2 | Host port 1 to IB switch 1 ("A" path) | |
| 5 | Host port 2 to IB switch 2 ("B" path) | |

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports.

Mapping host name



The mapping host name is created during the workflow.

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

NVMe over InfiniBand Setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, host, and recovery restrictions.

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Review NVMe over InfiniBand restrictions

Before using NVMe over InfiniBand, review the controller, host, and recovery restrictions. For an up-to-date listing of all restrictions, see the [NetApp Interoperability Matrix Tool](#).

Controller restrictions

- NVMe over InfiniBand can be configured for EF300 (100GB controllers only), EF600, EF570, or E5700 controllers. The controllers must have 100GB or 200GB InfiniBand host ports.
- This protocol can be used only for EF300, EF600, EF570, or EF570 controllers. A minimum of 32 GB of physical memory is required to use this protocol on EF600, EF570, and E5700 controllers. For the EF300, a minimum of 16 GB of physical memory is required. If the minimum memory requirements for the controllers are not met during start of day operations, a message is displayed that helps you diagnose the problem.
- No simplex (single controller) configurations are supported.
- There is no support for mixed NVMe over InfiniBand and SCSI host interfaces.
- For EF300 controllers, no more than 64 NVMe hosts can be supported on the IB interface.

Host, host protocol, and host operating system restrictions

- The host must be running the latest compatible RHEL 7, SUSE Linux Enterprise Server 12 or 15 service pack operating system. See the [NetApp Interoperability Matrix Tool](#) for a complete list of the latest requirements.
- The only supported host channel adapters are from Mellanox. See the [NetApp Interoperability Matrix Tool](#) for more information.
- The only supported host interface card (HIC) is the 100G or 200G EDR IB HIC, which also supports iSER and SRP (but iSER and SRP are not supported simultaneously).

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|--|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXXX64-11.25.0A00.0002.bin c. Run the chmod +x SMIA*.bin command to grant execute permission to the file. d. Run the ./SMIA*.bin command to start the installer. |

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HCA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Enable Subnet Manager on each port of the connected HCA on the host:

SLES example

- Add the following two lines to `/etc/rc.d/rc.after`. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

RHEL example

- Add the following two lines to `/etc/rc.d/rc.local`. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest:

```
opensm -B -g GUID0 -p P0 -f /var/log/opensm-ib0.log
opensm -B -g GUID1 -p P1 -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
# cat /etc/rc.d/rc.local
opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

Set up NVMe over InfiniBand on the host side

Configuring an NVMe initiator in an InfiniBand environment includes installing and configuring the infiniband, nvme-cli, and rdma packages, configuring initiator IP addresses, and setting up the NVMe-oF layer on the host.

What you'll need

You must be running the latest compatible RHEL 7, RHEL 8, SUSE Linux Enterprise Server 12 or 15 service pack operating system. See the [NetApp Interoperability Matrix Tool](#) for a complete list of the latest requirements.

Steps

1. Install the rdma, nvme-cli, and infiniband packages:

SLES 12 or SLES 15

```
# zypper install infiniband-diags
# zypper install rdma-core
# zypper install nvme-cli
```

RHEL 7 or RHEL 8

```
# yum install infiniband-diags
# yum install rdma-core
# yum install nvme-cli
```

2. Enable ipoib. Edit the /etc/rdma/rdma.conf file and modify the entry for loading ipoib:

```
IPOIB_LOAD=yes
```

3. Check that both ib port links are up and the State = Active:

```
# ibstat
```

```

CA 'mlx4_0'
    CA type: MT4099
    Number of ports: 2
    Firmware version: 2.40.7000
    Hardware version: 1
    Node GUID: 0x0002c90300317850
    System image GUID: 0x0002c90300317853
    Port 1:
        State: Active
        Physical state: LinkUp
        Rate: 40
        Base lid: 4
        LMC: 0
        SM lid: 4
        Capability mask: 0x0259486a
        Port GUID: 0x0002c90300317851
        Link layer: InfiniBand
    Port 2:
        State: Active
        Physical state: LinkUp
        Rate: 56
        Base lid: 5
        LMC: 0
        SM lid: 4
        Capability mask: 0x0259486a
        Port GUID: 0x0002c90300317852
        Link layer: InfiniBand

```

4. Set up IPv4 IP addresses on the ib ports.

SLES 12 or SLES 15

Create the file /etc/sysconfig/network/ifcfg-ib0 with the following contents.

```

BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='10.10.10.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'

```

Then, create the file /etc/sysconfig/network/ifcfg-ib1.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='11.11.11.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 7 or RHEL 8

Create the file /etc/sysconfig/network-scripts/ifcfg-ib0 with the following contents.

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='10.10.10.100/24'
DEFROUTE=no
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib0
ONBOOT=yes
```

Then, create the file /etc/sysconfig/network-scripts/ifcfg-ib1:

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='11.11.11.100/24'
DEFROUTE=no
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib1
ONBOOT=yes
```

5. Enable the ib interface:

```
# ifup ib0  
# ifup ib1
```

6. Verify the IP addresses you will use to connect to the array. Run this command for both `ib0` and `ib1`:

```
# ip addr show ib0  
# ip addr show ib1
```

As shown in the example below, the IP address for `ib0` is `10.10.10.255`.

```
10: ib0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast  
state UP group default qlen 256  
    link/infiniband  
    80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd  
    00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff  
        inet 10.10.10.255 brd 10.10.10.255 scope global ib0  
            valid_lft forever preferred_lft forever  
        inet6 fe80::202:c903:31:7851/64 scope link  
            valid_lft forever preferred_lft forever
```

As shown in the example below, the IP address for `ib1` is `11.11.11.255`.

```
10: ib1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast  
state UP group default qlen 256  
    link/infiniband  
    80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd  
    00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff  
        inet 11.11.11.255 brd 11.11.11.255 scope global ib0  
            valid_lft forever preferred_lft forever  
        inet6 fe80::202:c903:31:7851/64 scope link  
            valid_lft forever preferred_lft forever
```

7. Set up the NVMe-oF layer on the host. Create the following files under `/etc/modules-load.d/` to load the `nvme-rdma` kernel module and make sure the kernel module will always be on, even after a reboot:

```
# cat /etc/modules-load.d/nvme-rdma.conf  
nvme-rdma
```

To verify the `nvme-rdma` kernel module is loaded, run this command:

```
# lsmod | grep nvme
nvme_rdma           36864  0
nvme_fabrics         24576  1 nvme_rdma
nvme_core            114688  5 nvme_rdma,nvme_fabrics
rdma_cm              114688  7
rpcrdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm
ib_core              393216  15
rdma_cm,ib_ipoib, rpcrdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_umad,
ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm
t10_pi               16384  2 sd_mod,nvme_core
```

Configure storage array NVMe over InfiniBand connections

If your controller includes an NVMe over InfiniBand port, you can configure the IP address of each port using SANtricity System Manager.

Steps

1. From the System Manager interface, select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.

The graphic changes to show the controllers instead of the drives.

3. Click the controller with the NVMe over InfiniBand ports you want to configure.

The controller's context menu appears.

4. Select **Configure NVMe over InfiniBand ports**.



The Configure NVMe over InfiniBand ports option appears only if System Manager detects NVMe over InfiniBand ports on the controller.

The **Configure NVMe over InfiniBand Ports** dialog box opens.

5. In the drop-down list, select the HIC port you want to configure, and then enter the IP address of the port.
6. Click **Configure**.
7. Repeat steps 5 and 6 for the other HIC ports that will be used.

Discover and connect to the storage from the host

Before making definitions of each host in SANtricity System Manager, you must discover the target controller ports from the host, and then establish NVMe connections.

Steps

1. Discover available subsystems on the NVMe-oF target for all paths using the following command:

```
nvme discover -t rdma -a target_ip_address
```

In this command, `target_ip_address` is the IP address of the target port.



The `nvme discover` command discovers all controller ports in the subsystem, regardless of host access.

```
# nvme discover -t rdma -a 10.10.10.100
Discovery Log Number of Records 2, Generation counter 0
=====Discovery Log Entry 0=====
trtype: rdma
adrfam: ipv4
subtype: nvme subsystem
treq: not specified
portid: 0
trsvcid: 4420
subnqn: nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
traddr: 10.10.10.100
rdma_prtype: infiniband
rdma_qptype: connected
rdma_cms: rdma-cm
rdma_pkey: 0x0000
=====Discovery Log Entry 1=====
trtype: rdma
adrfam: ipv4
subtype: nvme subsystem
treq: not specified
portid: 1
trsvcid: 4420
subnqn: nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
traddr: 11.11.11.100
rdma_prtype: infiniband
rdma_qptype: connected
rdma_cms: rdma-cm
rdma_pkey: 0x0000
```

2. Repeat step 1 for any other connections.

3. Connect to the discovered subsystem on the first path using the command: `nvme connect -t rdma -n discovered_sub_nqn -a target_ip_address -Q queue_depth_setting -l controller_loss_timeout_period`



The above command does not persist through reboot. The `NVMe connect` command will need to be executed after each reboot to re-establish the NVMe connections.



The NVMe connections do not persist through system reboot or extended periods of the controller being unavailable.

- i Connections are not established for any discovered port inaccessible by the host.
- i If you specify a port number using this command, the connection fails. The default port is the only port set up for connections.
- i The recommended queue depth setting is 1024. Override the default setting of 128 with 1024 using the `-Q 1024` command line option, as shown in the following example.
- i The recommended controller loss timeout period in seconds is 60 minutes (3600 seconds). Override the default setting of 600 seconds with 3600 seconds using the `-l 3600` command line option, as shown in the following example:

```
# nvme connect -t rdma -a 10.10.10.100 -n nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

4. Use the `nvme list` command to see a list of the NVMe devices currently connected. In the example below, it is `nvme0n1`.

| # nvme list | | | | |
|---------------------------|--------------|-----------------|-----------|--|
| Node | SN | Model | Namespace | |
| <code>/dev/nvme0n1</code> | 021648023161 | NetApp E-Series | 1 | |

| Usage | Format | FW Rev |
|-------------------|-------------|----------|
| 5.37 GB / 5.37 GB | 512 B + 0 B | 0842XXXX |

5. Connect to the discovered subsystem on the second path:

```
# nvme connect -t rdma -a 11.11.11.100 -n nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

6. Use the Linux `lsblk` and `grep` commands to show additional information about each block device:

| # lsblk grep nvme | | | | | |
|----------------------|-------|---|----|---|------|
| <code>nvme0n1</code> | 259:0 | 0 | 5G | 0 | disk |
| <code>nvme1n1</code> | 259:0 | 0 | 5G | 0 | disk |

7. Use the `nvme list` command to see a new list of the NVMe devices currently connected. In the example

below, it is `nvme0n1` and `nvme1n1`.

| # nvme list | | | | |
|--------------|--------------|-----------------|-----------|--|
| Node | SN | Model | Namespace | |
| <hr/> | | | | |
| /dev/nvme0n1 | 021648023161 | NetApp E-Series | 1 | |
| /dev/nvme1n1 | 021648023161 | NetApp E-Series | 1 | |

| Usage | Format | FW Rev |
|------------------|-------------|----------|
| <hr/> | | |
| 5.37 GB /5.37 GB | 512 B + 0 B | 0842XXXX |
| 5.37 GB /5.37 GB | 512 B + 0 B | 0842XXXX |

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage > Hosts**.

2. Click **Create > Host**.

The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

| Setting | Description |
|---------|-------------------------------|
| Name | Type a name for the new host. |

| Setting | Description |
|----------------------------|--|
| Host operating system type | <p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • Linux for SANtricity 11.60 and newer • Linux DM-MP (Kernel 3.10 or later) for pre-SANtricity 11.60 |
| Host interface type | Select the host interface type that you want to use. |
| Host ports | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Select I/O Interface If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • Manual add If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the Host ports field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the Host ports field. If necessary, you also can remove an identifier by selecting the X next to it. |

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is <Hostname_Port Number>. For example, the default alias for the first port created for host IPT is IPT_1.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more

namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage > Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.
A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.
3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command. The output `<format>` can be normal (the default if `-o` is not used), column, or json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`



Refer to [NetApp Interoperability Matrix Tool](#) to ensure any required updates are installed as multipathing may not work correctly with the GA versions of SLES or RHEL.

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing when using NVMe over Infiniband. RHEL 8 and SLES 15 use a built in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the /etc/multipath.conf file, as shown in the following example:

```
devices {
    device {
        vendor "NVME"
        product "NetApp E-Series*"
        path_grouping_policy group_by_prio
        fallback immediate
        no_path_retry 30
    }
}
```

2. Configure multipathd to start at system boot.

```
# systemctl enable multipathd
```

3. Start multipathd if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of multipathd to make sure it is active and running:

```
# systemctl status multipathd
```

Setting up RHEL 8 with Native NVMe Multipathing

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the steps below.

1. Setup modprobe rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-nvme_core.conf
```

2. Remake `initramfs` with new `modprobe` parameter.

```
# dracut -f
```

3. Reboot server to bring it up with the Native NVMe Multipathing enabled.

```
# reboot
```

4. Verify Native NVMe Multipathing has been enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

a. If the command output is `N`, then Native NVMe Multipathing is still disabled.

b. If the command output is `Y`, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.



For SLES 15, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the `dm` device or the `symlink` in `/dev/mapper`. For example:

```
/dev/dm-1  
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example output

The following example output from the `nvme list` command shows the host node name and its correlation with the namespace ID.

| NODE | SN | MODEL | NAMESPACE |
|--------------|--------------|-----------------|-----------|
| /dev/nvme1n1 | 021648023072 | NetApp E-Series | 10 |
| /dev/nvme1n2 | 021648023072 | NetApp E-Series | 11 |
| /dev/nvme1n3 | 021648023072 | NetApp E-Series | 12 |
| /dev/nvme1n4 | 021648023072 | NetApp E-Series | 13 |
| /dev/nvme2n1 | 021648023151 | NetApp E-Series | 10 |
| /dev/nvme2n2 | 021648023151 | NetApp E-Series | 11 |
| /dev/nvme2n3 | 021648023151 | NetApp E-Series | 12 |
| /dev/nvme2n4 | 021648023151 | NetApp E-Series | 13 |

| Column | Description |
|-----------|--|
| Node | <p>The node name includes two parts:</p> <ul style="list-style-type: none"> The notation <code>nvme1</code> represents controller A and <code>nvme2</code> represents controller B. The notation <code>n1</code>, <code>n2</code>, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B. |
| Namespace | <p>The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.</p> |

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwandler='0' wp=rw
|--- policy='service-time 0' prio=50 status=active
|   `-- #:#:#:# nvme1n1 259:5 active ready running
`--- policy='service-time 0' prio=10 status=enabled
    `-- #:#:#:# nvme2n1 259:9 active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwandler='0' wp=rw
|--- policy='service-time 0' prio=0 status=enabled
|   `-- #:#:#:# nvme1n1 259:5 failed faulty running
`--- policy='service-time 0' prio=10 status=active
    `-- #:#:#:# nvme2n1 259:9 active ready running
```

| Line item | Description |
|---|---|
| policy='service-time 0' prio=50 status=active | This line and the following line show that nvme1n1, which is the namespace with an NSID of 10, is optimized on the path with a <code>prio</code> value of 50 and a <code>status</code> value of <code>active</code> . This namespace is owned by controller A. |
| policy='service-time 0' prio=10 status=enabled | This line shows the failover path for namespace 10, with a <code>prio</code> value of 10 and a <code>status</code> value of <code>enabled</code> . I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B. |
| policy='service-time 0' prio=0 status=enabled | This example shows <code>multipath -ll</code> output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as <code>failed faulty running</code> with a <code>prio</code> value of 0 and a <code>status</code> value of <code>enabled</code> . |
| policy='service-time 0' prio=10 status=active | Note that the <code>active</code> path refers to nvme2, so the I/O is being directed on this path to controller B. |

Access NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8 and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

It is best practice to use the links in `/dev/disk/by-id/` rather than `/dev/nvme0n1`. For example:

```
# ls /dev/disk/by-id/ -l lrwxrwxrwx 1 root root 13 Oct 18 15:14
nvme-eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

Physical NVMe devices are I/O targets

Run I/O to the physical nvme device path. There should only be one of these devices present for each namespace using the following format:

```
/dev/nvme[subsys#]n[id#]
```

All paths are virtualized using the native multipathing solution underneath this device.

You can view your paths by running:

```
# nvme list-subsy
```

Example output:

```
nvme-subsy0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a namespace device when using the 'nvme list-subsy' command, it provides additional information about the paths to that namespace:

```
# nvme list-subsy /dev/nvme0n1
nvme-subsy0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af4462000000058d5dd96
\
+- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
+- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
+- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
+- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```



To view the path information, the following must be set in /etc/multipath.conf:

```
defaults {
    enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-Series,08520001  
size=4194304 features='n/a' hwhandler='ANA' wp=rw  
|-- policy='n/a' prio=50 status=optimized  
| `-- 0:0:1 nvme0c0n1 0:0 n/a optimized live  
`-- policy='n/a' prio=10 status=non-optimized  
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized live
```

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the namespace and mount the filesystem.

Steps

1. Run the multipath -ll command to get a list of /dev/mapper/dm devices.

```
# multipath -ll
```

The result of this command shows two devices, dm-19 and dm-16:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series  
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n19 259:19 active ready running  
| `-- #:#:#:# nvme1n19 259:115 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n19 259:51 active ready running  
  `-- #:#:#:# nvme3n19 259:83 active ready running  
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series  
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n16 259:16 active ready running  
| `-- #:#:#:# nvme1n16 259:112 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n16 259:48 active ready running  
  `-- #:#:#:# nvme3n16 259:80 active ready running
```

2. Create a file system on the partition for each /dev/mapper/eui- device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an ext4 file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8 and SLES 15)

For RHEL 8 and SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/nvme` devices.

```
# multipath -ll
```

The result of this command shows device `nvme0n6`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe, NetApp E-
Series, 08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:1:1 nvme0c1n1 0:0 n/a optimized    live
|--- policy='n/a' prio=10 status=non-optimized
|   `-- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`--- policy='n/a' prio=10 status=non-optimized
   `-- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for each /dev/nvme0n# device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, you verify that the host can write data to the namespace and read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your NVMe over IB configuration

You can generate and print a PDF of this page, and then use the following worksheet to record NVMe over InfiniBand storage configuration information. You need this information to perform provisioning tasks.

Host identifiers



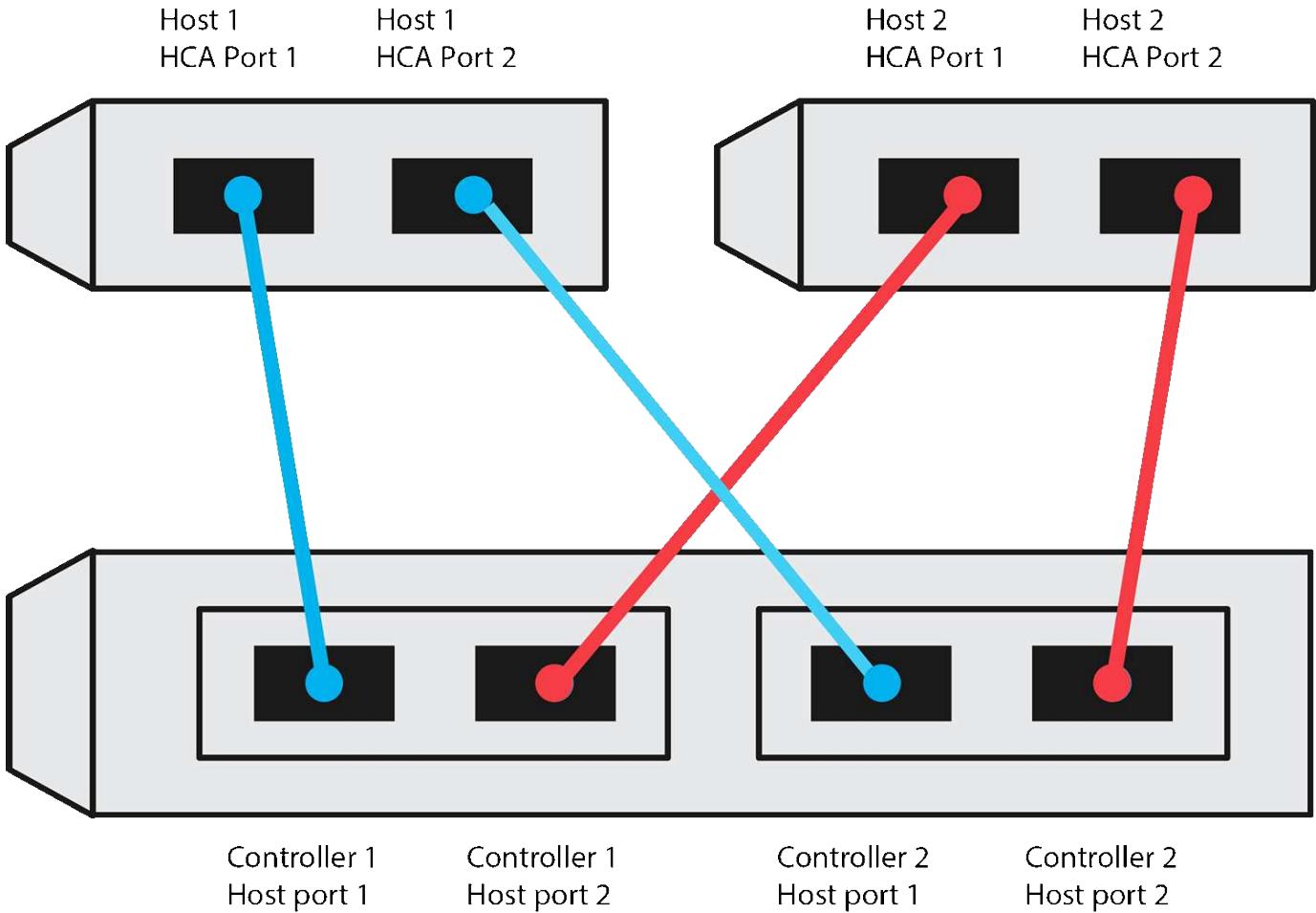
The software initiator NQN is determined during the task.

Locate and document the initiator NQN from each host. The NQN is typically found in the `/etc/nvme/hostnqn` file.

| Callout No. | Host port connections | Host NQN |
|-------------|-----------------------|----------|
| 1 | Host (initiator) 1 | |
| n/a | | |

Recommended configuration

In a direct connect topology, one or more hosts are directly connected to the subsystem. In the SANtricity OS 11.50 release, we support a single connection from each host to a subsystem controller, as shown below. In this configuration, one HCA (host channel adapter) port from each host should be on the same subnet as the E-Series controller port it is connected to, but on a different subnet from the other HCA port.



Target NQN

Document the target NQN for the storage array. You will use this information in [Configure storage array NVMe over InfiniBand connections](#).

Find the Storage Array NQN name using SANtricity: **Storage Array > NVMe over Infiniband > Manage Settings**. This information might be necessary when you create NVMe over InfiniBand sessions from operating systems that do not support send targets discovery.

| Callout No. | Array name | Target IQN |
|-------------|---------------------------|------------|
| 6 | Array controller (target) | |

Network configuration

Document the network configuration that will be used for the hosts and storage on the InfiniBand fabric. These instructions assume that two subnets will be used for full redundancy.

Your network administrator can provide the following information. You use this information in the topic, [Configure storage array NVMe over InfiniBand connections](#).

Subnet A

Define the subnet to be used.

| Network Address | Netmask |
|-----------------|---------|
|-----------------|---------|

Document the NQNs to be used by the array ports and each host port.

| Callout No. | Array controller (target) port connections | NQN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 5 | Controller A, port 1 | |
| 4 | Controller B, port 1 | |
| 2 | Host 1, port 1 | |
| | (Optional) Host 2, port 1 | |

Subnet B

Define the subnet to be used.

| Network Address | Netmask |
|-----------------|---------|
|-----------------|---------|

Document the IQNs to be used by the array ports and each host port.

| Callout No. | Array controller (target) port connections | NQN |
|-------------|--|-----------------------|
| 8 | Switch | <i>not applicable</i> |
| 10 | Controller A, port 2 | |
| 9 | Controller B, port 2 | |
| 7 | Host 1, port 2 | |
| | (Optional) Host 2, port 2 | |

Mapping host name



The mapping host name is created during the workflow.

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

NVMe over RoCE Setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, switch, host, and recovery restrictions.

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Verify NVMe over RoCE restrictions

Before using NVMe over RoCE, review the controller, switch, host, and recovery restrictions. For an up-to-date listing of all restrictions, see the [NetApp Interoperability Matrix Tool](#).

Controller restrictions

- NVME over RoCE can be configured for the EF300 (100GB controllers only), EF600, EF570, and E5700 controllers. The controllers must have 100GB or 200GB host port.
- This protocol can be used only for EF300, EF600, EF570, and E5700 controllers. A minimum of 32 GB of physical memory is required to use the protocol on EF600, EF570, and E5700 controllers. For the EF300, a minimum of 16 GB of physical memory is required. If the minimum memory requirements for the controllers are not met during start of day operations, a message is displayed that helps you diagnose the problem.
- No simplex (single-controller) configurations are supported.
- The only supported host interface card (HIC) is the 100G or 200G EDR HIC, which also supports NVMe over InfiniBand, iSER and SRP.
- There is no support for mixed NVMe over RoCE with NVMe over InfiniBand or SCSI host interfaces.

Switch restrictions



RISK OF DATA LOSS. You must enable Priority Flow Control or Global Pause Control on the switch to eliminate the risk of data loss in an NVMe over RoCE environment.

Host, host protocol, and host operating system restrictions

For a complete list of requirements, see the [NetApp Interoperability Matrix Tool](#).

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

 If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|---|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> Go to the directory where the SMIA*.bin installation package is located. If the temp mount point does not have execute permissions, set the IATEMPDIR variable. Example: IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin Run the chmod +x SMIA*.bin command to grant execute permission to the file. Run the ./SMIA*.bin command to start the installer. |

- Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.

- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the switch

You configure the switches according to the vendor's recommendations for NVMe over RoCE. These recommendations might include both configuration directives as well as code updates.



RISK OF DATA LOSS. You must enable Priority Flow Control or Global Pause Control on the switch to eliminate the risk of data loss in an NVMe over RoCE environment.

Steps

1. Enable Ethernet pause frame flow control **end to end** as the best practice configuration.
2. Consult your network administrator for tips on selecting the best configuration for your environment.

Set up NVMe over RoCE on the host side

NVMe initiator configuration in a RoCE environment includes installing and configuring the rdma-core and nvme-cli packages, configuring initiator IP addresses, and setting up the NVMe-oF layer on the host.

What you'll need

You must be running RHEL 7, RHEL 8, and the latest compatible SUSE Linux Enterprise Server 12 and 15 service pack operating system. See the [NetApp Interoperability Matrix Tool](#) for a complete list of the latest requirements.

Steps

1. Install the rdma and nvme-cli packages:

SLES 12 or SLES 15

```
# zypper install rdma-core  
# zypper install nvme-cli
```

RHEL 7 or RHEL 8

```
# yum install rdma-core  
# yum install nvme-cli
```

2. Set up IPv4 IP addresses on the ethernet ports used to connect NVMe over RoCE. For each network interface, create a configuration script that contains the different variables for that interface.

The variables used in this step are based on server hardware and the network environment. The variables include the IPADDR and GATEWAY. These are example instructions for SLES and RHEL:

SLES 12 and SLES 15

- Create the example file /etc/sysconfig/network/ifcfg-eth4 as follows:

```
BOOTPROTO='static'  
BROADCAST=  
ETHTOOL_OPTIONS=  
IPADDR='192.168.1.87/24'  
GATEWAY='192.168.1.1'  
MTU=  
NAME='MT27800 Family [ConnectX-5]'  
NETWORK=  
REMOTE_IPADDR=  
STARTMODE='auto'
```

- Create the file /etc/sysconfig/network/ifcfg-eth5 as follows:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 7 and RHEL 8

- Create the example file /etc/sysconfig/network-scripts/ifcfg-eth4 as follows:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.1.87/24'
GATEWAY='192.168.1.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

- Create the file /etc/sysconfig/network-scripts/ifcfg-eth5 as follows:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

3. Enable the network interfaces:

```
# ifup eth4  
# ifup eth5
```

4. Set up the NVMe-oF layer on the host.

- Create the following file under `/etc/modules-load.d/` to load the `nvme-rdma` kernel module and make sure the kernel module will always be on, even after a reboot:

```
# cat /etc/modules-load.d/nvme-rdma.conf  
nvme-rdma
```

To verify the `nvme-rdma` kernel module is loaded, run this command:

```
# lsmod | grep nvme  
nvme_rdma           36864  0  
nvme_fabrics        24576  1 nvme_rdma  
nvme_core           114688  5 nvme_rdma,nvme_fabrics  
rdma_cm             114688  7  
rprdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm  
ib_core             393216  15  
rdma_cm,ib_ipoib,rprdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_um  
ad,ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm  
t10_pi              16384  2 sd_mod,nvme_core
```

Configure storage array NVMe over RoCE connections

If your controller includes a connection for NVMe over RoCE (RDMA over Converged Ethernet), you can configure the NVMe port settings from the Hardware page or the System page in SANtricity System Manager.

What you'll need

- An NVMe over RoCE host port on your controller; otherwise, the NVMe over RoCE settings are not available in System Manager.
- The IP address of the host connection.

About this task

You can access the NVMe over RoCE configuration from the **Hardware** page or from **Settings > System**. This task describes how to configure the ports from the Hardware page.



The NVMe over RoCE settings and functions appear only if your storage array's controller includes an NVMe over RoCE port.

Steps

- From the System Manager interface, select **Hardware**.

2. Click the controller with the NVMe over RoCE port you want to configure.

The controller's context menu appears.

3. Select **Configure NVMe over RoCE ports**.

The **Configure NVMe over RoCE ports** dialog box opens.

4. In the drop-down list, select the port you want to configure, and then click **Next**.

5. Select the port configuration settings you want to use, and then click **Next**.

To see all port settings, click the **Show more port settings** link on the right of the dialog box.

| Port Setting | Description |
|---|--|
| Configured ethernet port speed | <p>Select the desired speed. The options that appear in the drop-down list depend on the maximum speed that your network can support (for example, 10 Gbps). Possible values include:</p> <ul style="list-style-type: none">• Auto-negotiate• 10 Gbps• 25 Gbps• 40 Gbps• 50 Gbps• 100 Gbps• 200 Gbps <p> When a 200Gb-capable HIC is attached with a QSFP56 cable, auto-negotiate is only available when you are connecting to Mellanox switches and/or adapters.</p> <p> The configured NVMe over RoCE port speed should match the speed capability of the SFP on the selected port. All ports must be set to the same speed.</p> |
| Enable IPv4 and/or Enable IPv6 | Select one or both options to enable support for IPv4 and IPv6 networks. |
| MTU size (Available by clicking Show more port settings .) | If necessary, enter a new size in bytes for the maximum transmission unit (MTU). The default MTU size is 1500 bytes per frame. You must enter a value between 1500 and 4200. |

If you selected **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you

selected **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you selected both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

6. Configure the IPv4 and/or IPv6 settings, either automatically or manually. To see all port settings, click the **Show more settings** link on the right of the dialog box.

| Port setting | Description |
|--|---|
| Automatically obtain configuration from DHCP server | Select this option to obtain the configuration automatically. |
| Manually specify static configuration | Select this option, and then enter a static address in the fields. For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP addresses and router IP address.  If there is only one routable IP address, set the remaining address to 0:0:0:0:0:0:0:0. |
| Enable VLAN support (Available by clicking Show more settings .) |  This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. |
| Enable ethernet priority (Available by clicking Show more settings .) |  This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. |

7. Click **Finish**.

Discover and connect to the storage from the host

Before making definitions of each host in SANtricity System Manager, you must discover the target controller ports from the host, and then establish NVMe connections.

Steps

1. Discover available subsystems on the NVMe-oF target for all paths using the following command:

```
nvme discover -t rdma -a target_ip_address
```

In this command, `target_ip_address` is the IP address of the target port.



The `nvme discover` command discovers all controller ports in the subsystem, regardless of host access.

```

# nvme discover -t rdma -a 192.168.1.77
Discovery Log Number of Records 2, Generation counter 0
=====Discovery Log Entry 0=====
trtype: rdma
adrfam: ipv4
subtype: nvme subsystem
treq: not specified
portid: 0
trsvcid: 4420
subnqn: nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr: 192.168.1.77
rdma_prttype: roce
rdma_qptype: connected
rdma_cms: rdma-cm
rdma_pkey: 0x0000
=====Discovery Log Entry 1=====
trtype: rdma
adrfam: ipv4
subtype: nvme subsystem
treq: not specified
portid: 1
trsvcid: 4420
subnqn: nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr: 192.168.2.77
rdma_prttype: roce
rdma_qptype: connected
rdma_cms: rdma-cm
rdma_pkey: 0x0000

```

2. Repeat step 1 for any other connections.
3. Connect to the discovered subsystem on the first path using the command: `nvme connect -t rdma -n discovered_sub_nqn-a target_ip_address -Q queue_depth_setting-l controller_loss_timeout_period`

- i The command listed above does not persist through reboot. The `NVMe connect` command will need to be executed after each reboot to re-establish the NVMe connections.
- i Connections are not established for any discovered port inaccessible by the host.
- i If you specify a port number using this command, the connection fails. The default port is the only port set up for connections.
- i The recommended queue depth setting is 1024. Override the default setting of 128 with 1024 using the `-Q 1024` command line option, as shown in the following example.



The recommended controller loss timeout period in seconds is 60 minutes (3600 seconds). Override the default setting of 600 seconds with 3600 seconds using the `-l 3600` command line option, as shown in the following example.

```
# nvme connect -t rdma -a 192.168.1.77 -n nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
# nvme connect -t rdma -a 192.168.2.77 -n nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
```

4. Repeat step 3 to connect the discovered subsystem on the second path.

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage > Hosts**.
2. Click **Create > Host**.

The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

| Setting | Description |
|----------------------------|---|
| Name | Type a name for the new host. |
| Host operating system type | Select one of the following options from the drop-down list: <ul style="list-style-type: none">• Linux for SANtricity 11.60 and newer• Linux DM-MP (Kernel 3.10 or later) for pre-SANtricity 11.60 |

| Setting | Description |
|---------------------|---|
| Host interface type | Select the host interface type that you want to use. If the array you configure only has one available host interface type, this setting may not be available to select. |
| Host ports | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Select I/O Interface If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • Manual add If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the Host ports field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the Host ports field. If necessary, you also can remove an identifier by selecting the X next to it. |

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is <Hostname_Port Number>. For example, the default alias for the first port created for host IPT is IPT_1.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage > Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.
A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.
3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command. The output `<format>` can be normal (the default if `-o` is not used), `column`, or `json`.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover on the host

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`



Refer to the [NetApp Interoperability Matrix Tool](#) to ensure any required updates are installed, as multipathing might not work correctly with the GA versions of SLES or RHEL.

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing for NVMe over RoCE. RHEL 8 and SLES 15 use a built-in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the `/etc/multipath.conf` file, as shown in the following example:

```
devices {
    device {
        vendor "NVME"
        product "NetApp E-Series*"
        path_grouping_policy group_by_prio
        fallback immediate
        no_path_retry 30
    }
}
```

2. Configure `multipathd` to start at system boot.

```
# systemctl enable multipathd
```

3. Start `multipathd` if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of `multipathd` to make sure it is active and running:

```
# systemctl status multipathd
```

Set up RHEL 8 with Native NVMe Multipathing

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the following procedure.

1. Set up the `modprobe` rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-nvme_core.conf
```

2. Remake `initramfs` with the new `modprobe` parameter.

```
# dracut -f
```

3. Reboot the server to bring it up with the Native NVMe Multipathing enabled.

```
# reboot
```

4. Verify that Native NVMe Multipathing is enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

- If the command output is `N`, then Native NVMe Multipathing is still disabled.
- If the command output is `Y`, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.



For SLES 15, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O that is directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the `dm` device or the symlink in `/dev/mapper`. For example:

```
/dev/dm-1  
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example

The following example output from the `nvme list` command shows the host node name and its correlation with the namespace ID.

| NODE | SN | MODEL | NAMESPACE |
|--------------|--------------|-----------------|-----------|
| /dev/nvme1n1 | 021648023072 | NetApp E-Series | 10 |
| /dev/nvme1n2 | 021648023072 | NetApp E-Series | 11 |
| /dev/nvme1n3 | 021648023072 | NetApp E-Series | 12 |
| /dev/nvme1n4 | 021648023072 | NetApp E-Series | 13 |
| /dev/nvme2n1 | 021648023151 | NetApp E-Series | 10 |
| /dev/nvme2n2 | 021648023151 | NetApp E-Series | 11 |
| /dev/nvme2n3 | 021648023151 | NetApp E-Series | 12 |
| /dev/nvme2n4 | 021648023151 | NetApp E-Series | 13 |

| Column | Description |
|-----------|--|
| Node | <p>The node name includes two parts:</p> <ul style="list-style-type: none"> The notation <code>nvme1</code> represents controller A and <code>nvme2</code> represents controller B. The notation <code>n1</code>, <code>n2</code>, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B. |
| Namespace | <p>The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.</p> |

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|--- policy='service-time 0' prio=50 status=active
|   `-- #:#:#:# nvme1n1 259:5 active ready running
`--- policy='service-time 0' prio=10 status=enabled
    `-- #:#:#:# nvme2n1 259:9 active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|--- policy='service-time 0' prio=0 status=enabled
|   `-- #:#:#:# nvme1n1 259:5 failed faulty running
`--- policy='service-time 0' prio=10 status=active
    `-- #:#:#:# nvme2n1 259:9 active ready running
```

| Line item | Description |
|---|---|
| policy='service-time 0' prio=50 status=active | This line and the following line show that nvme1n1, which is the namespace with an NSID of 10, is optimized on the path with a <code>prio</code> value of 50 and a <code>status</code> value of <code>active</code> . This namespace is owned by controller A. |
| policy='service-time 0' prio=10 status=enabled | This line shows the failover path for namespace 10, with a <code>prio</code> value of 10 and a <code>status</code> value of <code>enabled</code> . I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B. |
| policy='service-time 0' prio=0 status=enabled | This example shows <code>multipath -ll</code> output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as <code>failed faulty running</code> with a <code>prio</code> value of 0 and a <code>status</code> value of <code>enabled</code> . |
| policy='service-time 0' prio=10 status=active | Note that the <code>active</code> path refers to nvme2, so the I/O is being directed on this path to controller B. |

Accessing NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8 and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

It is best practice to use the links in `/dev/disk/by-id/` rather than `/dev/nvme0n1`. For example:

```
# ls /dev/disk/by-id/ -l lrwxrwxrwx 1 root root 13 Oct 18 15:14
nvme-eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

Physical NVMe devices are I/O targets

Run I/O to the physical nvme device path. There should only be one of these devices present for each namespace using the following format:

```
/dev/nvme[subsys#]n[id#]
```

All paths are virtualized using the native multipathing solution underneath this device.

You can view your paths by running:

```
# nvme list-subsys
```

Example output:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a namespace device when using the `nvme list-subsys` command, it provides additional information about the paths to that namespace:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
+- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
+- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
+- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
+- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```



To view the path information, the following must be set in `/etc/multipath.conf`:

```
defaults {
    enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-Series,08520001  
size=4194304 features='n/a' hwhandler='ANA' wp=rw  
|-- policy='n/a' prio=50 status=optimized  
| `-- 0:0:1 nvme0c0n1 0:0 n/a optimized live  
`-- policy='n/a' prio=10 status=non-optimized  
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized live
```

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the namespace and mount the filesystem.

Steps

1. Run the multipath -ll command to get a list of /dev/mapper/dm devices.

```
# multipath -ll
```

The result of this command shows two devices, dm-19 and dm-16:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series  
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n19 259:19 active ready running  
| `-- #:#:#:# nvme1n19 259:115 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n19 259:51 active ready running  
  `-- #:#:#:# nvme3n19 259:83 active ready running  
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series  
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n16 259:16 active ready running  
| `-- #:#:#:# nvme1n16 259:112 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n16 259:48 active ready running  
  `-- #:#:#:# nvme3n16 259:80 active ready running
```

2. Create a file system on the partition for each /dev/mapper/eui- device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an ext4 file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8 and SLES 15)

For RHEL 8 and SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/nvme` devices.

```
# multipath -ll
```

The result of this command shows device `nvme0n6`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe, NetApp E-
Series, 08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:1:1 nvme0c1n1 0:0 n/a optimized    live
|--- policy='n/a' prio=10 status=non-optimized
|   `-- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`--- policy='n/a' prio=10 status=non-optimized
   `-- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for each /dev/nvme0n# device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, verify that the host can write data to the namespace and read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

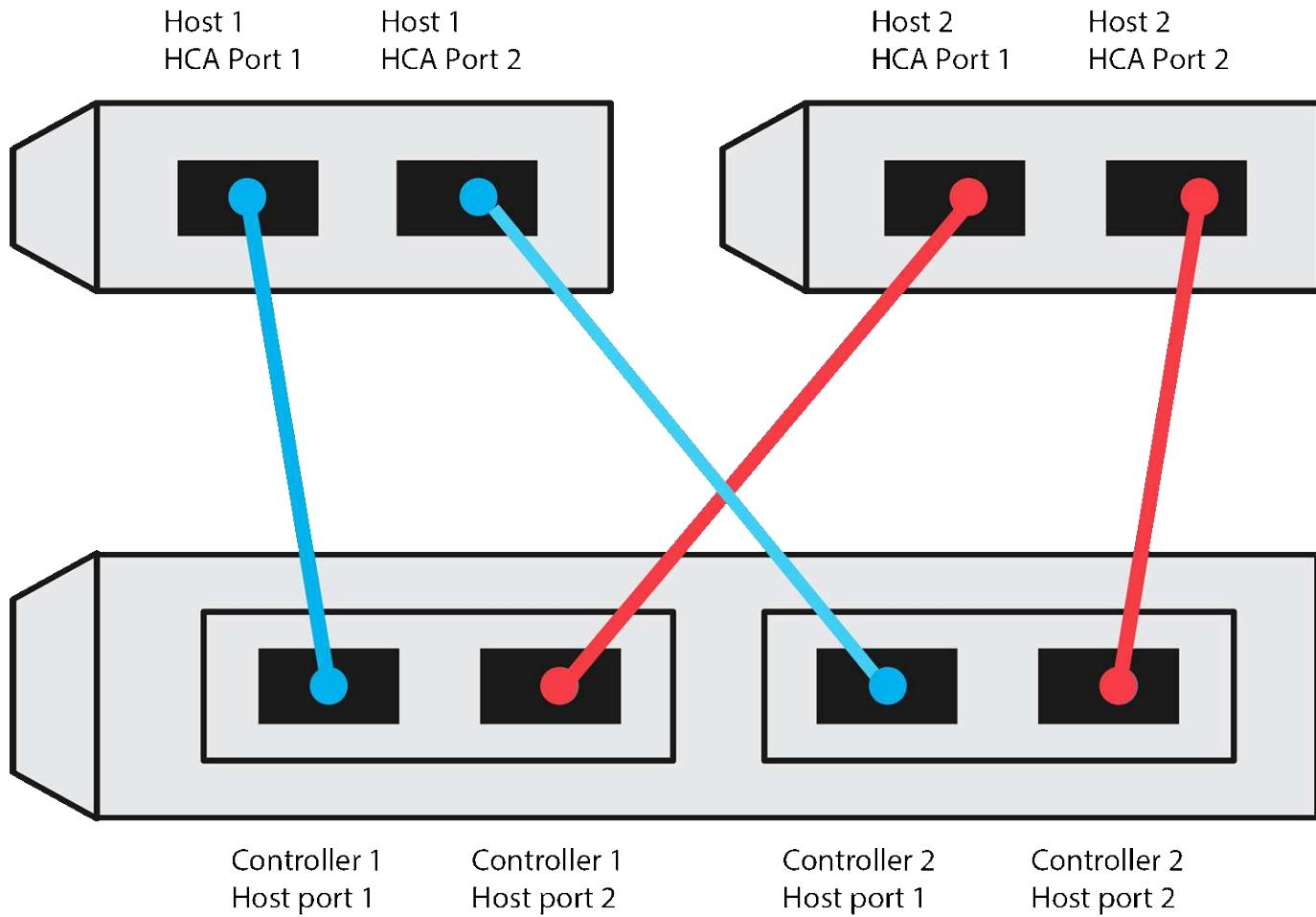
You remove the file and folder that you copied.

Record your NVMe over RoCE configuration

You can generate and print a PDF of this page, and then use the following worksheet to record NVMe over RoCE storage configuration information. You need this information to perform provisioning tasks.

Direct connect topology

In a direct connect topology, one or more hosts are directly connected to the subsystem. In the SANtricity OS 11.50 release, we support a single connection from each host to a subsystem controller, as shown below. In this configuration, one HCA (host channel adapter) port from each host should be on the same subnet as the E-Series controller port it is connected to, but on a different subnet from the other HCA port.

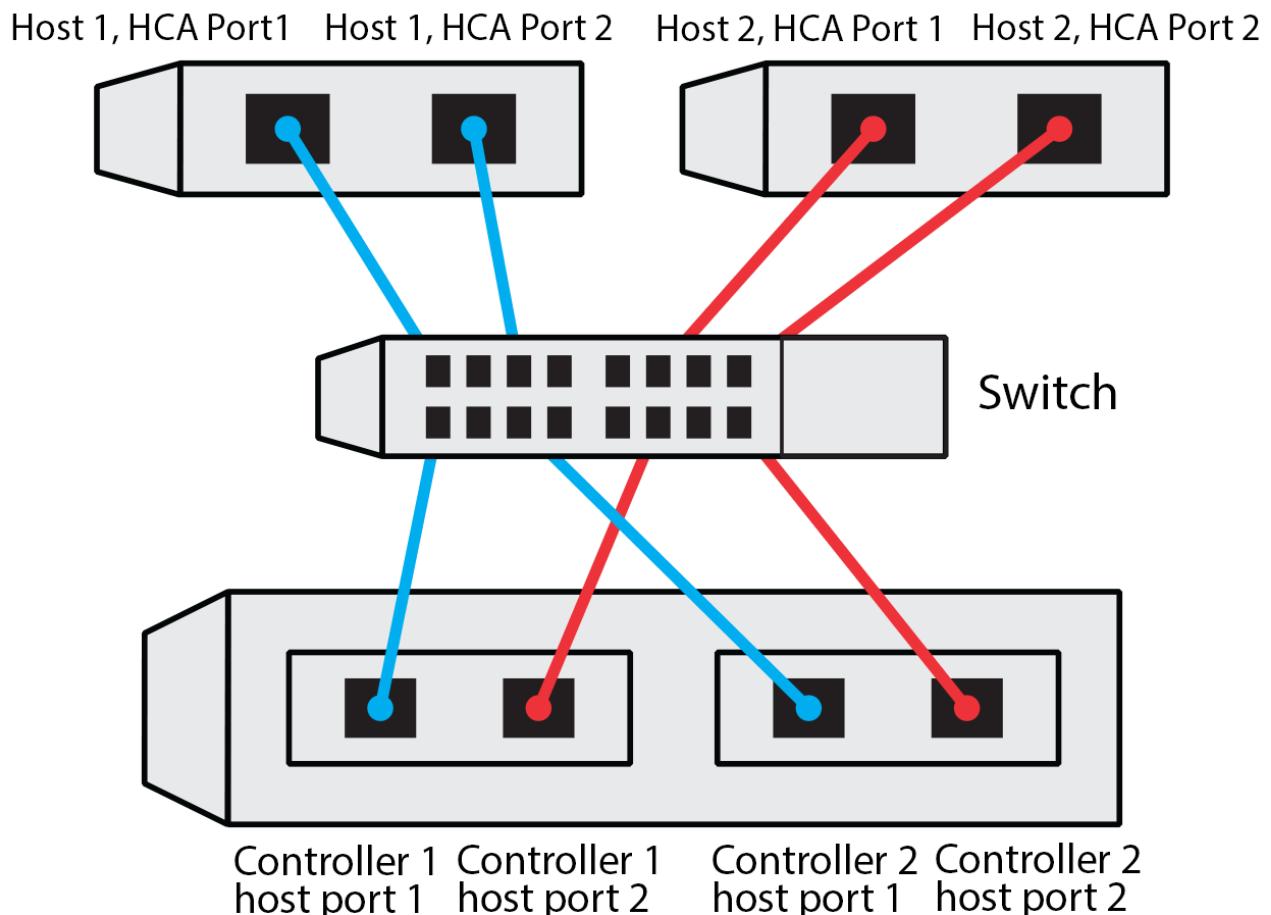


An example configuration that satisfies the requirements consists of four network subnets as follows:

- Subnet 1: Host 1 HCA Port 1 and Controller 1 Host port 1
- Subnet 2: Host 1 HCA Port 2 and Controller 2 Host port 1
- Subnet 3: Host 2 HCA Port 1 and Controller 1 Host port 2
- Subnet 4: Host 2 HCA Port 2 and Controller 2 Host port 2

Switch connect topology

In a fabric topology, one or more switches are used. Refer to [NetApp Interoperability Matrix Tool](#) for a list of supported switches.



Host identifiers

Locate and document the initiator NQN from each host.

| Host port connections | Software initiator NQN |
|-----------------------|------------------------|
| Host (initiator) 1 | |
| Host (initiator) 2 | |

| Host port connections | Software initiator NQN |
|-----------------------|------------------------|
| | |

Target NQN

Document the target NQN for the storage array.

| Array name | Target NQN |
|---------------------------|------------|
| Array controller (target) | |

Target NQNs

Document the NQNs to be used by the array ports.

| Array controller (target) port connections | NQN |
|--|-----|
| Controller A, port 1 | |
| Controller B, port 1 | |
| Controller A, port 2 | |
| Controller B, port 2 | |

Mapping host name



The mapping host name is created during the workflow.

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

NVMe over Fibre Channel setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, host, and recovery restrictions.

Verify the Linux configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).

2. Click on the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. As necessary, make the updates for your operating system and protocol that are prescribed in the tool.

Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

Review restrictions for NVMe over FC

Before using NVMe over Fibre Channel, review the controller, host, and recovery restrictions. For an up-to-date listing of all restrictions, see the [NetApp Interoperability Matrix Tool](#).

Controller restrictions

- NVMe over Fibre Channel can be configured for the EF300, EF600, EF570, and E5700 controllers. The controllers must have the quad 32GB host port.
- This protocol can be used only for EF300, EF600, EF570, or E5700 controllers with a minimum of 32 GB of physical memory. If the minimum memory requirements for the controllers are not met during start of day operations, a message is displayed that helps you diagnose the problem.
- No simplex (single-controller) configurations are supported.
- The only supported host interface card (HIC) is the quad 32GB Fibre Channel HIC.

Host, host protocol, and host operating system restrictions

For a complete list of requirements, see the [NetApp Interoperability Matrix Tool](#).

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine

- **Disk space:** 5 GB
- **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

| Windows | Linux |
|--|--|
| Double-click the SMIA*.exe installation package to start the installation. | <ol style="list-style-type: none"> Go to the directory where the SMIA*.bin installation package is located. If the temp mount point does not have execute permissions, set the <code>IATEMPDIR</code> variable. Example: <code>IATEMPDIR=/root ./SMIA-LINUXXX64-11.25.0A00.0002.bin</code> Run the <code>chmod +x SMIA*.bin</code> command to grant execute permission to the file. Run the <code>./SMIA*.bin</code> command to start the installer. |

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|---------------|-----------------|
| Google Chrome | 79 |

| Browser | Minimum version |
|-----------------------------|-----------------|
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Configure the FC switches

Configuring (zoning) the Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)

About this task

For details about zoning your switches, see the switch vendor's documentation.

Each initiator port must be in a separate zone with all of its corresponding target ports.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Set up NVMe over Fibre Channel on the host side

NVMe initiator configuration in a Fibre Channel environment includes installing and configuring the nvme-cli package and for enabling the NVMe/FC initiator on the host.

About this task

The following procedure is for RHEL 7, RHEL 8, SLES 12, and SLES 15 using Broadcom Emulex or QLogic NVMe/FC capable FC HBAs. For more information on which versions of these OS's or HBA's are supported, consult the [NetApp Interoperability Matrix Tool](#).

Steps

1. Install the nvme-cli package:

SLES 12 or SLES 15

```
# zypper install nvme-cli
```

RHEL 7 or RHEL 8

```
# yum install nvme-cli
```

- a. For RHEL 7 only, download and install an external Broadcom Autoconnect script for NVMe/FC connections through the [Broadcom website](#). Enter the keyword **Autoconnect Script File for Inbox NVMe over FC Drivers** and choose the latest version specific to your OS.
- b. For Qlogic, modify `/lib/systemd/system/nvmefc-boot-connections.service` after installing the Broadcom NVMe/FC autoconnect script to contain the following:

```
[Unit]
Description=Auto-connect to subsystems on FC-NVME devices found
during boot

[Service]
Type=oneshot
ExecStart=/bin/sh -c "echo add >
/sys/class/fc/fc_udev_device/nvme_discovery"

[Install]
WantedBy=default.target
```

2. Enable and start the `nvmefc-boot-connections` service.

```
systemctl enable nvmefc-boot-connections.service
```

```
systemctl start nvmefc-boot-connections.service
```

Host-side setup for Emulex HBAs:



The following steps are for Emulex HBAs only.

1. Set `lpfc_enable_fc4_type` to 3 to enable SLES12 SP4 as an NVMe/FC initiator.

```
# cat /etc/modprobe.d/lpfc.conf
options lpfc lpfc_enable_fc4_type=3
```

2. Re-build the `initrd` to get the Emulex change and the boot parameter change.

```
# dracut --force
```

3. Reboot the host to load the changes to the `lpfc` driver.

```
# reboot
```

The host is rebooted and the NVMe/FC initiator is enabled on the host.



After completing the host-side setup, connection of the NVMe over Fibre Channel ports occur automatically.

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage > Hosts**.

2. Click **Create > Host**.

The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

| Setting | Description |
|----------------------------|---|
| Name | Type a name for the new host. |
| Host operating system type | Select one of the following options from the drop-down list: <ul style="list-style-type: none">• Linux for SANtricity 11.60 and newer• Linux DM-MP (Kernel 3.10 or later) for pre-SANtricity 11.60 |
| Host interface type | Select the host interface type that you want to use. If the array you configure only has one available host interface type, this setting might not be available to select. |

| Setting | Description |
|------------|---|
| Host ports | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Select I/O Interface If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • Manual add If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the Host ports field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the Host ports field. If necessary, you also can remove an identifier by selecting the X next to it. |

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is <Hostname_Port Number>. For example, the default alias for the first port created for host IPT is IPT_1.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage > Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.

3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command.

The output `<format>` can be normal (the default if `-o` is not used), column, or json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover on the host

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing when using NVMe over Fibre Channel. RHEL 8 and SLES 15 use a built in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the /etc/multipath.conf file, as shown in the following example:

```
devices {
    device {
        vendor "NVME"
        product "NetApp E-Series*"
        path_grouping_policy group_by_prio
        fallback immediate
        no_path_retry 30
    }
}
```

2. Configure multipathd to start at system boot.

```
# systemctl enable multipathd
```

3. Start multipathd if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of multipathd to make sure it is active and running:

```
# systemctl status multipathd
```

Set up Native NVMe Multipathing for RHEL 8

About this task

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the steps below.

Steps

1. Setup modprobe rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-nvme_core.conf
```

2. Remake initramfs with new modprobe parameter.

```
# dracut -f
```

3. Reboot server to bring it up with the Native NVMe Multipathing enabled

```
# reboot
```

4. Verify Native NVMe Multipathing has been enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

- a. If the command output is N, then Native NVMe Multipathing is still disabled.
- b. If the command output is Y, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.



For SLES 15, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the dm device or the symlink in /dev/mapper; for example:

```
/dev/dm-1  
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example

The following example output from the nvme list command shows the host node name and its correlation with the namespace ID.

| NODE | SN | MODEL | NAMESPACE |
|--------------|--------------|-----------------|-----------|
| /dev/nvme1n1 | 021648023072 | NetApp E-Series | 10 |
| /dev/nvme1n2 | 021648023072 | NetApp E-Series | 11 |
| /dev/nvme1n3 | 021648023072 | NetApp E-Series | 12 |
| /dev/nvme1n4 | 021648023072 | NetApp E-Series | 13 |
| /dev/nvme2n1 | 021648023151 | NetApp E-Series | 10 |
| /dev/nvme2n2 | 021648023151 | NetApp E-Series | 11 |
| /dev/nvme2n3 | 021648023151 | NetApp E-Series | 12 |
| /dev/nvme2n4 | 021648023151 | NetApp E-Series | 13 |

| Column | Description |
|-----------|--|
| Node | <p>The node name includes two parts:</p> <ul style="list-style-type: none"> The notation <code>nvme1</code> represents controller A and <code>nvme2</code> represents controller B. The notation <code>n1</code>, <code>n2</code>, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B. |
| Namespace | <p>The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.</p> |

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|--- policy='service-time 0' prio=50 status=active
|   `-- #:#:#:# nvme1n1 259:5 active ready running
`--- policy='service-time 0' prio=10 status=enabled
    `-- #:#:#:# nvme2n1 259:9 active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|--- policy='service-time 0' prio=0 status=enabled
|   `-- #:#:#:# nvme1n1 259:5 failed faulty running
`--- policy='service-time 0' prio=10 status=active
    `-- #:#:#:# nvme2n1 259:9 active ready running
```

| Line item | Description |
|---|---|
| policy='service-time 0' prio=50 status=active | This line and the following line show that nvme1n1, which is the namespace with an NSID of 10, is optimized on the path with a <code>prio</code> value of 50 and a <code>status</code> value of <code>active</code> . This namespace is owned by controller A. |
| policy='service-time 0' prio=10 status=enabled | This line shows the failover path for namespace 10, with a <code>prio</code> value of 10 and a <code>status</code> value of <code>enabled</code> . I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B. |
| policy='service-time 0' prio=0 status=enabled | This example shows <code>multipath -ll</code> output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as <code>failed faulty running</code> with a <code>prio</code> value of 0 and a <code>status</code> value of <code>enabled</code> . |
| policy='service-time 0' prio=10 status=active | Note that the <code>active</code> path refers to nvme2, so the I/O is being directed on this path to controller B. |

Access NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8 and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

It is best practice to use the links in `/dev/disk/by-id/` rather than `/dev/nvme0n1`. For example:

```
# ls /dev/disk/by-id/ -l lrwxrwxrwx 1 root root 13 Oct 18 15:14
nvme-eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

Physical NVMe devices are I/O targets

Run I/O to the physical nvme device path. There should only be one of these devices present for each namespace using the following format:

```
/dev/nvme[subsys#]n[id#]
```

All paths are virtualized using the native multipathing solution underneath this device.

You can view your paths by running:

```
# nvme list-subsys
```

Example output:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a namespace device when using the `nvme list-subsys` command, it provides additional information about the paths to that namespace:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
+- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
+- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
+- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
+- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```



To view the path information, the following must be set in `/etc/multipath.conf`:

```
defaults {
    enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-Series,08520001  
size=4194304 features='n/a' hwhandler='ANA' wp=rw  
|-- policy='n/a' prio=50 status=optimized  
| `-- 0:0:1 nvme0c0n1 0:0 n/a optimized live  
`-- policy='n/a' prio=10 status=non-optimized  
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized live
```

Create filesystems

You can create a file system on the namespace or native NVMe device and mount the filesystem.

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the desired dm device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/mapper/dm` devices.

```
# multipath -ll
```

The result of this command shows two devices, `dm-19` and `dm-16`:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series  
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n19 259:19 active ready running  
| `-- #:#:#:# nvme1n19 259:115 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n19 259:51 active ready running  
  `-- #:#:#:# nvme3n19 259:83 active ready running  
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series  
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw  
|-- policy='service-time 0' prio=50 status=active  
| |- #:#:#:# nvme0n16 259:16 active ready running  
| `-- #:#:#:# nvme1n16 259:112 active ready running  
`-- policy='service-time 0' prio=10 status=enabled  
  |- #:#:#:# nvme2n16 259:48 active ready running  
  `-- #:#:#:# nvme3n16 259:80 active ready running
```

2. Create a file system on the partition for each `/dev/mapper/eui-` device.

The method for creating a file system varies depending on the file system chosen. This example shows

creating an ext4 file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8 and SLES 15)

For RHEL 8 and SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the multipath -ll command to get a list of /dev/nvme devices.

```
# multipath -ll
```

The result of this command shows device nvme0n6.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe, NetApp E-
Series, 08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
|--- policy='n/a' prio=50 status=optimized
|   `-- 0:1:1 nvme0c1n1 0:0 n/a optimized    live
|--- policy='n/a' prio=10 status=non-optimized
|   `-- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`--- policy='n/a' prio=10 status=non-optimized
   `-- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for each /dev/nvme0n# device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an ext4 file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, you verify that the host can write data to the namespace and read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the diff command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

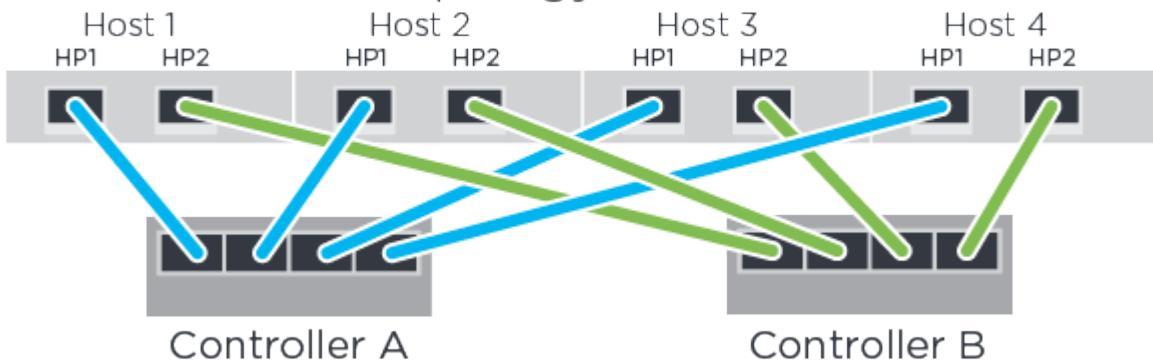
Record your NVMe over FC configuration

You can generate and print a PDF of this page, and then use the following worksheet to record NVMe over Fibre Channel storage configuration information. You need this information to perform provisioning tasks.

Direct connect topology

In a direct connect topology, one or more hosts are directly connected to the controller.

Direct Connect Topology

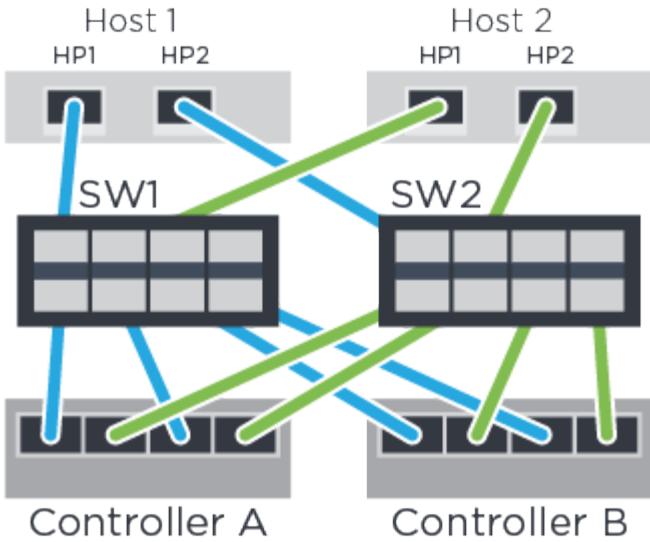


- Host 1 HBA Port 1 and Controller A Host port 1
- Host 1 HBA Port 2 and Controller B Host port 1
- Host 2 HBA Port 1 and Controller A Host port 2
- Host 2 HBA Port 2 and Controller B Host port 2
- Host 3 HBA Port 1 and Controller A Host port 3
- Host 3 HBA Port 2 and Controller B Host port 3
- Host 4 HBA Port 1 and Controller A Host port 4
- Host 4 HBA Port 2 and Controller B Host port 4

Switch connect topology

In a fabric topology, one or more switches are used. See the [NetApp Interoperability Matrix Tool](#) for a list of supported switches.

Fabric Topology



Host identifiers

Locate and document the initiator NQN from each host.

| Host port connections | Host NQN |
|-----------------------|----------|
| Host (initiator) 1 | |
| Host (initiator) 2 | |

Target NQN

Document the target NQN for the storage array.

| Array name | Target NQN |
|---------------------------|------------|
| Array controller (target) | |

Target NQNs

Document the NQNs to be used by the array ports.

| Array controller (target) port connections | NQN |
|--|-----|
| Controller A, port 1 | |
| Controller B, port 1 | |
| Controller A, port 2 | |

| | |
|---|-----|
| Array controller (target) port connections | NQN |
| Controller B, port 2 | |

Mapping host name



The mapping host name is created during the workflow.

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

VMware express configuration

VMware express configuration overview

The VMware express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone VMware host to an E-Series storage system. It is designed to get the storage system up and running as quickly as possible with minimal decision points.

Procedure overview

The express method includes the following steps, which are also outlined in the [VMware workflow](#).

1. Set up one of the following communication environments:
 - [NVMe over Fibre Channel](#)
 - [Fibre Channel](#)
 - [iSCSI](#)
 - [SAS](#)
2. Create logical volumes on the storage array.
3. Make the volumes available to the data host.

Find more information

- [Online help](#) — Describes how to use SANtricity System Manager to complete configuration and storage management tasks. It is available within the product.
- [NetApp Knowledgebase](#) (a database of articles) — Provides troubleshooting information, FAQs, and instructions for a wide range of NetApp products and technologies.
- [NetApp Interoperability Matrix Tool](#) — Enables you to search for configurations of NetApp products and components that meet the standards and requirements specified by NetApp.
- [VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.X](#) — Provides technical details on iSCSI integration with VMware.
- [VMware Configuration Maximums](#) — Describes how to configure virtual and physical storage to stay within the allowed maximums that ESX/ESXi supports.

- Requirements and limitations of VMware NVMe storage.
- VMware vSphere Documentation — Provides ESXi vCenter Server documentation.

Assumptions

The VMware express method is based on the following assumptions:

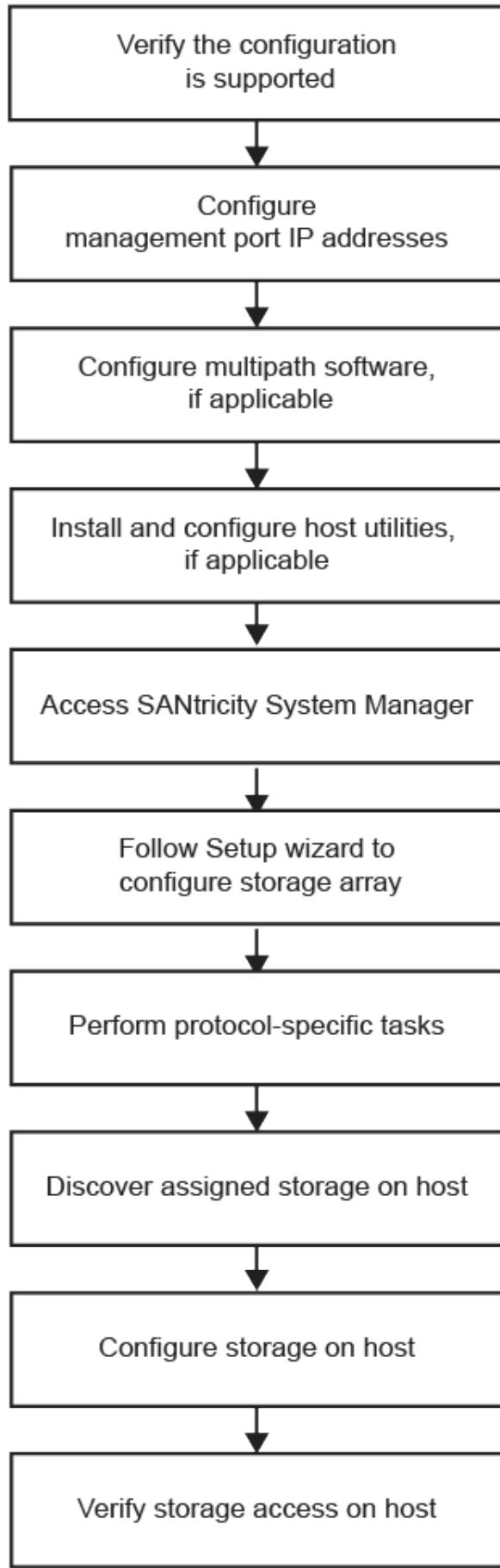
| Component | Assumptions |
|----------------------------|---|
| Hardware | <ul style="list-style-type: none"> • You have used the Installation and Setup Instructions included with the controller shelves to install the hardware. • You have connected cables between the optional drive shelves and the controllers. • You have applied power to the storage system. • You have installed all other hardware (for example, management station, switches) and made the necessary connections. |
| Host | <ul style="list-style-type: none"> • You have made a connection between the storage system and the data host. • You have installed the host operating system. • You are not using VMware as a virtualized guest. • You are not configuring the data (I/O attached) host to boot from SAN. |
| Storage management station | <ul style="list-style-type: none"> • You are using a 1 Gbps or faster management network. • You are using a separate station for management rather than the data (I/O attached) host. • You are using out-of-band management, in which a storage management station sends commands to the storage system through the Ethernet connections to the controller. • You have attached the management station to the same subnet as the storage management ports. |
| IP addressing | <ul style="list-style-type: none"> • You have installed and configured a DHCP server. • You have not yet made an Ethernet connection between the management station and the storage system. |
| Storage provisioning | <ul style="list-style-type: none"> • You will not use shared volumes. • You will create pools rather than volume groups. |

| Component | Assumptions |
|-----------------------------------|--|
| Protocol: FC | <ul style="list-style-type: none"> • You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: NVMe over Fibre Channel | <ul style="list-style-type: none"> • You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: iSCSI | <ul style="list-style-type: none"> • You are using Ethernet switches capable of transporting iSCSI traffic. • You have configured the Ethernet switches according to the vendor's recommendation for iSCSI. |
| Protocol: SAS | <ul style="list-style-type: none"> • You are using NetApp-supported SAS HBAs. • You are using SAS HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |

If these assumptions are not correct for your installation, or if you want more conceptual background information, see the following technical report: [VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.X](#)

Understand the VMware workflow

This workflow guides you through the "express method" for configuring your storage array and SANtricity System Manager to make storage available to a VMware host.



Verify the VMware configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click the **Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply. As necessary, make the updates for your operating system and protocol that are prescribed in the tool. Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

5. As necessary, make the updates for your operating system and protocol as listed in the table.

| Operating system updates | Protocol | Protocol-related updates |
|--|----------|--|
| <ul style="list-style-type: none"> You might need to install out-of-box drivers to ensure proper functionality and supportability. You can install HBA drivers using the ESXi shell or a remote SSH connection to the ESXi host. To access the host using either of those methods, you must enable the ESXi shell and SSH access. For more information about the ESXi shell, refer to the VMware Knowledge Base regarding using the ESXi shell in ESXi. For installation commands, refer to the instructions that accompany the HBA drivers. | FC | Host bus adapter (HBA) driver, firmware, and bootcode |
| <ul style="list-style-type: none"> Each HBA vendor has specific methods for updating boot code and firmware. Some of these methods could include the use of a vCenter plugin or the installation of CIM provider on the ESXi host. vCenter plugins can be used to obtain information about the vendor's specific HBA. Refer to the support section of the vendor's website to obtain the instructions and software necessary to update the HBA boot code or firmware. Refer to the <i>VMware Compatibility Guide</i> or the HBA vendor's website to obtain the correct boot code or firmware. | iSCSI | Network interface card (NIC) driver, firmware and bootcode |
| | SAS | Host bus adapter (HBA) driver, firmware, and bootcode |

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
 - Controller B, port 1: 169.254.128.102
 - Subnet mask: 255.255.0.0
2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device. For VMware, NVMe/FC uses High Performance Plugin (HPP).

Applicable only for FC, iSCSI, and SAS protocols, VMware provides plug-ins, known as Storage Array Type Plug-ins (SATP), to handle the failover implementations of specific vendors' storage arrays.

The SATP you should use is **VMW_SATP_ALUA**.

For more information, see [VMware SATPs](#).

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system

configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

If you are an iSCSI user, make sure you have closed the Setup wizard while configuring iSCSI.

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

If the Setup wizard does not automatically appear, contact technical support.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`<IPAddress>` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)**— Verify the number of controllers and drives in the storage array. Assign a name to the array.
 - **Verify hosts and operating systems**— Verify the host and operating system types that the storage array can access.
 - **Accept pools**— Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
 - **Configure alerts**— Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
 - **Enable AutoSupport**— Automatically monitor the health of your storage array and have dispatches sent to technical support.
4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.



For EF300 and EF600, you must set the block size to 512 bytes to ensure compatibility with VMware. Refer to the SANtricity System Manager online help for more information on setting a volume to 512 bytes.

Perform FC-specific tasks

For the Fibre Channel protocol, you configure the switches and determine the host port identifiers.

Step 1: Configure the FC switches—VMware

Configuring (zoning) the Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)



A vendor's HBA utility can be used to upgrade and obtain specific information about the HBA. Refer to the support section of the vendor's website for instructions on how to obtain the HBA utility.

About this task

Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Step 2: Determine the host port WWPNs—FC

To configure FC zoning, you must determine the worldwide port name (WWPN) of each initiator port.

Steps

1. Connect to the ESXi host using SSH or the ESXi shell.
2. Run the following command:

```
esxcfg-scsidevs -a
```

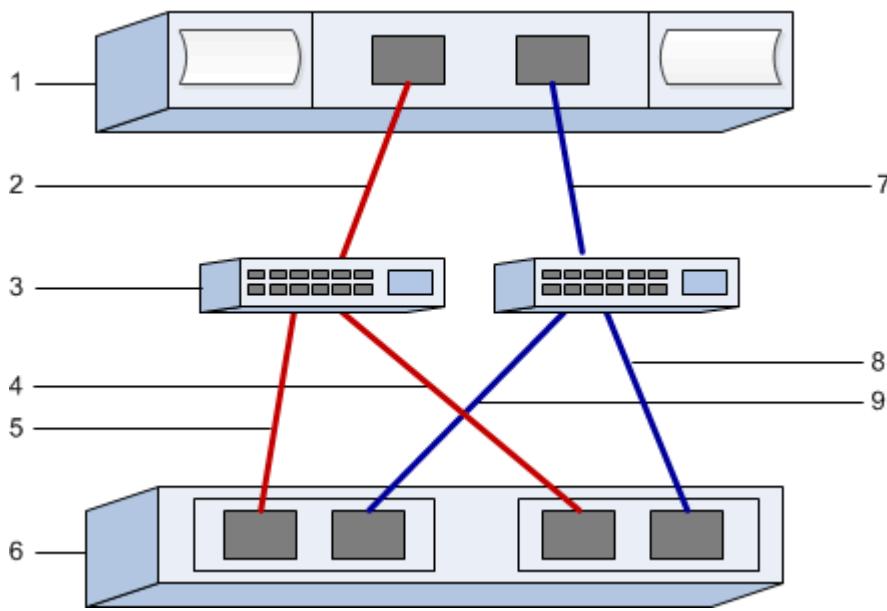
3. Record the initiator identifiers. The output will be similar to this example:

```
vhba3 lpfc link-up fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vhba4 lpfc link-up fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Step 3: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record FC storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Each zone contains one initiator port and all target ports.



Host identifiers

| Callout No. | Host (initiator) port connections | WWPN |
|-------------|-----------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host port 0 to FC switch zone 0 | |
| 7 | Host port 1 to FC switch zone 1 | |

Target identifiers

| Callout No. | Array controller (target) port connections | WWPN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 6 | Array controller (target) | <i>not applicable</i> |
| 5 | Controller A, port 1 to FC switch 1 | |
| 9 | Controller A, port 2 to FC switch 2 | |
| 4 | Controller B, port 1 to FC switch 1 | |
| 8 | Controller B, port 2 to FC switch 2 | |

Mapping host

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

Perform NVMe over FC-specific tasks

For the NVMe over Fibre Channel protocol, you configure the switches and determine the host port identifiers.

Step 1: Configure the NVMe/FC switches

Configuring (zoning) the NVMe over Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)



A vendor's HBA utility can be used to upgrade and obtain specific information about the HBA. Refer to the support section of the vendor's website for instructions on how to obtain the HBA utility.

About this task

Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Step 2: Determine the host ports WWPNs—NVMe/FC VMware

To configure FC zoning, you must determine the worldwide port name (WWPN) of each initiator port.

Steps

1. Connect to the ESXi host using SSH or the ESXi shell.
2. Run the following command:

```
esxcfg-scsidevs -a
```

3. Record the initiator identifiers. The output will be similar to this example:

```
vmhba3 lpfc link-up fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vmhba4 lpfc link-up fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Step 3: Enable HBA drivers

Support for NVMe must be enabled within Broadcom/Emulex and Marvell/Qlogic HBA drivers.

Steps

1. Execute one of the following commands from the ESXi shell:
 - **Broadcom/Emulex HBA Driver**

```
esxcli system module parameters set -m lpfc -p
"lpfc_enable_fc4_type=3"
```

- **Marvell/Qlogic HBA Driver**

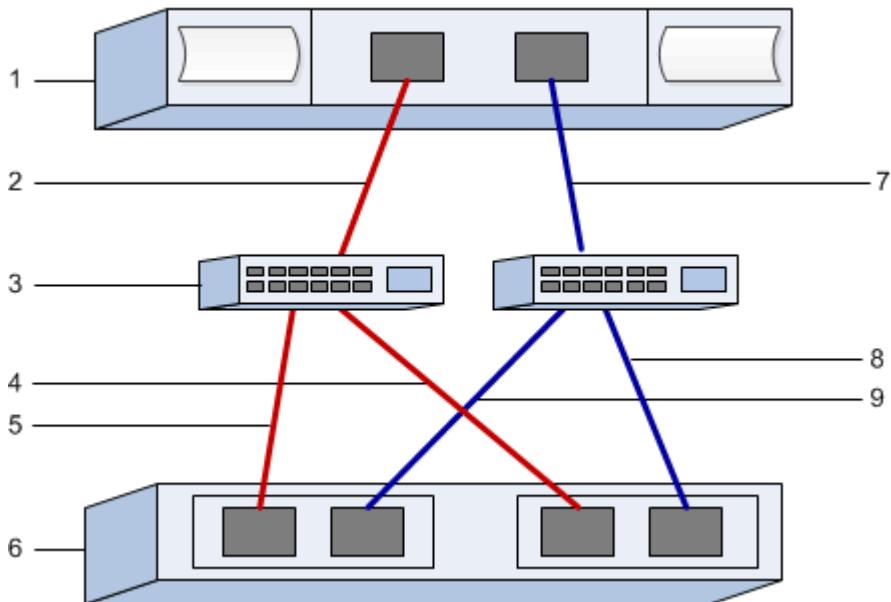
```
esxcfg-module -s "ql2xnvmesupport=1" qlnativefc
```

2. Reboot the host.

Step 4: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record NVMe over Fibre Channel storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Each zone contains one initiator port and all target ports.



Host identifiers

| Callout No. | Host (initiator) port connections | WWPN |
|-------------|-----------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host port 0 to FC switch zone 0 | |
| 7 | Host port 1 to FC switch zone 1 | |

Target identifiers

| Callout No. | Array controller (target) port connections | WWPN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 6 | Array controller (target) | <i>not applicable</i> |

| Callout No. | Array controller (target) port connections | WWPN |
|-------------|--|------|
| 5 | Controller A, port 1 to FC switch 1 | |
| 9 | Controller A, port 2 to FC switch 2 | |
| 4 | Controller B, port 1 to FC switch 1 | |
| 8 | Controller B, port 2 to FC switch 2 | |

Mapping host

| | |
|-------------------|--|
| Mapping host name | |
| Host OS type | |

Perform iSCSI-specific tasks

For the iSCSI protocol, you configure the switches and configure networking on the array side and the host side. Then you verify the IP network connections.

Step 1: Configure the switches—iSCSI, VMware

You configure the switches according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as code updates.

What you'll need

- Two separate networks for high availability. Make sure that you isolate your iSCSI traffic to separate network segments.
- Enabled send and receive hardware flow control **end to end**.
- Disabled priority flow control.
- If appropriate, enabled jumbo frames.



Port channels/LACP is not supported on the controller's switch ports. Host-side LACP is not recommended; multipathing provides the same benefits or better.

Steps

Consult your switch vendor's documentation.

Step 2: Configure networking—iSCSI VMware

You can set up your iSCSI network in many ways, depending on your data storage requirements. Consult your network administrator for tips on selecting the best configuration for your environment.

What you'll need

- Enabled send and receive hardware flow control **end to end**.

- Disabled priority flow control.
- If appropriate, enabled jumbo frames.

If you are using jumbo frames within the IP SAN for performance reasons, make sure to configure the array, switches, and hosts to use jumbo frames. Consult your operating system and switch documentation for information on how to enable jumbo frames on the hosts and on the switches. To enable jumbo frames on the array, complete the steps in Step 3.

About this task

While planning your iSCSI networking, remember that the [VMware Configuration Maximums](#) guide states that the maximum supported iSCSI storage paths is 8. You must consider this requirement to avoid configuring too many paths.

By default, the VMware iSCSI software initiator creates a single session per iSCSI target when you are not using iSCSI port binding.

 VMware iSCSI port binding is a feature that forces all bound VMkernel ports to log into all target ports that are accessible on the configured network segments. It is meant to be used with arrays that present a single network address for the iSCSI target. NetApp recommends that iSCSI port binding not be used. For additional information, see the [VMware Knowledge Base](#) for the article regarding considerations for using software iSCSI port binding in ESX/ESXi. If the ESXi host is attached to another vendor's storage, NetApp recommends that you use separate iSCSI vmkernel ports to avoid any conflict with port binding.

For best practice, you should NOT use port binding on E-Series storage arrays.

To ensure a good multipathing configuration, use multiple network segments for the iSCSI network. Place at least one host-side port and at least one port from each array controller on one network segment, and an identical group of host-side and array-side ports on another network segment. Where possible, use multiple Ethernet switches to provide additional redundancy.

Steps

Consult your switch vendor's documentation.



Many network switches have to be configured above 9,000 bytes for IP overhead. Consult your switch documentation for more information.

Step 3: Configure array-side networking—iSCSI, VMware

You use the SANtricity System Manager GUI to configure iSCSI networking on the array side.

What you'll need

- The IP address or domain name for one of the storage array controllers.
- Password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service is configured for the appropriate security access to the storage array. See the SANtricity System Manager online help for more information about Access Management.

About this task

This task describes how to access the iSCSI port configuration from the Hardware page. You can also access the configuration from **System > Settings > Configure iSCSI ports**.



For additional information on how to set up the array-side networking on your VMware configuration, see the following technical report: [VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.x and 7.x](#).

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. See the SANtricity System Manager online help for more information on the four local user roles.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Close the Setup wizard.

You will use the wizard later to complete additional setup tasks.

4. Select **Hardware**.

5. If the graphic shows the drives, click **Show back of shelf**.

The graphic changes to show the controllers instead of the drives.

6. Click the controller with the iSCSI ports you want to configure.

The controller's context menu appears.

7. Select **Configure iSCSI ports**.

The Configure iSCSI Ports dialog box opens.

8. In the drop-down list, select the port you want to configure, and then click **Next**.

9. Select the configuration port settings, and then click **Next**.

To see all port settings, click the **Show more port settings** link on the right of the dialog box.

| Port Setting | Description |
|---|--|
| Configured ethernet port speed | <p>Select the desired speed. The options that appear in the drop-down list depend on the maximum speed that your network can support (for example, 10 Gbps).</p> <p></p> <p>The optional 25Gb iSCSI host interface cards available on the controllers do not auto-negotiate speeds. You must set the speed for each port to either 10 Gb or 25 Gb. All ports must be set to the same speed.</p> |
| Enable IPv4 / Enable IPv6 | <p>Select one or both options to enable support for IPv4 and IPv6 networks.</p> |
| TCP listening port (Available by clicking Show more port settings .) | <p>If necessary, enter a new port number.</p> <p>The listening port is the TCP port number that the controller uses to listen for iSCSI logins from host iSCSI initiators. The default listening port is 3260. You must enter 3260 or a value between 49152 and 65535.</p> |
| MTU size (Available by clicking Show more port settings .) | <p>If necessary, enter a new size in bytes for the Maximum Transmission Unit (MTU).</p> <p>The default Maximum Transmission Unit (MTU) size is 1500 bytes per frame. You must enter a value between 1500 and 9000.</p> |
| Enable ICMP PING responses | <p>Select this option to enable the Internet Control Message Protocol (ICMP). The operating systems of networked computers use this protocol to send messages. These ICMP messages determine whether a host is reachable and how long it takes to get packets to and from that host.</p> |

If you selected **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you selected **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you selected both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

10. Configure the IPv4 and/or IPv6 settings, either automatically or manually. To see all port settings, click the **Show more settings** link on the right of the dialog box.

| Port setting | Description |
|---------------------------------------|--|
| Automatically obtain configuration | Select this option to obtain the configuration automatically. |
| Manually specify static configuration | Select this option, and then enter a static address in the fields. For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address. |

11. Click **Finish**.

12. Close System Manager.

Step 4: Configure host-side networking—iSCSI

Configuring iSCSI networking on the host side enables the VMware iSCSI initiator to establish a session with the array.

About this task

In this express method for configuring iSCSI networking on the host side, you allow the ESXi host to carry iSCSI traffic over four redundant paths to the storage.

After you complete this task, the host is configured with a single vSwitch containing both VMkernel ports and both VMNICs.

For additional information on configuring iSCSI networking for VMware, see the [VMware vSphere Documentation](#) for your version of vSphere.

Steps

1. Configure the switches that will be used to carry iSCSI storage traffic.
2. Enable send and receive hardware flow control **end to end**.
3. Disable priority flow control.
4. Complete the array side iSCSI configuration.
5. Use two NIC ports for iSCSI traffic.
6. Use either the vSphere client or vSphere web client to perform the host-side configuration.

The interfaces vary in functionality and the exact workflow will vary.

Step 5: Verify IP network connections—iSCSI, VMware

You verify Internet Protocol (IP) network connections by using ping tests to ensure the host and array are able to communicate.

Steps

1. On the host, run one of the following commands, depending on whether jumbo frames are enabled:
 - If jumbo frames are not enabled, run this command:

```
vmkping <iSCSI_target_IP_address\>
```

- If jumbo frames are enabled, run the ping command with a payload size of 8,972 bytes. The IP and ICMP combined headers are 28 bytes, which when added to the payload, equals 9,000 bytes. The -s switch sets the packet size bit. The -d switch sets the DF (Don't Fragment) bit on the IPv4 packet. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

```
vmkping -s 8972 -d <iSCSI_target_IP_address\>
```

In this example, the iSCSI target IP address is 192.0.2.8.

```
vmkping -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Issue a vmkping command from each host's initiator address (the IP address of the host Ethernet port used for iSCSI) to each controller iSCSI port. Perform this action from each host server in the configuration, changing the IP addresses as necessary.



If the command fails with the message `sendto() failed (Message too long)`, verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

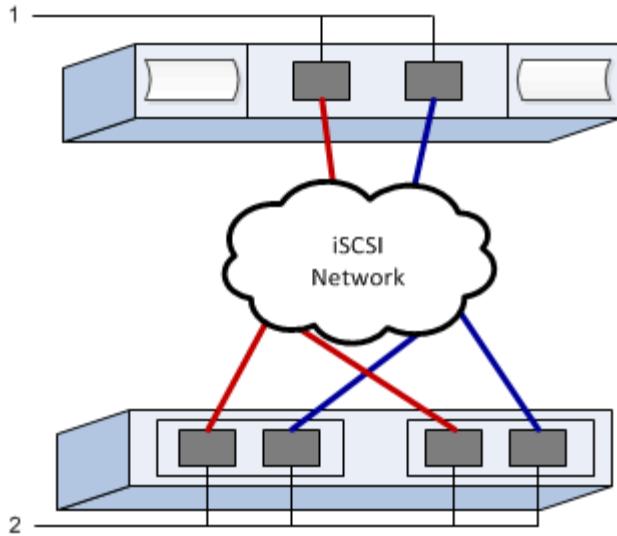
3. Return to the iSCSI Configuration procedure to finish target discovery.

Step 6: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record your protocol-specific storage configuration information. You need this information to perform provisioning tasks.

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports with one or more VLANs.



Target IQN

| Callout No. | Target port connection | IQN |
|-------------|------------------------|-----|
| 2 | Target port | |

Mapping host name

| Callout No. | Host information | Name and type |
|-------------|-------------------|---------------|
| 1 | Mapping host name | |
| | Host OS type | |

Perform SAS-specific tasks

For the SAS protocol, you determine host port addresses and make the recommended settings.

Step 1: Determine SAS host identifiers—VMware

Find the SAS addresses using the HBA utility, and then use the HBA BIOS to make the appropriate configuration settings.

About this task

Review the guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility.
- Host I/O ports might automatically register if the host context agent is installed.

Steps

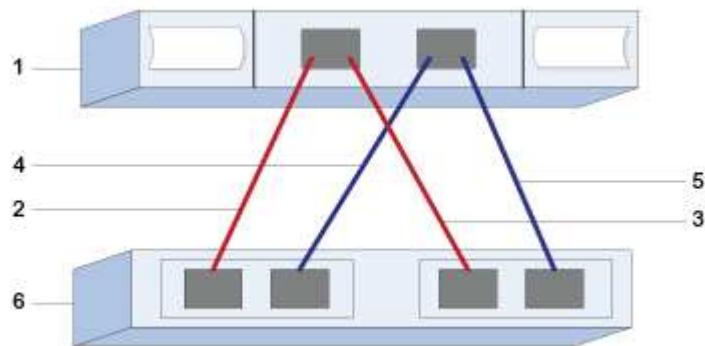
1. Download the HBA utility from your HBA vendor's web site.
2. Install the utility.

3. Use the HBA BIOS to select the appropriate settings for your configuration.

For appropriate settings, see the Notes column of the [NetApp Interoperability Matrix Tool](#) for recommendations.

Step 2: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record your protocol-specific storage configuration information. You need this information to perform provisioning tasks.



Host identifiers

| Callout No. | Host (initiator) port connections | SAS address |
|-------------|---|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host (initiator) port 1 connected to Controller A, port 1 | |
| 3 | Host (initiator) port 1 connected to Controller B, port 1 | |
| 4 | Host (initiator) port 2 connected to Controller A, port 1 | |
| 5 | Host (initiator) port 2 connected to Controller B, port 1 | |

Target identifiers

Recommended configurations consist of two target ports.

Mapping host name

| | |
|-------------------|--|
| Mapping host name | |
|-------------------|--|

| | |
|--------------|--|
| Host OS type | |
|--------------|--|

Discover storage on the host

After assigning volumes to the host, you perform a rescan so that the host detects and configures the volumes for multipathing.

By default, an ESXi host automatically performs a rescan every five minutes. A volume might appear between the time you create it and assign it to a host, before you perform a manual rescan. Regardless, you can perform a manual rescan to ensure all volumes are configured properly.

Steps

1. Create one or more volumes and assign them to the ESXi host.
2. If using a vCenter Server, add the host to the server's inventory.
3. Use the vSphere Client or the vSphere Web Client to connect directly to the vCenter Server or to the ESXi host.
4. For instructions on how to perform a rescan of the storage on an ESXi host, search for the [VMware Knowledge Base](#) article on this topic.

Configure storage on the host

You can use the storage assigned to an ESXi host as either a Virtual Machine File System (VMFS) datastore or a raw device mapping (RDM). RDMs are not supported on the NVMe over Fibre Channel protocol.

All 6.x and 7.x versions of ESXi support VMFS versions 5 and 6.

Steps

1. Make sure the volumes mapped to the ESXi host have been discovered properly.
2. For instructions on creating VMFS datastores or using volumes as RDMs with either the vSphere Client or the vSphere Web Client, see the [VMware Documentation web site](#).

Verify storage access on the host

Before using a volume, verify that the host can write data to the volume and read it back.

To do this, verify that the volume has been used as a Virtual Machine File System (VMFS) datastore or has been mapped directly to a VM for use as a raw device mapping (RDM).

Windows express configuration

Windows express configuration overview

The Windows express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone Windows host to an E-Series system. It is designed to get the storage system up and running as quickly as possible with minimal decision points.

Procedure overview

The express method includes the following steps, which are also outlined in the [Windows workflow](#).

1. Set up one of the following communication environments:

- [Fibre Channel \(FC\)](#)
- [iSCSI](#)
- [SAS](#)

2. Create logical volumes on the storage array.

3. Make the volumes available to the data host.

Find more information

- Online help — Describes how to use SANtricity System Manager to complete configuration and storage management tasks. It is available within the product.
- [NetApp Knowledgebase](#) (a database of articles) — Provides troubleshooting information, FAQs, and instructions for a wide range of NetApp products and technologies.
- [NetApp Interoperability Matrix Tool](#) — Enables you to search for configurations of NetApp products and components that meet the standards and requirements specified by NetApp.
- [NetApp Documentation: Host Utilities](#) — Provides documentation for the current Windows Unified Host Utilities version.

Assumptions

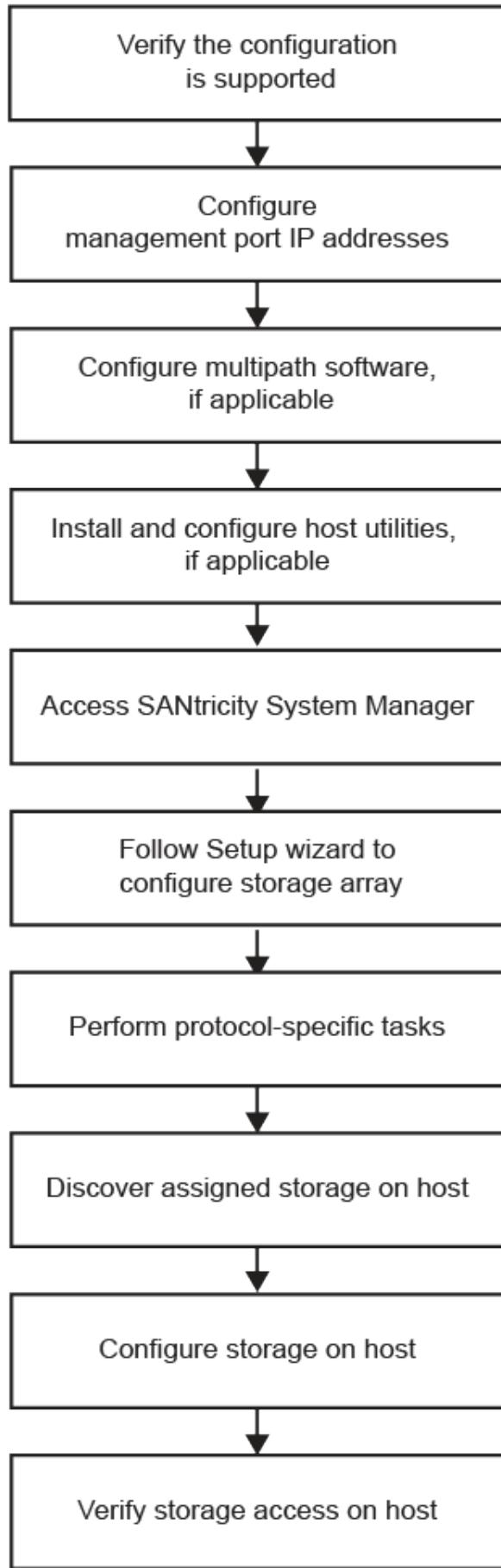
The Windows express method is based on the following assumptions:

| Component | Assumptions |
|-----------|---|
| Hardware | <ul style="list-style-type: none">• You have used the Installation and Setup Instructions included with the controller shelves to install the hardware.• You have connected cables between the optional drive shelves and the controllers.• You have applied power to the storage system.• You have installed all other hardware (for example, management station, switches) and made the necessary connections. |
| Host | <ul style="list-style-type: none">• You have made a connection between the storage system and the data host.• You have installed the host operating system.• You are not using Windows as a virtualized guest.• You are not configuring the data (I/O attached) host to boot from SAN. |

| Component | Assumptions |
|----------------------------|---|
| Storage management station | <ul style="list-style-type: none"> • You are using a 1 Gbps or faster management network. • You are using a separate station for management rather than the data (I/O attached) host. • You are using out-of-band management, in which a storage management station sends commands to the storage system through the Ethernet connections to the controller. • You have attached the management station to the same subnet as the storage management ports. |
| IP addressing | <ul style="list-style-type: none"> • You have installed and configured a DHCP server. • You have not yet made an Ethernet connection between the management station and the storage system. |
| Storage provisioning | <ul style="list-style-type: none"> • You will not use shared volumes. • You will create pools rather than volume groups. |
| Protocol: FC | <ul style="list-style-type: none"> • You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |
| Protocol: iSCSI | <ul style="list-style-type: none"> • You are using Ethernet switches capable of transporting iSCSI traffic. • You have configured the Ethernet switches according to the vendor's recommendation for iSCSI. |
| Protocol: SAS | <ul style="list-style-type: none"> • You are using NetApp-supported SAS HBAs. • You are using SAS HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool. |

Understand the Windows workflow

This workflow guides you through the express method for configuring your storage array and SANtricity System Manager to make storage available to a Windows host.



Verify the Windows configuration is supported

To ensure reliable operation, create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the [NetApp Interoperability Matrix Tool](#).
2. Click on the **Storage Solution Search** tile.
3. In the **Protocols > SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply. As necessary, make the updates for your operating system and protocol that are prescribed in the tool. Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

5. As necessary, make the updates for your operating system and protocol as listed in the table.

| Operating system updates | Protocol | Protocol-related updates |
|--|----------|---|
| You might need to install out-of-box drivers to ensure proper functionality and supportability. | FC | Host bus adapter (HBA) driver, firmware, and bootcode |
| Each HBA vendor has specific methods for updating boot code and firmware. Refer to the support section of the vendor's website to obtain the instructions and software necessary to update the HBA boot code and firmware. | iSCSI | Network interface card (NIC) driver, firmware and bootcode. |
| | SAS | Host bus adapter (HBA) driver, firmware, and bootcode |

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to

management port 1 on each controller (A and B).

The DHCP server assigns an IP address to port 1 of each controller.



Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.



If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

- Controller A, port 1: 169.254.128.101
- Controller B, port 1: 169.254.128.102
- Subnet mask: 255.255.0.0

2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Configure the multipath software

To provide a redundant path to the storage array, you can install the SANtricity Windows DSM package and use the multipath package for Windows.

What you'll need

The correct administrator or superuser privileges.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. Before you can use multipathing, you need to install the SANtricity Windows DSM package. This package contains the multipath software for Windows.

Windows installations use the native MPIO Device Specific Module (DSM) driver for failover. When you install and enable the SANtricity Windows DSM package, you do not need to take further action to use multipath.

Steps

1. Download the **SANtricity Windows DSM** package from the [SANtricity OS software page](#). Select your software version, accept the license agreement, and select **SANtricity Windows DSM** under Additional Downloads.
2. Run the **SANtricity Windows DSM** installer. Double-click the install package to execute.
3. Use the installation wizard to install the package on the management station.

Install and configure Windows Unified Host Utilities

The Windows Unified Host Utilities tools help you to connect host computers to NetApp storage systems and set required parameters on host computers. You can also set appropriate disk timeouts for best read/write performance with NetApp storage.



For more information, see the *Windows Host Utilities Installation Guide*, found under [NetApp Documentation: Host Utilities](#).

Steps

1. Use the [NetApp Interoperability Matrix Tool](#) to determine the appropriate version of Unified Host Utilities to install.

The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from [NetApp Support](#).



This utilities package cannot be installed using the SANtricity Storage Manager installer.



Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMUtils package. The SMUtils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli and Host Context Agent (HCA)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.



If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- The correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client that has the following minimum requirements:
 - **RAM:** 2 GB for Java Runtime Engine
 - **Disk space:** 5 GB
 - **OS/Architecture:** For guidance on determining the supported operating system versions and architectures, go to [NetApp Support](#). From the **Downloads** tab, go to **Downloads > E-Series SANtricity Storage Manager**.

Steps

1. Download the SANtricity software release at [NetApp Support](#). From the **Downloads** tab, **Downloads > E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer. Double-click the SMIA*.exe install package to execute.
3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

| Browser | Minimum version |
|-----------------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer (MSE) | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

About this task

If you are an iSCSI user, make sure you have closed the Setup wizard while configuring iSCSI.

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools or volume groups are detected.
- No workloads are detected.
- No notifications are configured.

If the Setup wizard does not automatically appear, contact technical support.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`<IPAddress>` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:

- **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
- **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
- **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
- **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
- **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.

4. If you have not already created a volume, create one by going to **Storage > Volumes > Create > Volume**.

For more information, see the online help for SANtricity System Manager.

Perform FC-specific tasks

For the Fibre Channel protocol, you configure the switches and determine the host port identifiers.

Step 1: Configure the FC switches—Windows

Configuring (zoning) the Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)

About this task

You must zone by WWPN, not by physical port. Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that

- connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
 4. Save the zones, and then activate the new zoning configuration.

Step 2: Determine host WWPNs and make recommended settings—FC, Windows

You install an FC HBA utility so you can view the worldwide port name (WWPN) of each host port. Additionally, you can use the HBA utility to change any settings recommended in the Notes column of the [NetApp Interoperability Matrix Tool](#) for the supported configuration.

About this task

Review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. You will need the correct version of HBA for your host operating system and CPU. Examples of FC HBA utilities include:
 - Emulex OneCommand Manager for Emulex HBAs
 - QLogic QConverge Console for QLogic HBAs
- Host I/O ports might automatically register if the host context agent is installed.

Steps

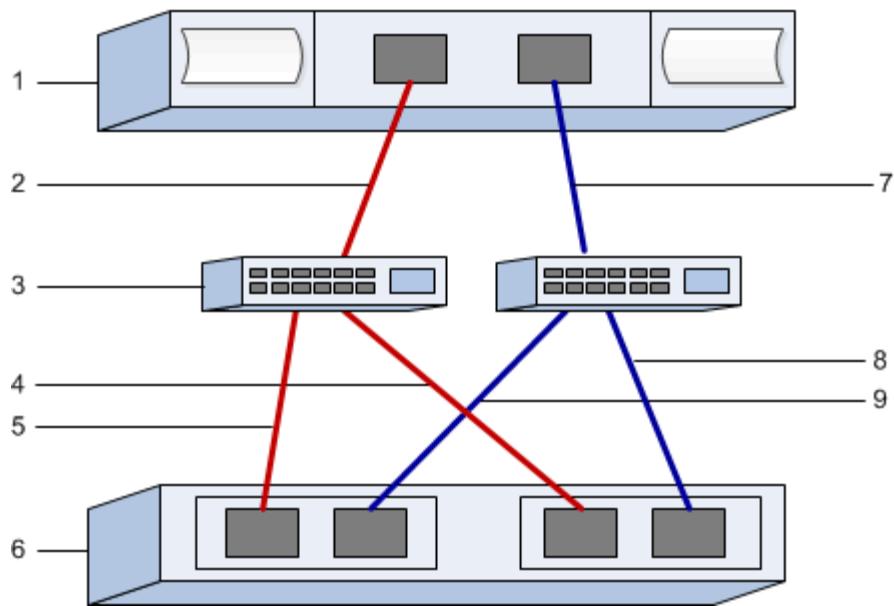
1. Download the appropriate utility from your HBA vendor's web site.
2. Install the utility.
3. Select the appropriate settings in the HBA utility.

Appropriate settings for your configuration are listed in the Notes column of the [NetApp Interoperability Matrix Tool](#).

Step 3: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record FC storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Any single port has two paths to the storage (one to each controller).



Host identifiers

| Callout No. | Host (initiator) port connections | WWPN |
|-------------|-----------------------------------|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host port 0 to FC switch zone 0 | |
| 7 | Host port 1 to FC switch zone 1 | |

Target identifiers

| Callout No. | Array controller (target) port connections | WWPN |
|-------------|--|-----------------------|
| 3 | Switch | <i>not applicable</i> |
| 6 | Array controller (target) | <i>not applicable</i> |
| 5 | Controller A, port 1 to FC switch 1 | |
| 9 | Controller A, port 2 to FC switch 2 | |
| 4 | Controller B, port 1 to FC switch 1 | |
| 8 | Controller B, port 2 to FC switch 2 | |

Mapping host name

| | |
|-------------------|--|
| Mapping host name | |
|-------------------|--|

| | |
|--------------|--|
| Host OS type | |
|--------------|--|

Perform iSCSI-specific tasks

For the iSCSI protocol, you configure the switches, configure networking on the array side and host side, and then verify the IP network connections.

Step 1: Configure the switches—iSCSI, Windows

You configure the switches according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as code updates.

What you'll need

- Two separate networks for high availability. Make sure that you isolate your iSCSI traffic to separate network segments by using VLANs or two separate networks.
- Enabled send and receive hardware flow control **end to end**.
- Disabled priority flow control.
- If appropriate, enabled jumbo frames.



Port channels/LACP is not supported on the controller's switch ports. Host-side LACP is not recommended; multipathing provides the same benefits or better.

Steps

Consult your switch vendor's documentation.

Step 2: Configure networking—iSCSI Windows

You can set up your iSCSI network in many ways, depending on your data storage requirements. Consult your network administrator for tips on selecting the best configuration for your environment.

An effective strategy for configuring the iSCSI network with basic redundancy is to connect each host port and one port from each controller to separate switches and partition each set of host and controller ports on separate network segments using VLANs.

What you'll need

- Enabled send and receive hardware flow control **end to end**.
- Disabled priority flow control.
- If appropriate, enabled jumbo frames.

If you are using jumbo frames within the IP SAN for performance reasons, make sure to configure the array, switches, and hosts to use jumbo frames. Consult your operating system and switch documentation for information on how to enable jumbo frames on the hosts and on the switches. To enable jumbo frames on the array, complete the procedure in Step 3.

Steps

Consult your switch vendor's documentation.



Many network switches have to be configured above 9,000 bytes for IP overhead. Consult your switch documentation for more information.

Step 3: Configure array-side networking—iSCSI, Windows

You use the SANtricity System Manager GUI to configure iSCSI networking on the array side.

What you'll need

- The IP address or domain name for one of the storage array controllers.
- A password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service configured for the appropriate security access to the storage array. See the SANtricity System Manager online help for more information about Access Management.

About this task

This task describes how to access the iSCSI port configuration from the Hardware page. You can also access the configuration from **System > Settings > Configure iSCSI ports**.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

`IPAddress` is the address for one of the storage array controllers.

The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. See the SANtricity System Manager online help for more information on the four local user roles.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then select the **Set Password** button.

When you open System Manager and no pools, volumes groups, workloads, or notifications have been configured, the Setup wizard launches.

3. Close the Setup wizard.

You will use the wizard later to complete additional setup tasks.

4. Select **Hardware**.

5. If the graphic shows the drives, click **Show back of shelf**.

The graphic changes to show the controllers instead of the drives.

6. Click the controller with the iSCSI ports you want to configure.

The controller's context menu appears.

7. Select **Configure iSCSI ports**.

The Configure iSCSI Ports dialog box opens.

8. In the drop-down list, select the port you want to configure, and then click **Next**.

9. Select the configuration port settings, and then click **Next**.

To see all port settings, click the **Show more port settings** link on the right of the dialog box.

| Port Setting | Description |
|---|--|
| Configured ethernet port speed | <p>Select the desired speed. The options that appear in the drop-down list depend on the maximum speed that your network can support (for example, 10 Gbps).</p> <p> The optional iSCSI host interface cards in the E5700 and EF570 controllers do not auto-negotiate speeds. You must set the speed for each port to either 10 Gb or 25 Gb. All ports must be set to the same speed.</p> |
| Enable IPv4 / Enable IPv6 | <p>Select one or both options to enable support for IPv4 and IPv6 networks.</p> |
| TCP listening port (Available by clicking Show more port settings .) | <p>If necessary, enter a new port number. The listening port is the TCP port number that the controller uses to listen for iSCSI logins from host iSCSI initiators. The default listening port is 3260. You must enter 3260 or a value between 49152 and 65535.</p> |
| MTU size (Available by clicking Show more port settings .) | <p>If necessary, enter a new size in bytes for the Maximum Transmission Unit (MTU). The default Maximum Transmission Unit (MTU) size is 1500 bytes per frame. You must enter a value between 1500 and 9000.</p> |
| Enable ICMP PING responses | <p>Select this option to enable the Internet Control Message Protocol (ICMP). The operating systems of networked computers use this protocol to send messages. These ICMP messages determine whether a host is reachable and how long it takes to get packets to and from that host.</p> |

If you selected **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you selected **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you selected both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

10. Configure the IPv4 and/or IPv6 settings, either automatically or manually. To see all port settings, click the **Show more settings** link on the right of the dialog box.

| Port setting | Description |
|--|---|
| Automatically obtain configuration | Select this option to obtain the configuration automatically. |
| Manually specify static configuration | Select this option, and then enter a static address in the fields. For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address. |
| Enable VLAN support (Available by clicking Show more settings .) |  This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. Select this option to enable a VLAN and enter its ID. A VLAN is a logical network that behaves like it is physically separate from other physical and virtual local area networks (LANs) supported by the same switches, the same routers, or both. |
| Enable ethernet priority (Available by clicking Show more settings .) |  This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. Select this option to enable the parameter that determines the priority of accessing the network. Use the slider to select a priority between 1 and 7. In a shared local area network (LAN) environment, such as Ethernet, many stations might contend for access to the network. Access is on a first-come, first-served basis. Two stations might try to access the network at the same time, which causes both stations to back off and wait before trying again. This process is minimized for switched Ethernet, where only one station is connected to a switch port. |

11. Click **Finish**.

12. Close System Manager.

Step 4: Configure host-side networking—iSCSI

You must configure iSCSI networking on the host side so that the Microsoft iSCSI Initiator can establish sessions with the array.

What you'll need

- Fully configured switches that will be used to carry iSCSI storage traffic.
- Enabled send and receive hardware flow control **end to end**
- Disabled priority flow control.

- Array side iSCSI configuration completed.
- The IP address of each port on the controller.

About this task

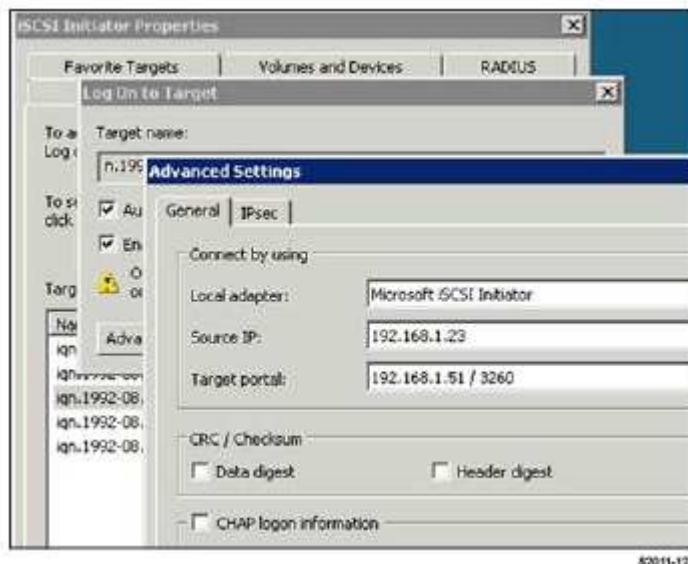
These instructions assume that two NIC ports will be used for iSCSI traffic.

Steps

1. Disable unused network adapter protocols.

These protocols include, but are not limited to, QoS, File and Print Sharing, and NetBIOS.

2. Execute > `iscsicpl.exe` from a terminal window on the host to open the **iSCSI Initiator Properties** dialog box.
3. On the **Discovery** tab, select **Discover Portal**, and then enter the IP address of one of the iSCSI target ports.
4. On the **Targets** tab, select the first target portal you discovered and then select **Connect**.
5. Select **Enable multi-path**, select **Add this connection to the list of Favorite Targets**, and then select **Advanced**.
6. For **Local adapter**, select **Microsoft iSCSI Initiator**.
7. For **Initiator IP**, select the IP address of a port on the same subnet or VLAN as one of the iSCSI targets.
8. For **Target IP**, select the IP address of a port on the same subnet as the **Initiator IP** selected in the step above.
9. Retain the default values for the remaining check boxes, and then select **OK**.
10. Select **OK** again as you return to the **Connect to Target** dialog box.
11. Repeat this procedure for each initiator port and session (logical path) to the storage array that you want to establish.



Step 5: Verify IP network connections—iSCSI, Windows

You verify Internet Protocol (IP) network connections by using ping tests to ensure the host and array are able to communicate.

1. Select **Start > All Programs > Accessories > Command Prompt**, and then use the Windows CLI to run one of the following commands, depending on whether jumbo frames are enabled:

- If jumbo frames are not enabled, run this command:

```
ping -s <hostIP\> <targetIP\>
```

- If jumbo frames are enabled, run the ping command with a payload size of 8,972 bytes. The IP and ICMP combined headers are 28 bytes, which when added to the payload, equals 9,000 bytes. The -f switch sets the don't fragment (DF) bit. The -l switch allows you to set the size. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

```
ping -l 8972 -f <iSCSI_target_IP_address\>
```

In this example, the iSCSI target IP address is 192.0.2.8.

```
C:\>ping -l 8972 -f 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Issue a ping command from each host's initiator address (the IP address of the host Ethernet port used for iSCSI) to each controller iSCSI port. Perform this action from each host server in the configuration, changing the IP addresses as necessary.



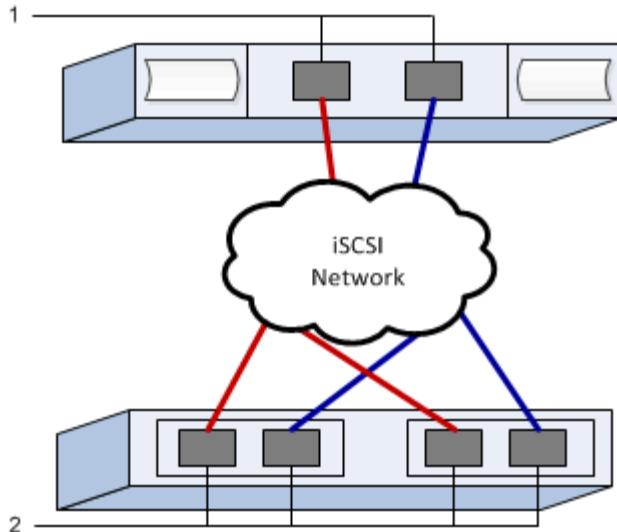
If the command fails (for example, returns Packet needs to be fragmented but DF set), verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

Step 6: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record iSCSI storage configuration information. You need this information to perform provisioning tasks.

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports with one or more VLANs.



Target IQN

| Callout No. | Target port connection | IQN |
|-------------|------------------------|-----|
| 2 | Target port | |

Mapping host name

| Callout No. | Host information | Name and type |
|-------------|-------------------|---------------|
| 1 | Mapping host name | |
| | Host OS type | |

Perform SAS-specific tasks

For the SAS protocol, you determine host port addresses and make the appropriate settings.

Step 1: Determine SAS host identifiers—Windows

Find the SAS addresses using the HBA utility, then use the HBA BIOS to make the appropriate configuration settings.

About this task

Review the guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. Depending on your host operating system and CPU, use either the LSI-sas2flash(6G) or sas3flash(12G) utility.
- Host I/O ports might automatically register if the host context agent is installed.

Steps

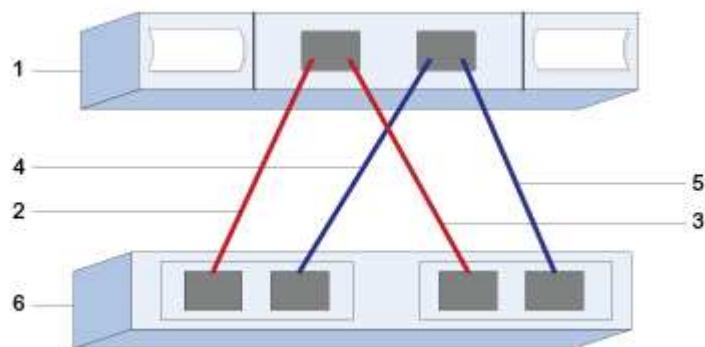
1. Download the LSI-sas2flash(6G) or sas3flash(12G) utility from your HBA vendor's web site.

2. Install the utility.
3. Use the HBA BIOS to select the appropriate settings for your configuration.

For setting recommendations, see the Notes column of the [NetApp Interoperability Matrix Tool](#).

Step 2: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record your protocol-specific storage configuration information. You need this information to perform provisioning tasks.



Host identifiers

| Callout No. | Host (initiator) port connections | SAS address |
|-------------|---|-----------------------|
| 1 | Host | <i>not applicable</i> |
| 2 | Host (initiator) port 1 connected to Controller A, port 1 | |
| 3 | Host (initiator) port 1 connected to Controller B, port 1 | |
| 4 | Host (initiator) port 2 connected to Controller A, port 1 | |
| 5 | Host (initiator) port 2 connected to Controller B, port 1 | |

Target identifiers

Recommended configurations consist of two target ports.

Mapping host name

| | |
|-------------------|--|
| Mapping host name | |
|-------------------|--|

| | |
|--------------|--|
| Host OS type | |
|--------------|--|

Discover storage on the host

When you add new LUNs, you must manually rescan the associated disks to discover them. The host does not automatically discover new LUNs.

LUNs on your storage system appear as disks to the Windows host.

Steps

1. Log on as an administrator.
2. To discover the storage, run the following command from a Windows command prompt.

```
# echo rescan | diskpart
```

3. To verify the addition of new storage, run the following command.

```
# echo list disk | diskpart
```

Configure storage on the host

Because a new LUN is offline and has no partition or file system when a Windows host first discovers it, you must bring the volume online and initialize it in Windows. Optionally, you can format the LUN with a file system.

You can initialize the disk as a basic disk with a GPT or MBR partition table. Typically, you format the LUN with a file system such as New Technology File System (NTFS).

What you'll need

A LUN discovered by the host.

Steps

1. From a Windows command prompt, enter the `diskpart` context.

```
> diskpart
```

2. View the list of available disks.

```
> list disk
```

3. Select the disk to bring online.

```
> select disk 1
```

4. Bring the disk online.

```
> online disk
```

5. Create a partition.

```
> create partition primary
```



In Windows Server 2008 and later, you are prompted immediately after creating the partition to format the disk and give it a name. Select **Cancel** on the prompt to continue using these instructions for formatting and naming the partition.

6. Assign a drive letter.

```
> assign letter=f
```

7. Format the disk.

```
> format FS=NTFS LABEL="New Volume" QUICK
```

8. Exit the diskpart context.

```
> exit
```

Verify storage access on the host

Before using the volume, verify that the host can write data to the LUN and read it back.

What you'll need

You must have initialized the LUN and formatted it with a file system.

Steps

1. Create and write to a file on the new LUN.

```
> echo test file > f:\\test.txt
```

2. Read the file and verify data was written.

```
> type f:\\test.txt
```

3. To verify that multipath is working, change the volume ownership.
 - a. From the SANtricity System Manager GUI, go to **Storage > Volumes**, and then select **More > Change ownership**.
 - b. On the Change Volume Ownership dialog box, use the **Preferred Owner** pull-down to select the other controller for one of the volumes in the list, and then confirm the operation.
 - c. Verify that you can still access the files on the LUN.

```
> dir f:\\
```

4. Find the target ID.



The dsmUtil utility is case sensitive.

```
> C:\\Program Files \\(x86\\) \\DSMDrivers\\mppdsm\\dsmUtil.exe -a
```

5. View the paths to the LUN and verify that you have the expected number of paths. In the `<target ID>` portion of the command, use the target ID that you found in the previous step.

```
> C:\\Program Files \\(x86\\) \\DSMDrivers\\mppdsm\\dsmUtil.exe -g <target ID\\>
```

Upgrade systems

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 |
|--|---|
| <p>SAS-2 shelves include the following models:</p> <ul style="list-style-type: none"> • 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 | <p>SAS-3 shelves include the following models:</p> <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> <li data-bbox="855 160 1496 502">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 <code>export storageArray securityKey</code> 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 <i>Command Line Reference</i>. <li data-bbox="855 523 1421 587">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). | <p data-bbox="855 642 1307 677">Perform the following steps, in order:</p> <ul style="list-style-type: none"> <li data-bbox="855 699 1496 882">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. <li data-bbox="855 903 1496 1311">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 <code>save storageArray keyManagementCertificate</code> CLI command to save the certificates. Be sure to run the command twice, once with the <code>certificateType</code> parameter set to <code>client</code>, and the other with the parameter set to <code>server</code>. For information about using this command, see the <i>Command Line Reference</i>. <li data-bbox="855 1332 1421 1438">c. Transition to internal key management by running the <code>disable storageArray externalKeyManagement</code> CLI command. <li data-bbox="855 1459 1496 1803">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 <code>export storageArray securityKey</code> 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 <i>Command Line Reference</i>. <li data-bbox="855 1824 1421 1888">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. | <p>Perform the following steps, in order:</p> <ol style="list-style-type: none"> <li data-bbox="861 228 1486 397">a. Record the External KMS server address and port number. From System Manager, go to Settings > System > Security Key Management Management > View/Edit Key Management Server Settings. <li data-bbox="861 418 1486 840">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 <code>storageArray keyManagementCertificate</code> CLI command to save the certificates. Be sure to run the command twice, once with the <code>certificateType</code> parameter set to <code>client</code>, and the other with the parameter set to <code>server</code>. For information about using this command, see the <i>Command Line Reference</i>. |
| 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.

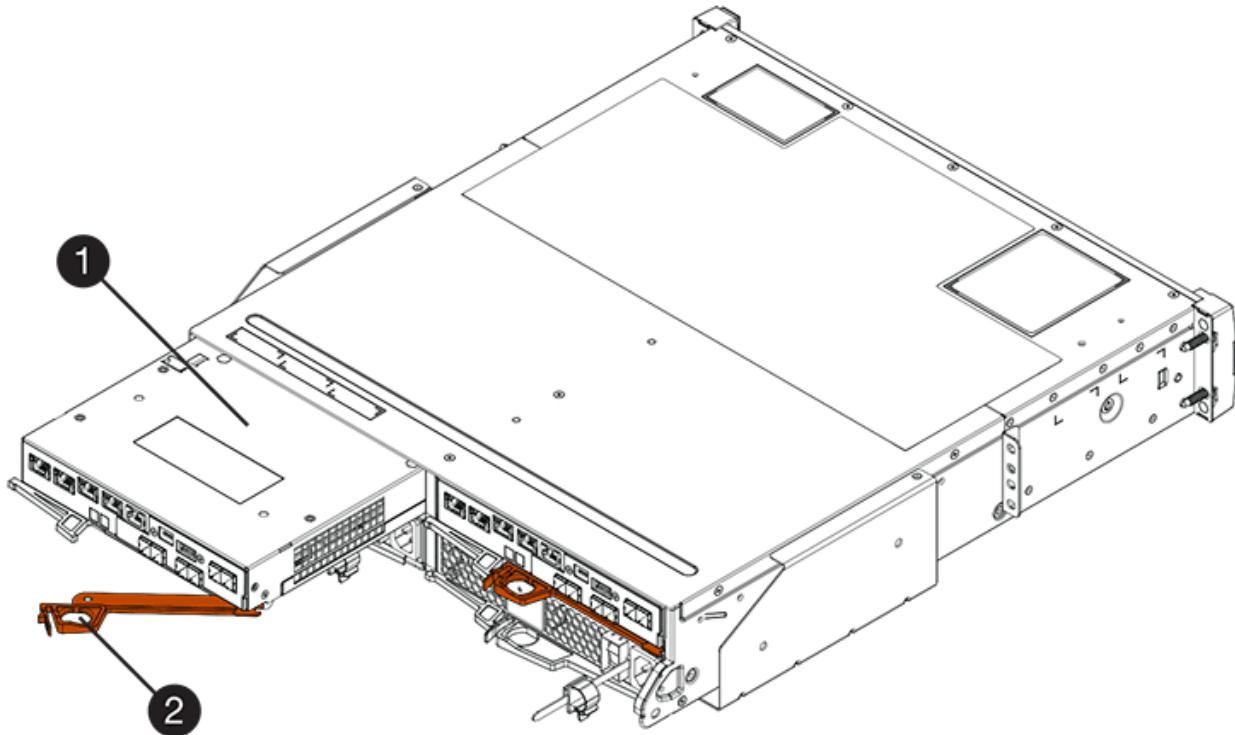


To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

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 | <p>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.</p> <ul style="list-style-type: none"> 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 | <p>Proceed to the next step.</p> <p>After performing the controller replacement, the controllers will automatically resynchronize with the External Key Management Server and the drives will unlock and be accessible.</p> <p> If you receive a seven-segment display lock-down code of 15 after performing a controller replacement of mixed secured drives with internal key management, contact technical support.</p> |
| All secured drives, External Key Management, you have temporarily switched back to Internal Key Management for the controller replacement procedure | <p>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.</p> <ul style="list-style-type: none"> 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 `cfrmgr` 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.xxxxx`.
 - 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.

SANtricity OS

Overview of upgrading the SANtricity OS

You can upgrade your operating system and system hardware components to the latest version of SANtricity software and firmware.

These upgrade procedures include separate instructions for the following:

- Single controller — Includes procedures for upgrading the storage array's software and, optionally, the IOM firmware and the nonvolatile static random access memory (NVS RAM).
- Multiple controllers — Includes procedures for upgrading SANtricity OS software on multiple storage arrays of the same type.
- Drive — Includes instructions for upgrading the drive's firmware.

Before you begin the upgrade, be sure to review the [Upgrade considerations](#).

Upgrade considerations

To ensure a successful upgrade, review the following upgrade considerations.

Controller upgrades (single or multiple)

Review these key considerations before upgrading controllers.

Current versions

You can view the current versions of your software and firmware, as follows:

- For a single controller, use the SANtricity System Manager interface. Go to **Support > Upgrade Center**, and then click the link for **Software and Firmware Inventory**.
- For multiple controllers, use the SANtricity Unified Manager interface. Go to the **Manage** page for discovered storage arrays. The versions are shown in the **SANtricity OS Software** column. The controller firmware and NVSRAM information is available in a pop-up dialog box when you click on the SANtricity OS version in each row.

Components included in the upgrade

The following components are included in the SANtricity OS upgrade process:

- **System Manager**— System Manager is the software that manages the storage array.
- **Controller firmware**— Controller firmware manages the I/O between hosts and volumes.
- **IOM firmware**— The I/O module (IOM) firmware manages the connection between a controller and a drive shelf. It also monitors the status of the components.
- **Supervisor software**— Supervisor software is the virtual machine on a controller in which the software runs.

Components to upgrade separately

The following components must be upgraded separately:

- **Controller NVSRAM**— Controller NVSRAM is a controller file that specifies the default settings for the controllers. Instructions for upgrading the NVSRAM are included with the instructions for upgrading the controllers.
- **Drive firmware**— See [Upgrade drive firmware](#) for separate instructions.
- **Multipath/failover driver**— As part of the upgrade process, the host's multipath/failover driver might also need to be upgraded so the host can interact with the controllers correctly. If hosts running operating systems other than Microsoft Windows have I/O connections to your storage system, upgrade the multipath drivers for those hosts. For compatibility information, refer to the [NetApp Interoperability Matrix](#). For upgrade instructions, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).
- **SANtricity Unified Manager**— Unified Manager is the software that manages multiple storage systems, including the E2800, E5700, EF300, and EF600 models. Unified Manager is part of the SANtricity Web Services Proxy, which is a RESTful API server installed separately on a host system to manage hundreds of new and legacy NetApp E-Series storage systems. For more information, see [SANtricity Web Services Proxy overview](#).
- **Utilities**— Other management utilities require separate upgrades, such as the SANtricity Windows Host Utility, the SANtricity Linux Host Utility, and SANtricity Windows DSM. For more information about these utilities, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).
- **Legacy systems**— If your storage system is part of a storage network that includes older storage systems, you might need to use the legacy SANtricity Storage Manager Enterprise Management Window (EMW) to provide an enterprise view of all of your storage systems. In this case, check to see if there is a newer maintenance release of SANtricity Storage Manager.

Dual controllers and I/O processing

If a storage array contains two controllers and you have a multipath driver installed, the storage array can continue to process I/O while the upgrade occurs. During the upgrade, the following process occurs:

1. Controller A fails over all its LUNs to controller B.
2. Upgrade occurs on controller A.
3. Controller A takes back its LUNs and all of controller B's LUNs.
4. Upgrade occurs on controller B.

After the upgrade completes, you might need to manually redistribute volumes between the controllers to

ensure volumes return to the correct owning controller.

Health check

A health check runs as part of the upgrade process. This health check assesses all storage array components to make sure the upgrade can proceed. The following conditions might prevent the upgrade:

- Failed assigned drives
- Hot spares in use
- Incomplete volume groups
- Exclusive operations running
- Missing volumes
- Controller in non-optimal status
- Excess number of event log events
- Configuration database validation failure
- Drives with old versions of DACstore

You also can run the pre-upgrade health check separately without doing an upgrade.

Immediate or staged upgrade

You can activate the upgrade immediately or stage it for a later time. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. Depending on the I/O load and cache size, a controller upgrade can typically take between 15 to 25 minutes to complete. The controllers reboot and fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

Drive firmware upgrade

Review these key considerations before upgrading your drive firmware.

Drive compatibility

Each drive firmware file contains information about the drive type on which the firmware runs. You can download the specified firmware file only to a compatible drive. System Manager automatically checks compatibility during the upgrade process.

Drive upgrade methods

There are two types of drive firmware upgrade methods: online and offline.

| Online upgrade | Offline upgrade |
|---|---|
| <p>During an online upgrade, drives are upgraded sequentially, one at a time. The storage array continues processing I/O while the upgrade occurs. You do not have to stop I/O. If a drive can do an online upgrade, the online method is used automatically.</p> <p>Drives that can do an online upgrade include the following:</p> <ul style="list-style-type: none"> • Drives in an Optimal pool • Drives in an Optimal redundant volume group (RAID 1, RAID 5, and RAID 6) • Unassigned drives • Standby hot spare drives <p>Doing an online drive firmware upgrade can take several hours exposing the storage array to potential volume failures. Volume failure could occur in these cases:</p> <ul style="list-style-type: none"> • In a RAID 1 or RAID 5 volume group, one drive fails while a different drive in the volume group is being upgraded. • In a RAID 6 pool or volume group, two drives fail while a different drive in the pool or volume group is being upgraded. | <p>During an offline upgrade, all drives of the same drive type are upgraded at the same time. This method requires stopping I/O activity to the volumes associated with the selected drives. Because multiple drives can be upgraded concurrently (in parallel), the overall downtime is significantly reduced. If a drive can do only an offline upgrade, the offline method is used automatically.</p> <p>The following drives MUST use the offline method:</p> <ul style="list-style-type: none"> • Drives in a non-redundant volume group (RAID 0) • Drives in a non-optimal pool or volume group • Drives in SSD cache |

Upgrade software and firmware for a single controller

You can upgrade a single controller, which ensures that you have all the latest features and fixes.

This process involves upgrading the storage array's software and, optionally, the IOM firmware and the nonvolatile static random access memory (NVSRAM).

Before you begin

- Review [Upgrade considerations](#).
- Determine if you want to upgrade the controller NVSRAM file at the same time as the OS firmware.

Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the controller NVSRAM file if your file has either been patched or is a custom version and you do not want to overwrite it.

- Determine if you want to upgrade your IOM firmware.

Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the IOM firmware if you do not want to upgrade it as part of the SANtricity OS software upgrade or if technical support has instructed you to downgrade your IOM firmware (you can only downgrade firmware

by using the command line interface).

- Decide if you want to activate your OS upgrade now or later.

Reasons for activating later might include:

- **Time of day** – Activating the software and firmware can take a long time, so you might want to wait until I/O loads are lighter. The controllers fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** – You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

Step 1: Download software files from support site

In this step, you go to the NetApp Support site to save the new downloadable package (DLP) software files to your management host system.

The time required for the upgrade depends on your storage array configuration and the components that you are upgrading.

Steps

1. If your storage array contains only one controller or you do not have a multipath driver installed, stop I/O activity to the storage array to prevent application errors. If your storage array has two controllers and you have a multipath driver installed, you do not need to stop I/O activity.



If you are upgrading SANtricity OS on a StorageGRID appliance (for example, SG5612 or SG5760), you need to stop I/O activity by placing the appliance into maintenance mode before continuing with this procedure, or data could be lost. For detailed steps, see the installation and maintenance instructions for your StorageGRID appliance.

2. From the System Manager interface, select **Support > Upgrade Center**.
 3. In the area labeled "SANtricity OS Software upgrade," click **NetApp SANtricity OS Downloads** to open the NetApp Support site.
 4. From the Downloads page, select **E-Series SANtricity OS Controller Software**.
-
- Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.
5. Follow the on-screen instructions to download the most recent OS software for your controller model. If you also want to upgrade the NVSRAM, download the NVSRAM file for a single controller.

Step 2: Transfer software files to the controllers

In this step, you transfer the software files to your controller so you can begin the upgrade process. The components are copied from the management client to the controllers and placed in a staging area in flash memory.



Risk of data loss or risk of damage to the storage array — Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

Steps

1. (Optional). If you are planning to perform an upgrade during a specific maintenance window, you might want to run a pre-upgrade health check to determine if there are any major storage array problems in advance. If this is the case, select **pre-upgrade health check** from the Upgrade Center in System Manager (**Support > Upgrade Center**), and follow any on-screen instructions. Otherwise, you can skip this step, because a health check is part of the upgrade process.
2. If you do NOT want to upgrade the IOM firmware at this time, click **Suspend IOM Auto-Synchronization** and follow the instructions in the dialog box.

If you have a storage array with a single controller, the IOM firmware is not upgraded.

3. From the Upgrade Center in System Manager, click **Begin Upgrade** from "SANtricity OS Software upgrade."

The Upgrade SANtricity OS Software dialog appears.

4. Select one or more files to begin the upgrade process:

- a. Select the SANtricity OS Software file by clicking **Browse** and navigating to the OS software file you downloaded from the Support site.
- b. Select the Controller NVSRAM file by clicking **Browse** and navigating to the NVSRAM file that you downloaded from the Support site. Controller NVSRAM files have a filename similar to N2800-830000-000.dlp.

These actions occur:

- By default, only the files that are compatible with the current storage array configuration appear.
- When you select a file for upgrade, the file's name and size appear.

5. (Optional) If you selected a SANtricity OS Software file to upgrade, you can transfer the files to the controller without activating them by selecting the **Transfer files now, but do not upgrade (activate upgrade later)** check box.

6. Click **Start**, and confirm that you want to perform the operation.

You can cancel the operation during the pre-upgrade health check, but not during transferring or activating.

7. (Optional) To see a list of what was upgraded, click **Save Log**.

The file is saved in the Downloads folder for your browser with the name, `drive_upgrade_log-timestamp.txt`.

If you have already activated your software files, go to [Step 4: Complete software and firmware upgrade](#); otherwise, go to [Step 3: Activate software files](#).

Step 3: Activate software files

Follow this step only if you have software or firmware that has been transferred but not activated. To check this state, look for a notification in the Notifications area of the System Manager Home page or in the Upgrade Center page.

When you perform the activation operation, the current software and firmware is replaced with the new software and firmware. You cannot stop the activation process after it starts.

Steps

1. From the System Manager interface, select **Support > Upgrade Center**.
2. In the area labeled "SANtricity OS Software upgrade," click **Activate**, and confirm that you want to perform the operation.
3. (Optional) To see a list of what was upgraded, click **Save Log**.

The file is saved in the Downloads folder for your browser with the name, `drive_upgrade_log-timestamp.txt`.

Step 4: Complete software and firmware upgrade

Complete the software and firmware upgrade by verifying the versions in the Software and Firmware Inventory dialog box.

Before you begin

- You must have activated your software or firmware.

Steps

1. From System Manager, verify that all components appear on the Hardware page.
2. Verify the new software and firmware versions by checking the Software and Firmware Inventory dialog box (go to **Support > Upgrade Center**, and then click the link for **Software and Firmware Inventory**).
3. If you upgraded controller NVSRAM, any custom settings that you have applied to the existing NVSRAM are lost during the process of activation. You need to apply the custom settings to the NVSRAM again after the process of activation is complete.
4. If any of the following errors occur during the upgrade procedure, take the appropriate recommended action.

| If you encounter this firmware download error... | Then do the following... |
|--|--|
| Failed assigned drives | <p>One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information.</p> <p>When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing.</p> <p>You can replace the failed drive while the storage array is receiving I/O.</p> |
| Check storage array | <ul style="list-style-type: none"> • Make sure that an IP address has been assigned to each controller. • Make sure that all cables connected to the controller are not damaged. • Make sure that all cables are tightly connected. |

| If you encounter this firmware download error... | Then do the following... |
|---|---|
| Integrated hot spare drives | This error condition must be corrected before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Incomplete volume groups | If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Exclusive operations (other than background media/parity scan) currently running on any volume groups | If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations. |
| Missing volumes | You must correct the missing volume condition before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Either controller in a state other than Optimal | One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Mismatched Storage Partition information between Controller Object Graphs | An error occurred while validating the data on the controllers. Contact technical support to resolve this issue. |
| SPM Verify Database Controller check fails | A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue. |
| Configuration Database Validation (if supported by the storage array's controller version) | A configuration database error occurred on a controller. Contact technical support to resolve this issue. |
| MEL Related Checks | Contact technical support to resolve this issue. |
| More than 10 DDE Informational or Critical MEL events were reported in the last 7 days | Contact technical support to resolve this issue. |
| More than 2 Page 2C Critical MEL Events were reported in the last 7 days | Contact technical support to resolve this issue. |

| If you encounter this firmware download error... | Then do the following... |
|---|--|
| More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days | Contact technical support to resolve this issue. |
| More than 4 critical MEL entries in the last 7 days | Contact technical support to resolve this issue. |

What's next?

Your controller software upgrade is complete. You can resume normal operations.

Upgrade software and firmware for multiple controllers

You can upgrade multiple controllers of the same type with SANtricity Unified Manager.

Before you begin

- Review [Upgrade considerations](#).
- Determine if you want to activate your software upgrade now or later. You might choose to activate later for these reasons:
 - Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers fail over during activation, so performance might be lower than usual until the upgrade completes.
 - Type of package** — You might want to test the new OS software on one storage array before you upgrade the files on other storage arrays.
- Review these precautions:



Risk of data loss or risk of damage to the storage array - Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.



If you are upgrading SANtricity OS on a StorageGRID appliance (for example, SG5612 or SG5760), you need to stop I/O activity by placing the appliance into maintenance mode before continuing with this procedure, or data could be lost. For detailed steps, see the installation and maintenance instructions for your StorageGRID appliance.

Step 1: Perform pre-upgrade health check

A health check runs as part of the upgrade process, but you also can run a health check separately before you begin. The health check assesses components of the storage array to make sure that the upgrade can proceed.

Steps

- Open Unified Manager.
- From the main view, select **Manage**, and then select **Upgrade Center > Pre-Upgrade Health Check**.

The Pre-Upgrade Health Check dialog box opens and lists all the discovered storage systems.

- If needed, filter or sort the storage systems in the list, so you can view all systems that are not currently in the Optimal state.

4. Select the check boxes for the storage systems that you want to run through the health check.
 5. Click **Start**.
- The progress is shown in the dialog box while the health check is performed.
6. When the health check completes, you can click on the ellipses (...) to the right of each row to view more information and perform other tasks.



If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.

Step 2: Download software files from support site

In this step, you go to the NetApp Support site to save the new downloadable package (DLP) software files to your management host system.

Steps

1. If your storage array contains only one controller or a multipath driver is not in use, stop I/O activity to the storage array to prevent application errors. If your storage array has two controllers and you have a multipath driver installed, you do not need to stop I/O activity.
2. From Unified Manager's main view, select **Manage**, and then select one or more storage arrays that you want to upgrade.
3. Select **Upgrade Center > Upgrade SANtricity OS Software**.

The Upgrade SANtricity OS software page appears.

4. Download the latest SANtricity OS software package from the NetApp support site to your local machine.
 - a. Click **Add new file to software repository**.
 - b. Click the link for finding the latest **SANtricity OS Downloads**.
 - c. Click the **Download Latest Release** link.
 - d. Follow the remaining instructions to download the SANtricity OS file and the NVSRAM file to your local machine.



Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.

Step 3: Transfer software files to the controllers

You load the SANtricity OS software file and the NVSRAM file into the repository so it is accessible to the Unified Manager Upgrade Center.



Risk of data loss or risk of damage to the storage array - Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

Steps

1. From Unified Manager's main view, select **Manage**, and then select one or more storage arrays that you want to upgrade.

2. Select **Upgrade Center > Upgrade SANtricity OS Software**.

The Upgrade SANtricity OS software page appears.

3. Download the latest SANtricity OS software package from the NetApp support site to your local machine.

a. Click **Add new file to software repository**.

b. Click the link for finding the latest **SANtricity OS Downloads**.

c. Click the **Download Latest Release** link.

d. Follow the remaining instructions to download the SANtricity OS file and the NVSRAM file to your local machine.



Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.

4. Select the OS software file and the NVSRAM file that you want to use to upgrade the controllers:

a. From the **Select a SANtricity OS software file** drop-down, select the OS file that you downloaded to your local machine.

If there are multiple files available, the files are sorted from newest date to oldest date.



The software repository lists all software files associated with the Web Services Proxy. If you do not see the file that you want to use, you can click the link, **Add new file to software repository**, to browse to the location where the OS file that you want to add resides.

b. From the **Select an NVSRAM file** drop-down, select the controller file that you want to use.

If there are multiple files, the files are sorted from newest date to oldest date.

5. In the Compatible Storage Array table, review the storage arrays that are compatible with the OS software file that you selected, and then select the arrays you want to upgrade.

- The storage arrays that you selected in the Manage view and that are compatible with the selected firmware file are selected by default in the Compatible Storage Array table.
- The storage arrays that cannot be updated with the selected firmware file are not selectable in the Compatible Storage Array table as indicated by the status **Incompatible**.

6. (Optional) To transfer the software file to the storage arrays without activating them, select the **Transfer the OS software to the storage arrays, mark it as staged, and activate at a later time** check box.

7. Click **Start**.

8. Depending on whether you chose to activate now or later, do one of the following:

- Type **TRANSFER** to confirm that you want to transfer the proposed OS software versions on the arrays you selected to upgrade, and then click **Transfer**.

To activate the transferred software, select **Upgrade Center > Activate Staged OS Software**.

- Type **UPGRADE** to confirm that you want to transfer and activate the proposed OS software versions on the arrays you selected to upgrade, and then click **Upgrade**.

The system transfers the software file to each storage array you selected to upgrade and then activates

that file by initiating a reboot.

The following actions occur during the upgrade operation:

- A pre-upgrade health check runs as part of the upgrade process. The pre-upgrade health check assesses all storage array components to make sure that the upgrade can proceed.
 - If any health check fails for a storage array, the upgrade stops. You can click the ellipsis (...) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the upgrade.
 - You can cancel the upgrade operation after the pre-upgrade health check.
9. (Optional) Once the upgrade has completed, you can see a list of what was upgraded for a specific storage array by clicking the ellipsis (...) and then selecting **Save Log**.

The file is saved in the Downloads folder for your browser with the name `upgrade_log-<date>.json`.

Step 4: Activate staged software files (optional)

You can choose to activate the software file immediately or wait until a more convenient time. This procedure assumes you chose to activate the software file at a later time.



You cannot stop the activation process after it starts.

Steps

1. From Unified Manager's main view, select **Manage**. If necessary, click the Status column to sort all storage arrays with a status of "OS Upgrade (awaiting activation)."
2. Select one or more storage arrays that you want to activate software for, and then select **Upgrade Center > Activate Staged OS Software**.

The following actions occur during the upgrade operation:

- A pre-upgrade health check runs as part of the activate process. The pre-upgrade health check assesses all storage array components to make sure that the activation can proceed.
 - If any health check fails for a storage array, the activation stops. You can click the ellipsis (...) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the activation.
 - You can cancel the activate operation after the pre-upgrade health check.
- On successful completion of the pre-upgrade health check, activation occurs. The time it takes to activate depends on your storage array configuration and the components that you are activating.
3. (Optional) After the activation is complete, you can see a list of what was activated for a specific storage array by clicking the ellipsis (...) and then selecting **Save Log**.

The file is saved in the Downloads folder for your browser with the name `activate_log-<date>.json`.

What's next?

Your controller software upgrade is complete. You can resume normal operations.

Upgrade drive firmware

Follow this procedure to upgrade your drives' firmware, which ensures you have all the

latest features and fixes.

Step 1: Download drive firmware files

In this step, you go to the NetApp Support site to download the drive firmware files to your management client.

Steps

1. In SANtricity System Manager, select **Support > Upgrade Center**.
2. Under Drive Firmware upgrade, click **NetApp Support** and log in to the NetApp Support site.
3. From the Support site, click the **Downloads** tab, and then select **Disk Drive & Firmware Matrix**.
4. Select **E-Series and EF-Series Disk Firmware**.
5. Follow the on-screen instructions to download the files.

Step 2: Begin drive firmware upgrade

In this step, you upgrade the drives' firmware.

Before you begin

- Back up your data using disk-to-disk backup, volume copy (to a volume group not affected by the planned firmware upgrade), or a remote mirror.
- Make sure the storage array has an Optimal status.
- Make sure all drives have an Optimal status.
- Make sure no configuration changes are running on the storage array.
- Understand that if the drives are capable of only an offline upgrade, I/O activity to all volumes associated with the drives is stopped.

Steps

1. From the System Manager Upgrade Center (**Support > Upgrade Center**), click **Begin Upgrade** from the "Drive Firmware upgrade" section.

A dialog box appears, which lists the drive firmware files currently in use.

2. Extract (unzip) the files you downloaded from the Support site.
3. Click **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to D_HUC101212CSS600_30602291_MS01_2800_0002 with the extension of .d1p.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

4. Click **Next**.

The Select Drives dialog box appears, which lists the drives that you can upgrade with the selected files.

Only drives that are compatible appear.

The selected firmware for the drive appears in the **Proposed Firmware** information area. If you must change the firmware, click **Back** to return to the previous dialog.

5. Select the type of upgrade you want to perform:

- **Online (default)**— Shows the drives that can support a firmware download *while the storage array is processing I/O*. You do not have to stop I/O to the associated volumes using these drives when you select this upgrade method. These drives are upgraded one at a time while the storage array is processing I/O to those drives.
- **Offline (parallel)**— Shows the drives that can support a firmware download *only while all I/O activity is stopped* on any volumes that use the drives. You must stop all I/O activity on any volumes that use the drives you are upgrading when you select this upgrade method. Drives that do not have redundancy must be processed as an offline operation. This requirement includes any drive associated with SSD cache, a RAID 0 volume group, or any pool or volume group that is degraded. The offline (parallel) upgrade is typically faster than the online (default) method.

6. In the first column of the table, select the drive or drives you want to upgrade.

7. Click **Start**, and confirm that you want to perform the operation.

If you need to stop the upgrade, click **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.

8. (Optional) To see a list of what was upgraded, click **Save Log**.

The file is saved in the Downloads folder for your browser with the name `drive_upgrade_log-timestamp.txt`.

9. If any of the following errors occur during the upgrade procedure, take the appropriate recommended action.

| If you encounter this firmware download error... | Then do the following... |
|--|--|
| <ul style="list-style-type: none">• Failed assigned drives | <p>One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information.</p> <p>When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing.</p> <p>You can replace the failed drive while the storage array is receiving I/O.</p> |
| Check storage array | <ul style="list-style-type: none">• Make sure that an IP address has been assigned to each controller.• Make sure that all cables connected to the controller are not damaged.• Make sure that all cables are tightly connected. |
| Integrated hot spare drives | This error condition must be corrected before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem. |

| If you encounter this firmware download error... | Then do the following... |
|---|---|
| Incomplete volume groups | If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Exclusive operations (other than background media/parity scan) currently running on any volume groups | If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations. |
| Missing volumes | You must correct the missing volume condition before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Either controller in a state other than Optimal | One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem. |
| Mismatched Storage Partition information between Controller Object Graphs | An error occurred while validating the data on the controllers. Contact technical support to resolve this issue. |
| SPM Verify Database Controller check fails | A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue. |
| Configuration Database Validation (if supported by the storage array's controller version) | A configuration database error occurred on a controller. Contact technical support to resolve this issue. |
| MEL Related Checks | Contact technical support to resolve this issue. |
| More than 10 DDE Informational or Critical MEL events were reported in the last 7 days | Contact technical support to resolve this issue. |
| More than 2 Page 2C Critical MEL Events were reported in the last 7 days | Contact technical support to resolve this issue. |
| More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days | Contact technical support to resolve this issue. |
| More than 4 critical MEL entries in the last 7 days | Contact technical support to resolve this issue. |

What's next?

Your drive firmware upgrade is complete. You can resume normal operations.

Maintain systems

EF300 and EF600

Maintain EF300 and EF600 hardware

For the EF300 and EF600 storage systems, you can perform maintenance procedures on the following components.

Batteries

A battery is included with a controller and preserves cached data if the AC power fails.

Controllers

A controller consists of a board, firmware, and software. It controls the drives and implements the SANtricity System Manager functions.

DIMMs

You must replace a DIMM (dual in-line memory module) when a memory mismatch is present, or you have a failed DIMM.

Drives

A drive is a device that provides the physical storage media for data.

Fans

Each EF300 or EF600 controller shelf or drive shelf includes five fans for cooling the controller.

Host interface cards (HICs)

A host interface card (HIC) must be installed within a controller canister. The EF600 controller includes host ports on the optional HIC. Host ports that are built into the HIC are called HIC ports.

Host port protocol

You can convert the protocol of a host to a different protocol so that compatibility and communication can be established.

Power supplies

A power supply provides a redundant power source in a controller shelf.

SAS expansion cards

A SAS expansion card may be installed within a controller canister. The EF300 controller supports SAS expansion.

Batteries

Requirements for EF300 or EF600 battery replacement

Before you replace an EF300 or EF600 battery, review the requirements and considerations.

A battery is included with a controller and preserves cached data if the AC power fails.

Recovery Guru alerts

If the Recovery Guru in SANtricity System Manager reports one of following statuses, you must replace the affected battery:

- Battery Failed
- Battery Replacement Required

From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.

Procedure overview

To protect your data, you must replace a failed battery as soon as possible.

The following is an overview of the steps to replace a battery in EF300 or EF600 controllers:

1. Take controller offline.
2. Remove the controller canister.
3. Replace the battery.
4. Replace the controller canister.
5. Bring the controller online.

Requirements

If you plan to replace a battery, you must have:

- A replacement battery.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Optionally, you can use the command line interface (CLI) to perform some of the procedures. If you do not have access to the CLI, you can do one of the following:

- **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
- **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW

by selecting **Tools > Execute Script**.

Replace EF300 or EF600 battery

You can replace a battery in an EF300 or EF600 storage system.

About this task

Each controller canister includes a battery that preserves cached data if the AC power fails. If the Recovery Guru in SANtricity System Manager reports either a Battery Failed status or a Battery Replacement Required status, you must replace the affected battery.

Before you begin

- Verify that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.
- Review the [Requirements for EF300 or EF600 battery replacement](#).

What you'll need

- The replacement battery.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller offline

Back up data and place the affected controller offline.

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which battery to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.
 - a. Select **Hardware**.

- b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
- c. Select the controller that you want to place offline.
- d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

5. Wait for SANtricity System Manager to update the controller's status to offline.
-
- Do not begin any other operations until after the status has been updated.
6. Select **Recheck** from the Recovery Guru, and confirm that the OK to remove field in the Details area displays Yes, indicating that it is safe to remove this component.

Step 2: Remove controller canister

Replace the failed battery with a new one.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
 2. Label each cable that is attached to the controller canister.
 3. Disconnect all the cables from the controller canister.
-
- To prevent degraded performance, do not twist, fold, pinch, or step on the cables.
4. Confirm that the Cache Active LED on the back of the controller is off.
 5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 3: Remove failed battery

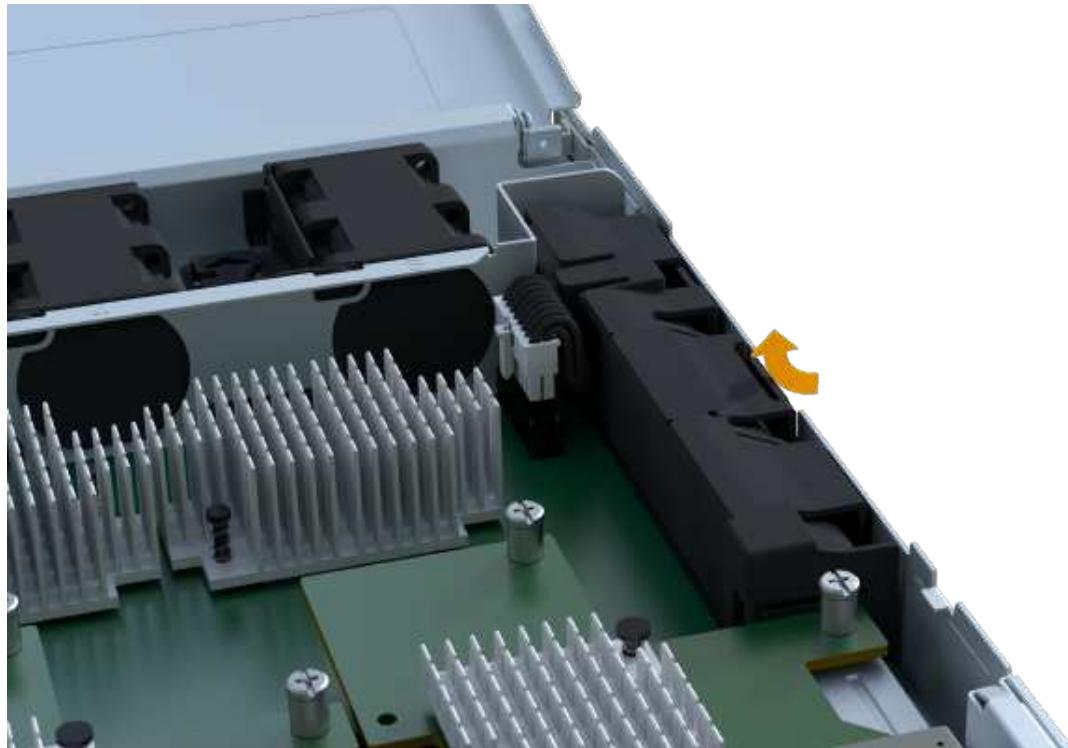
Pull the failed battery out of the controller.

Steps

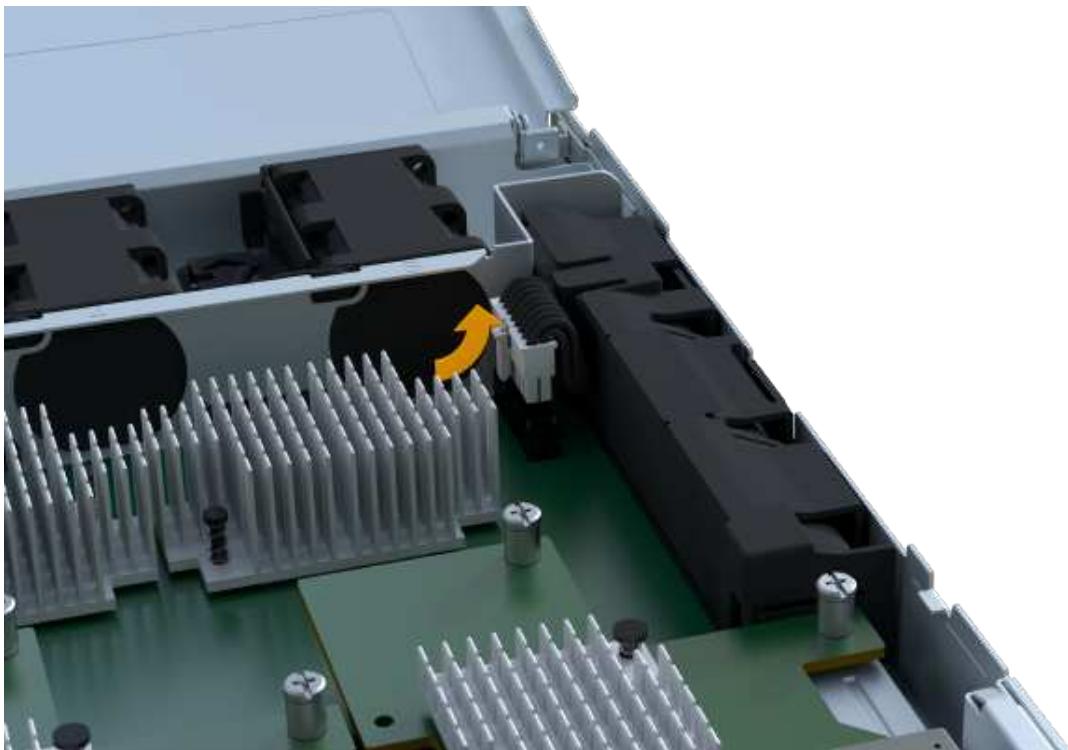
1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

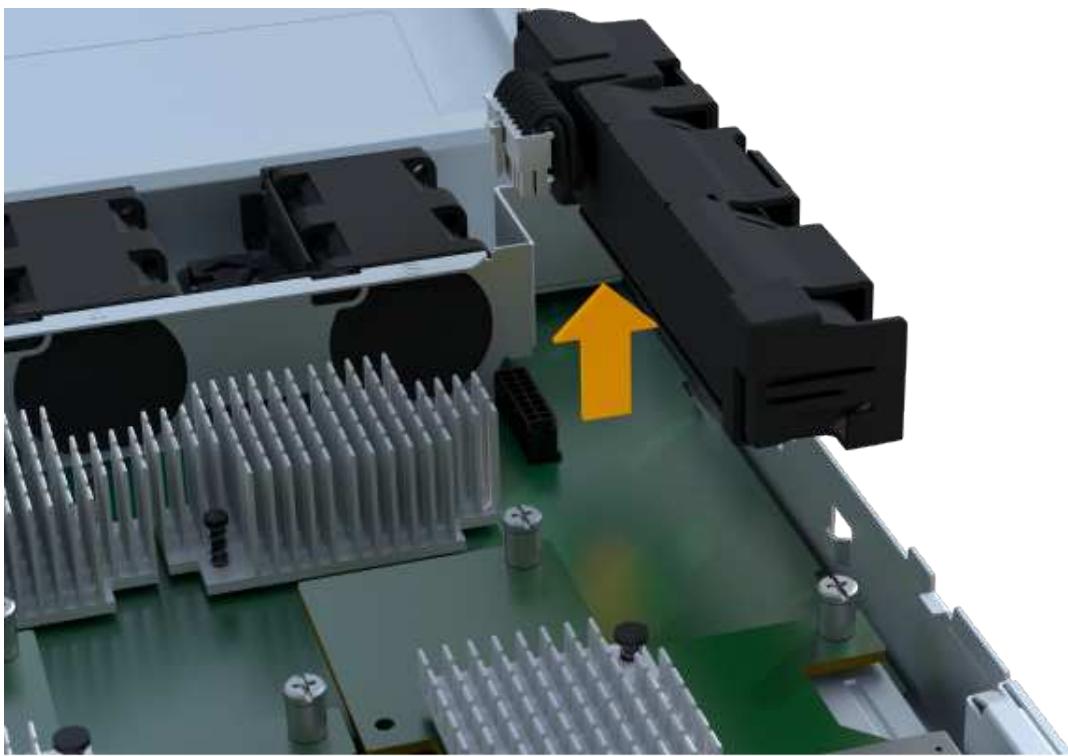
3. Locate the 'press' tab on the side of the controller.
4. Unlatch the battery by pressing the tab and squeezing the battery casing.



5. Gently squeeze the connector housing the battery wiring. Pull up, disconnecting the battery from the board.



6. Lift the battery out of the controller and place on a flat, static-free surface.



7. Follow the appropriate procedures for your location to recycle or dispose of the failed battery.



To comply with International Air Transport Association (IATA) regulations, never ship a lithium battery by air unless it is installed within the controller shelf.

Step 4: Install new battery

After you have removed the failed battery from the controller canister, follow this step to install the new battery.

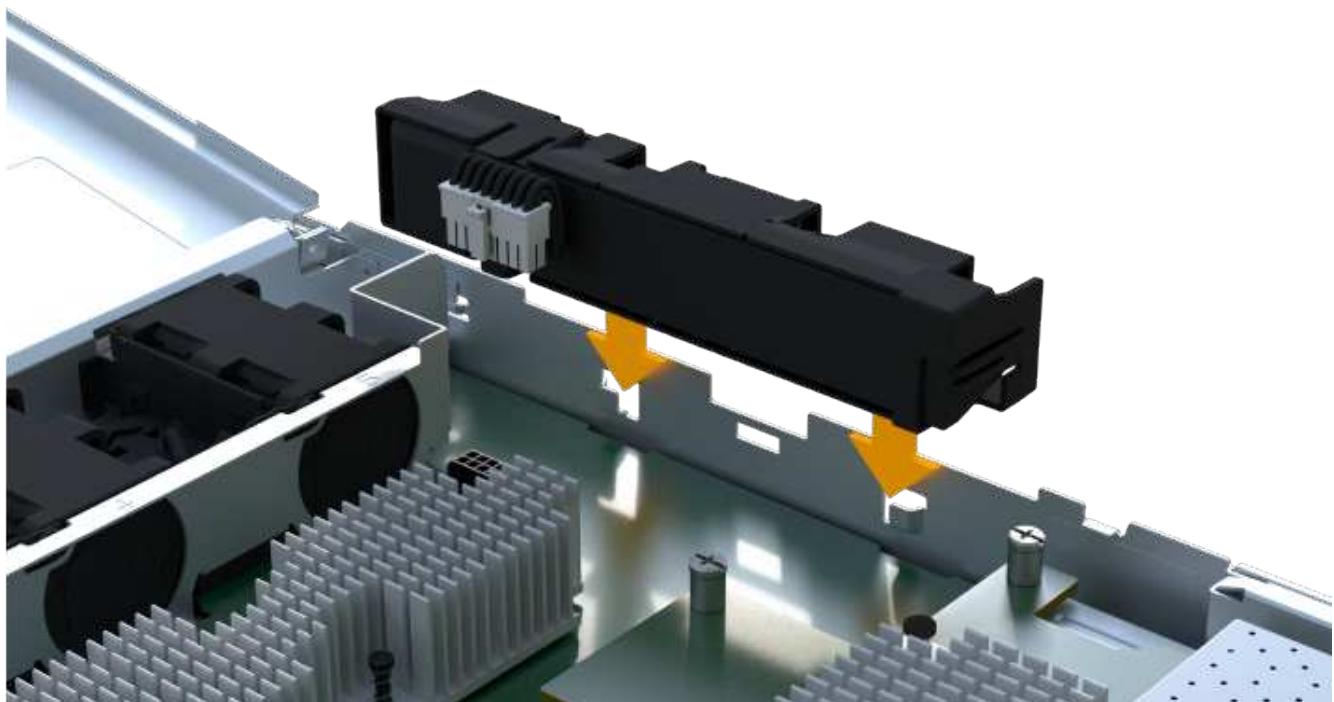
Steps

1. Unpack the new battery, and set it on a flat, static-free surface.



To comply with IATA safety regulations, replacement batteries are shipped with a state of charge (SoC) of 30 percent or less. When you reapply power, keep in mind that write caching does not resume until the replacement battery is fully charged and it has completed its initial learn cycle.

2. Insert the battery into the controller by lining up the battery casing with the metal latches on the side of the controller.



The battery clicks into place.

3. Plug the battery connector back into the board.

Step 5: Reinstall controller canister

Reinstall the controller into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



Step 6: Complete battery replacement

Place the controller online, collect support data, and resume operations.

Steps

1. Place controller online.
 - a. In System Manager, navigate to the Hardware page.
 - b. Select **Show back of controller**.
 - c. Select the controller with the replaced battery.
 - d. Select **Place online** from the drop-down list.
2. As the controller boots, check the controller LEDs.

When communication with the other controller is reestablished:

- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.

3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
 - d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
 - e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your battery replacement is complete. You can resume normal operations.

Controllers

Requirements for EF300 or EF600 controller replacement

Before you replace an EF300 or EF600 controller, review the requirements and considerations.

A controller consists of a board, firmware, and software. It controls the drives and implements the SANtricity System Manager functions.

Controller replacement requirements

Before you replace a controller, you must have:

- A replacement controller canister with the same part number as the controller canister you are replacing.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Replacement while powered on

You can replace a controller canister while your storage array is powered on and performing host I/O operations, if the following conditions are true:

- The second controller canister in the shelf has Optimal status.

- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.

Replace EF300 or EF600 controller

You can replace a single controller in your EF300 or EF600 controller shelf.

About this task

When you replace a failed controller canister, you must remove the battery, power supply, DIMMs, fans, and host interface card (HIC) from the original controller canister, and then install them in the replacement controller canister.

Before you begin

- Review [Requirements for EF300 or EF600 controller replacement](#).
- Determine if you have a failed controller canister in one of two ways:
 - The Recovery Guru in SANtricity System Manager directs you to replace the controller canister.
 - The amber Attention LED on the controller canister is on, indicating that the controller has a fault.

What you'll need

- A replacement controller canister with the same part number as the controller canister you are replacing.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- A #1 Phillips screwdriver
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace controller

Prepare to replace a failed controller canister by verifying that the replacement controller canister has the correct FRU part number, backing up the configuration, and collecting support data.

Steps

1. Unpack the new controller canister, and set it on a flat, static-free surface.

Save the packing materials to use when shipping the failed controller canister.

2. Locate the MAC address and FRU part number labels on the back of the controller canister.
3. From SANtricity System Manager, locate the replacement part number for the controller canister you are replacing.

When a controller has a fault and needs to be replaced, the replacement part number is displayed in the Details area of the Recovery Guru. If you need to find this number manually, follow these steps:

- a. Select **Hardware**.
- b. Locate the controller shelf, which is marked with the controller icon
- c. Click the controller icon.
- d. Select the controller, and click **Next**.

- e. On the **Base** tab, make a note of the **Replacement Part Number** for the controller.
4. Confirm that the replacement part number for the failed controller is the same as the FRU part number for the replacement controller.



Possible loss of data access — If the two-part numbers are not the same, do not attempt this procedure. In addition, if the failed controller canister includes a host interface card (HIC), you must install that HIC into the new controller canister. The presence of mismatched controllers or HICs causes the new controller to lock down when you bring it online.

5. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

6. If the controller is not already offline, take it offline now using SANtricity System Manager.

- a. Select **Hardware**.
- b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
- c. Select the controller that you want to place offline.
- d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

7. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

8. Select **Recheck** from the Recovery Guru, and confirm that the **OK to remove** field in the Details area displays **Yes**, indicating that it is safe to remove this component.

Step 2: Remove failed controller

Remove a controller canister to replace the failed canister with a new one.

This is a multi-step procedure that requires you to remove the following components: battery, host interface card, power supply, DIMMs, and fans.

Step 2a: Remove controller canister

Remove the failed controller canister so you can replace it with a new one.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. If the controller canister has a HIC that uses SFP+ transceivers, remove the SFPs.

Because you must remove the HIC from the failed controller canister, you must remove any SFPs from the HIC ports. When you reconnect the cables, you can move those SFPs to the new controller canister.

5. Confirm that the Cache Active LED on the back of the controller is off.
6. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



7. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



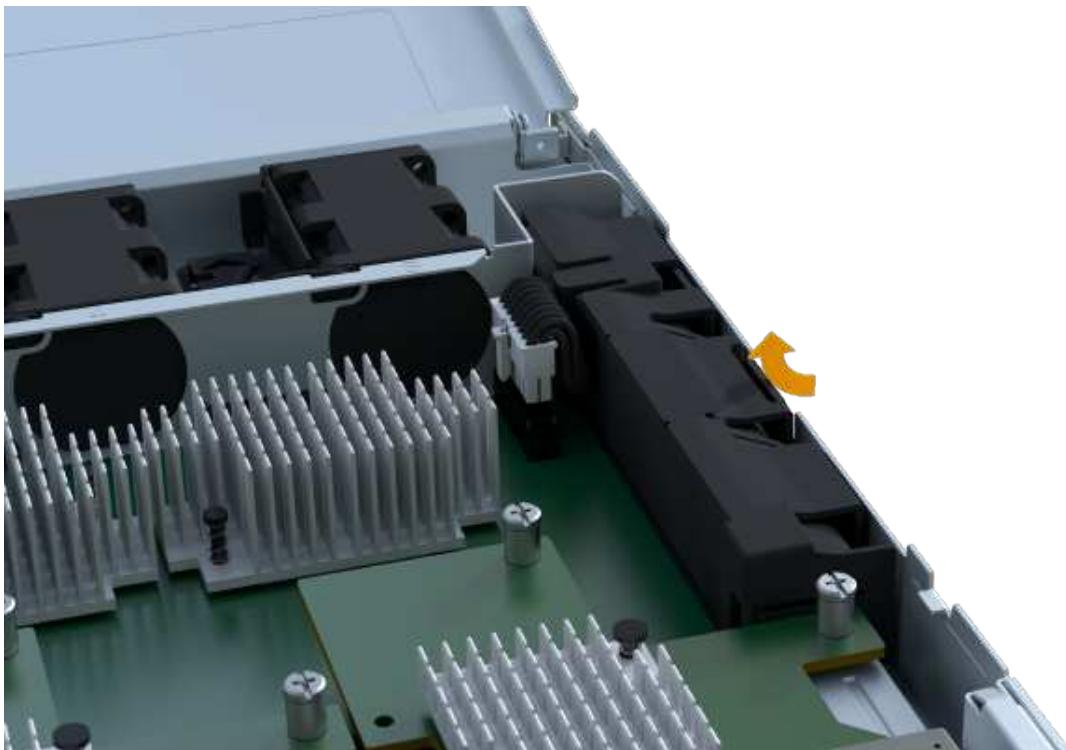
8. Place the controller canister on a flat, static-free surface.

Step 2b: Remove battery

Remove the battery from the failed controller canister so you can install it in the new controller canister.

Steps

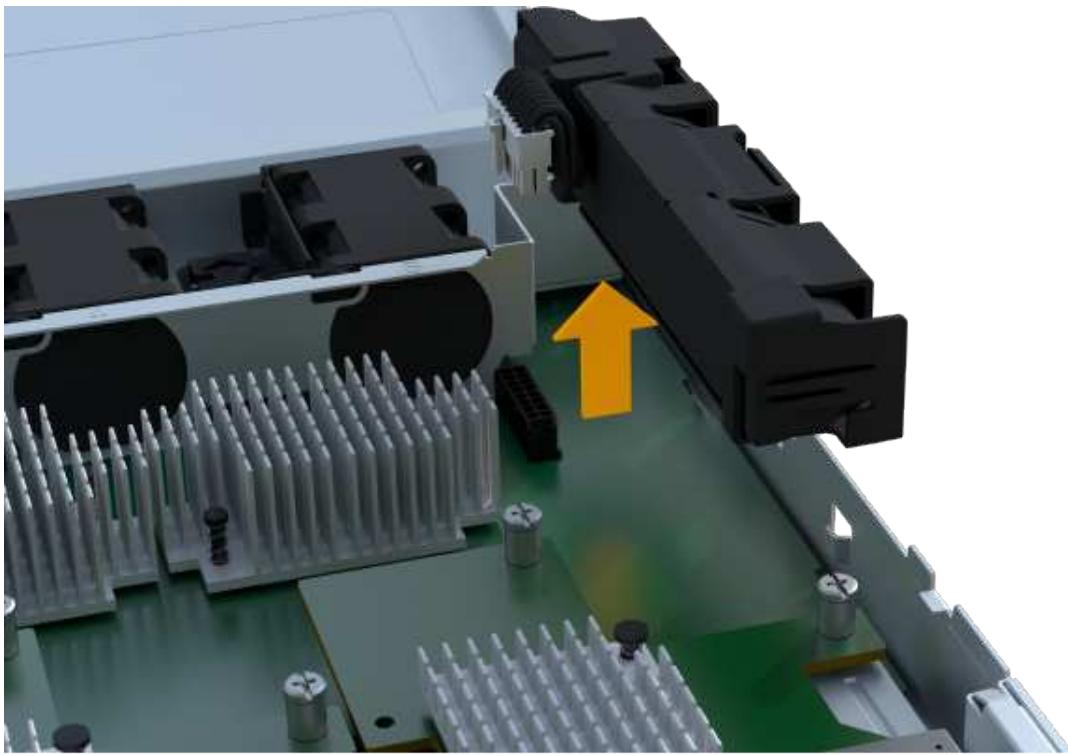
1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Locate the 'press' tab on the side of the controller.
3. Unlatch the battery by pressing the tab and squeezing the battery casing.



4. Gently squeeze the connector housing the battery wiring. Pull up, disconnecting the battery from the board.



5. Lift the battery out of the controller and place on a flat, static-free surface.

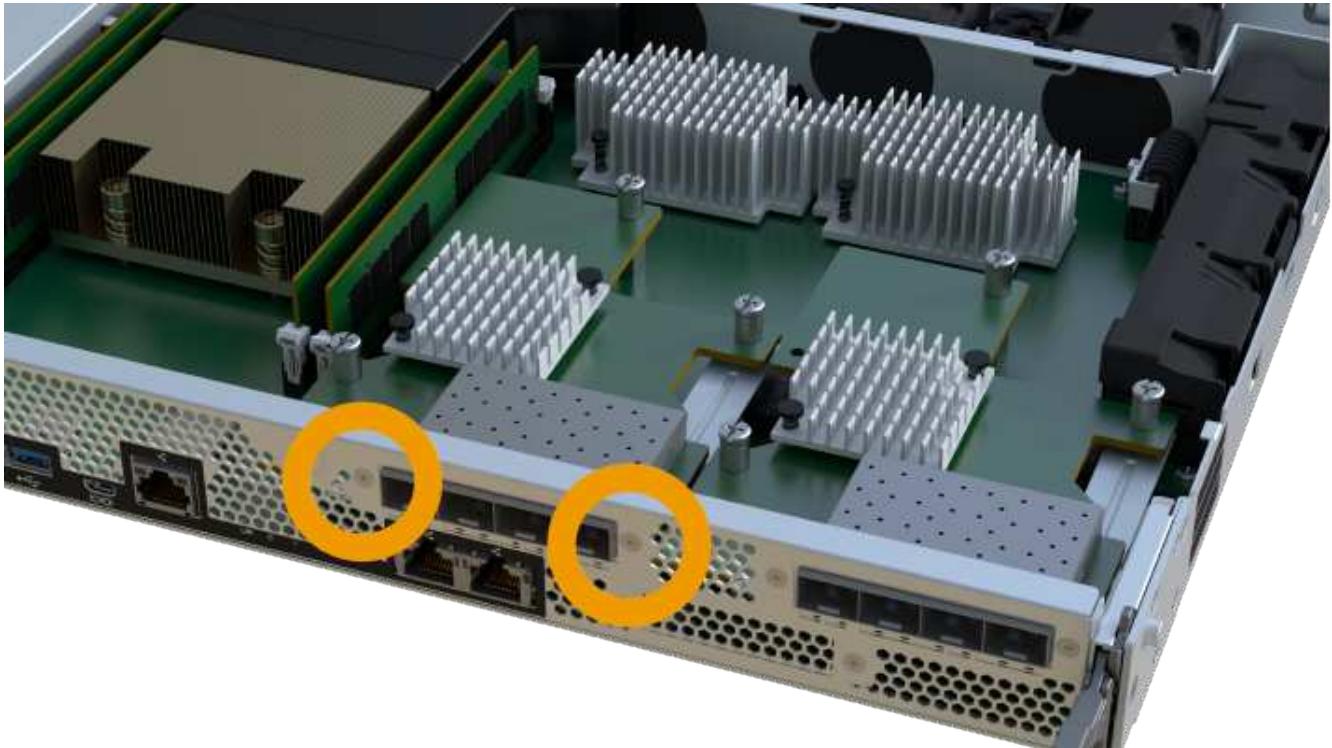


Step 2c: Remove the HIC

If the controller canister includes a HIC, you must remove the HIC from the original controller canister. Otherwise, you can skip this step.

Steps

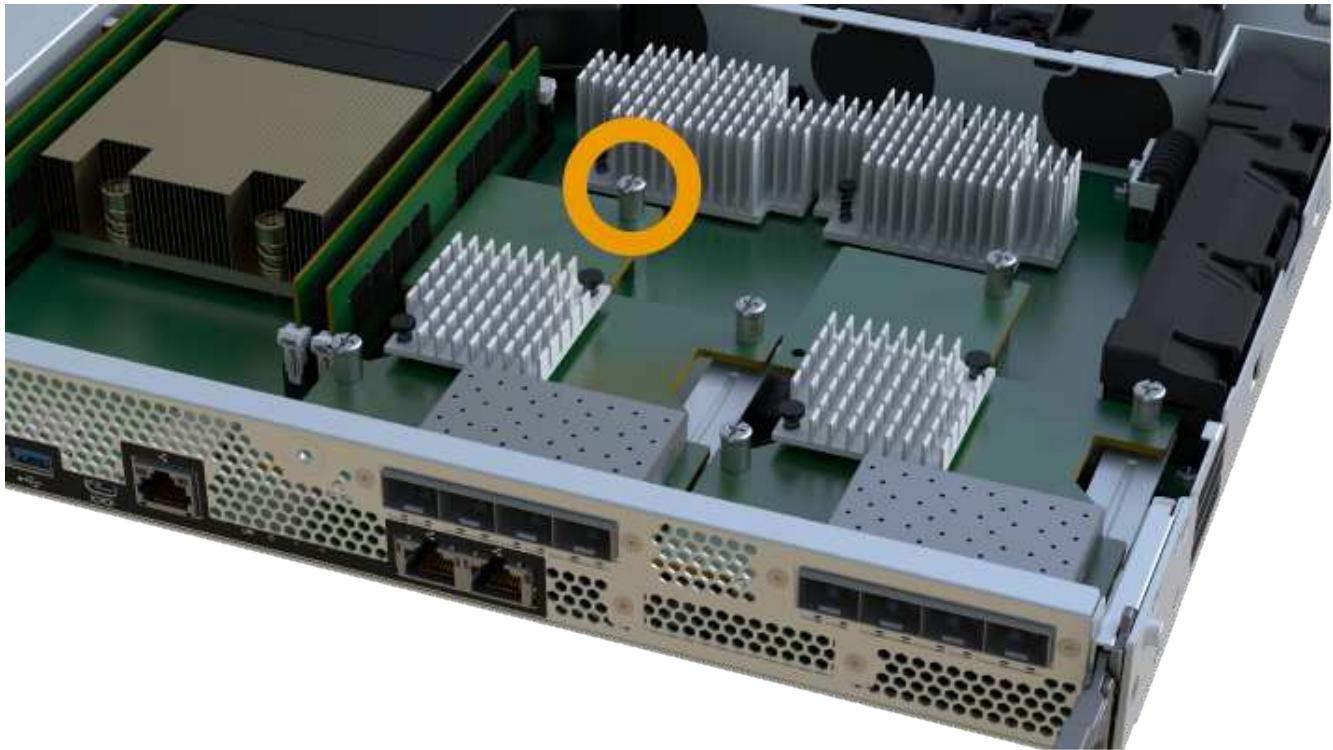
1. Using a Phillips screwdriver, remove the two screws that attach the HIC faceplate to the controller canister.





The image above is an example, the appearance of your HIC may differ.

2. Remove the HIC faceplate.
3. Using your fingers or a Phillips screwdriver, loosen the single thumbscrew that secure the HIC to the controller card.

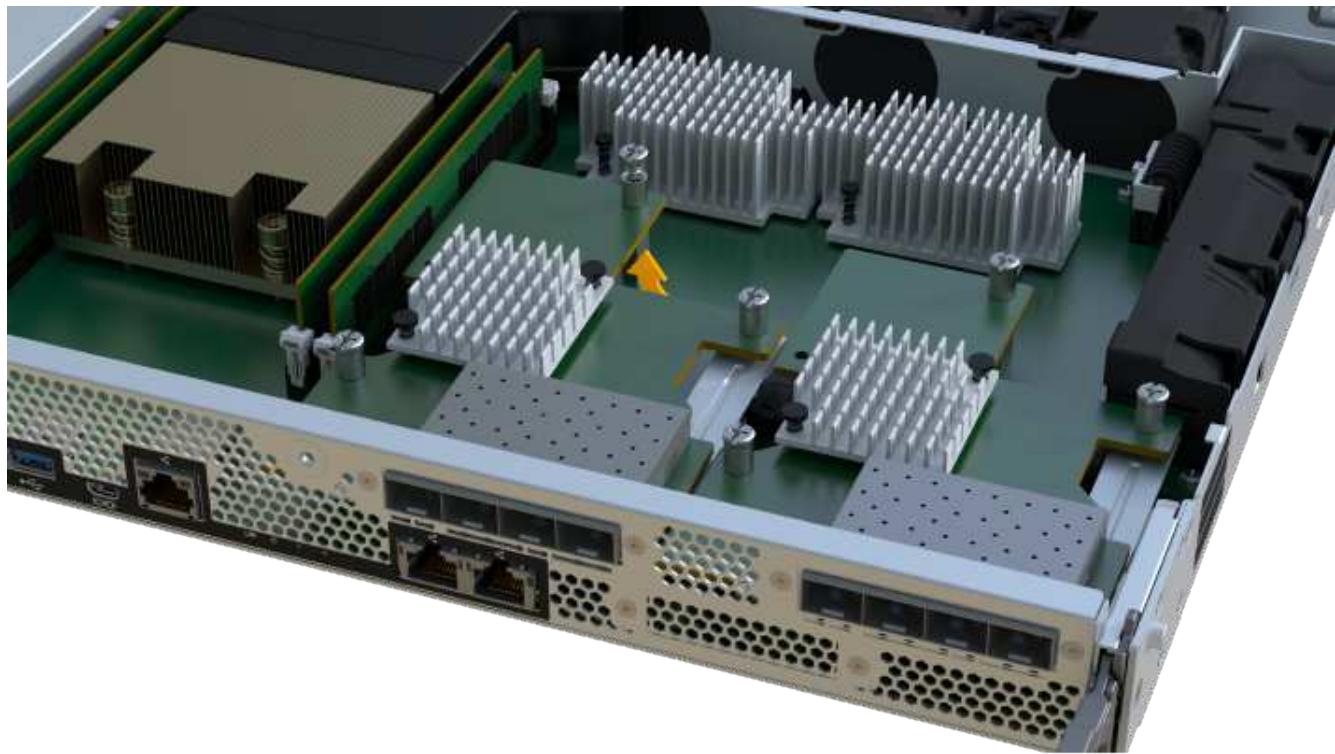


The HIC comes with three screw locations on the top but is secured with only one.

4. Carefully detach the HIC from the controller card by lifting the card up and out of the controller.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



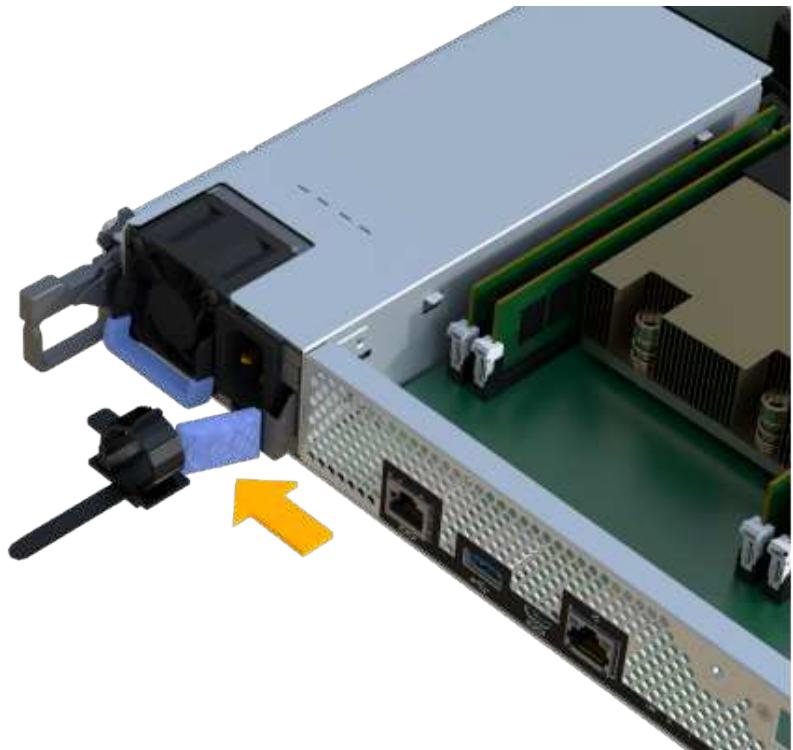
5. Place the HIC on a flat, static-free surface.

Step 2d: Remove power supply

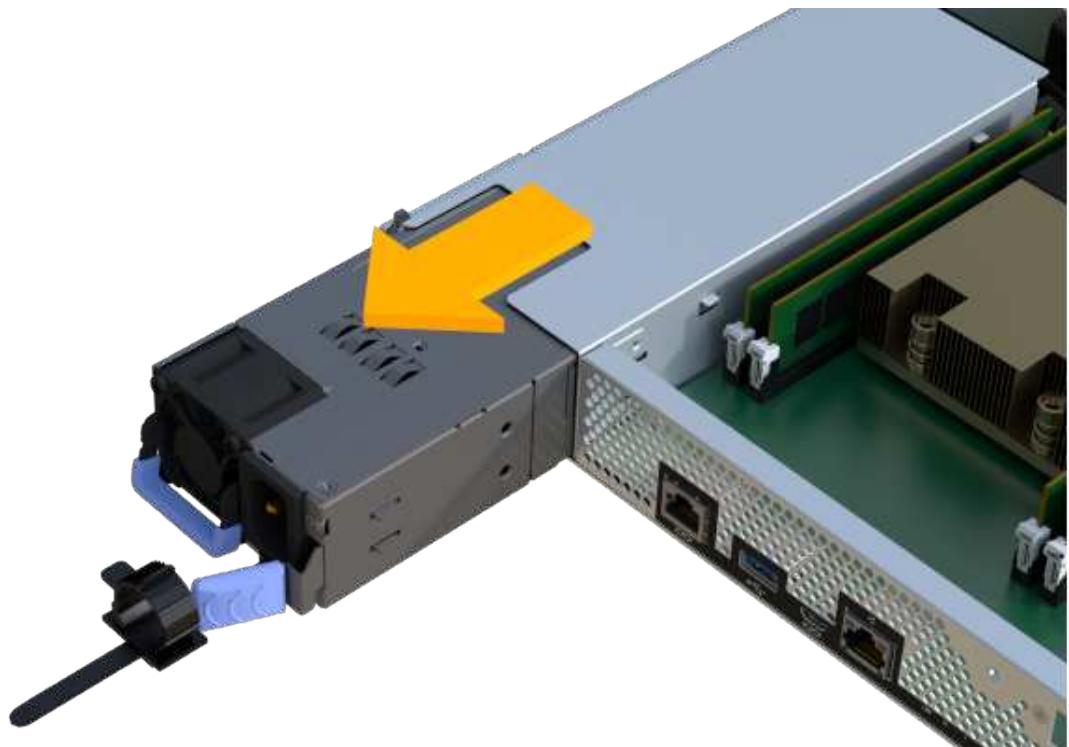
Remove the power supply so you can install it in the new controller.

Steps

1. Disconnect the power cables:
 - a. Open the power cord retainer, and then unplug the power cord from the power supply.
 - b. Unplug the power cord from the power source.
2. Locate the tab to the right of the power supply and press it towards the power supply unit.



3. Locate the handle on the front of the power supply.
4. Use the handle to slide the power supply straight out of the system.



When removing a power supply, always use two hands to support its weight.

Step 2e: Remove DIMMs

Remove the DIMMs so you can install them in the new controller.

Steps

1. Locate the DIMMs on your controller.
2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.

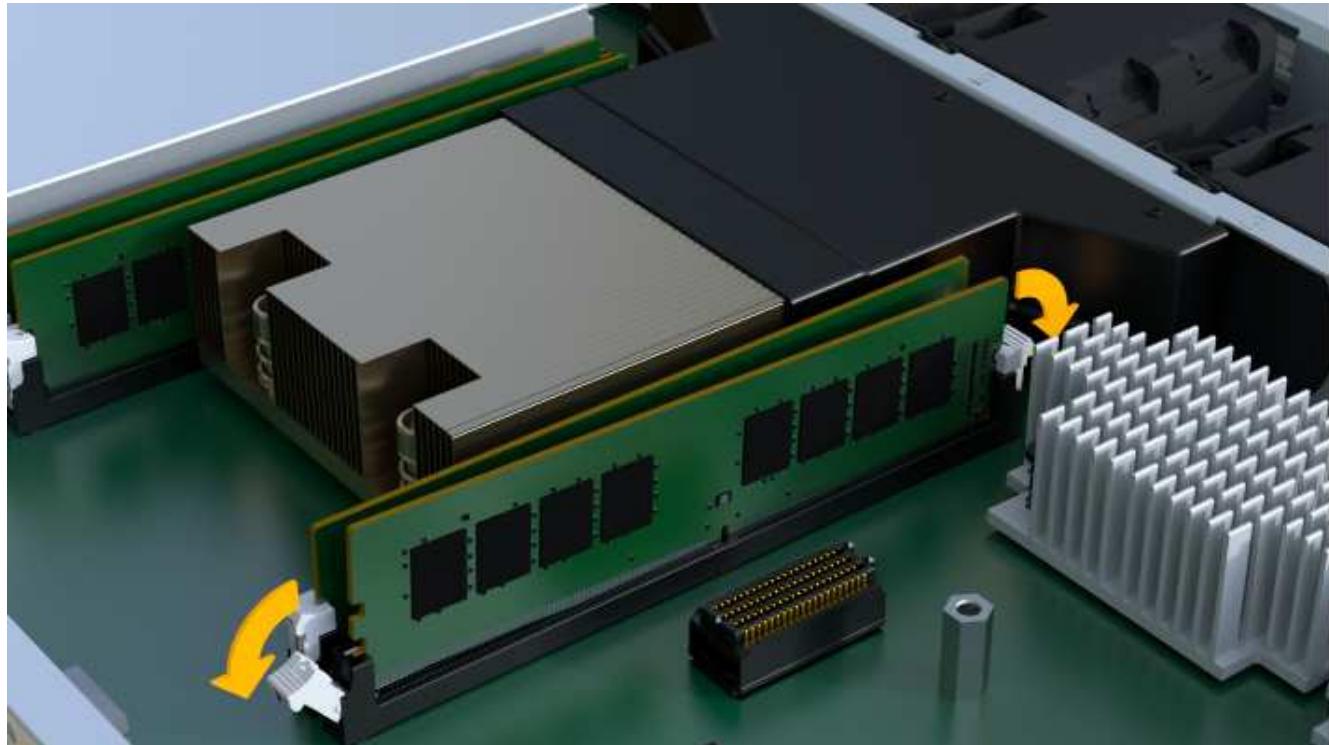


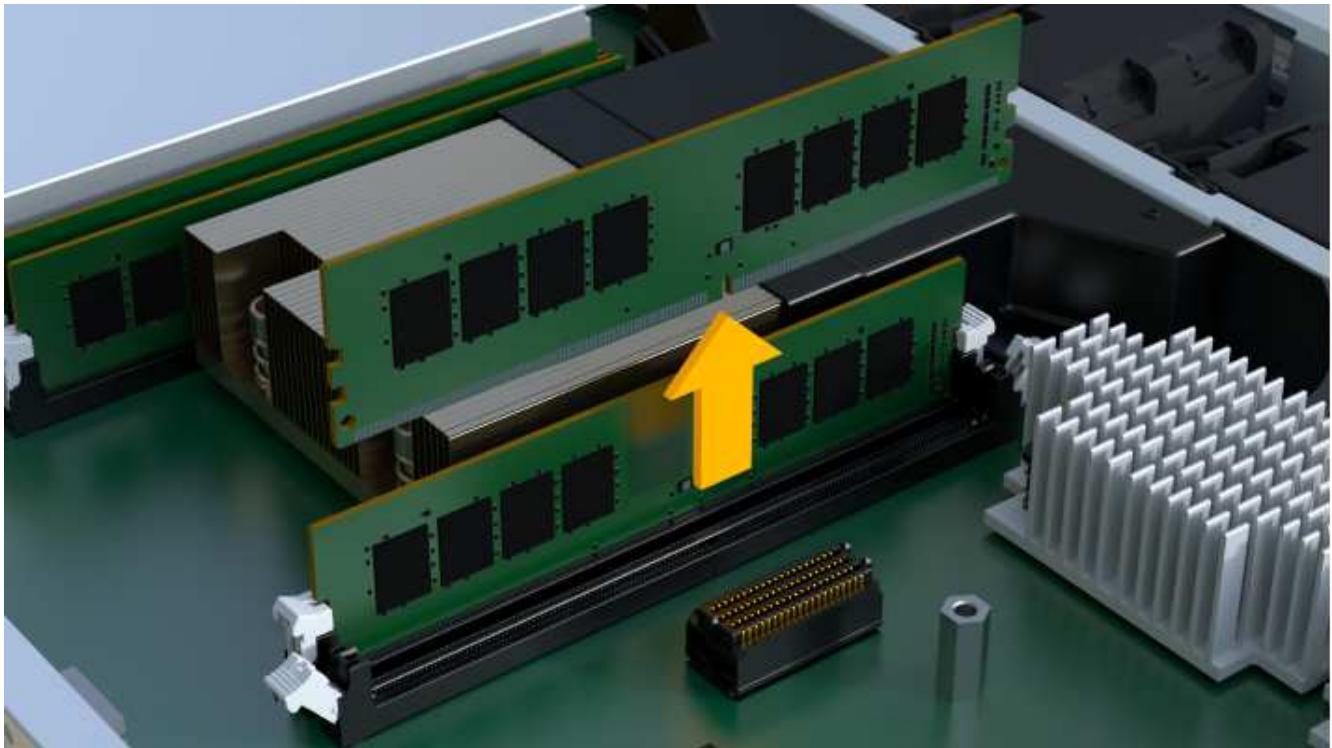
A notch at the bottom of the DIMM helps you align the DIMM during installation.

3. Slowly push apart on the two DIMM ejector tabs on either side of the DIMM to eject the DIMM from its slot, and then slide it out of the slot.



Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.



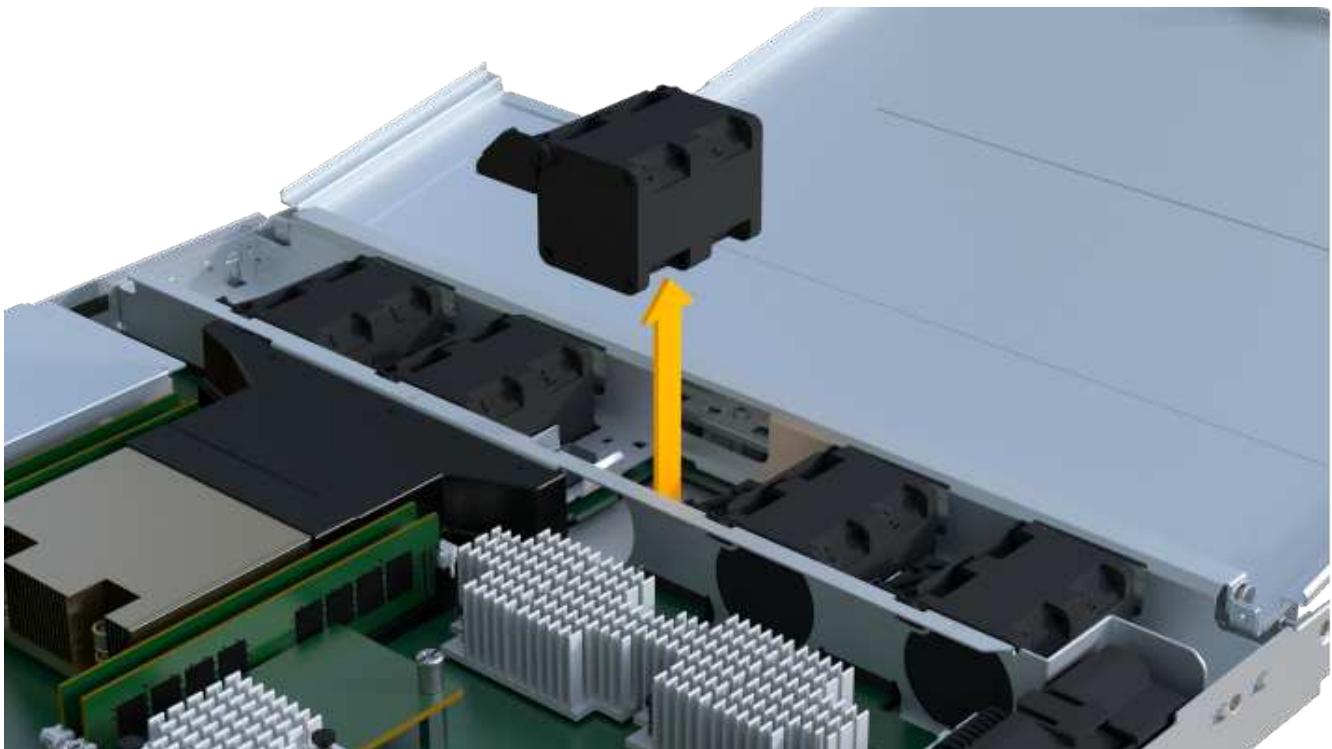


Step 2f: Remove fans

Remove the fans so you can install them in the new controller.

Steps

1. Gently lift the fan from the controller.



2. Repeat until all fans are removed.

Step 3: Install new controller

Install a new controller canister to replace the failed one.

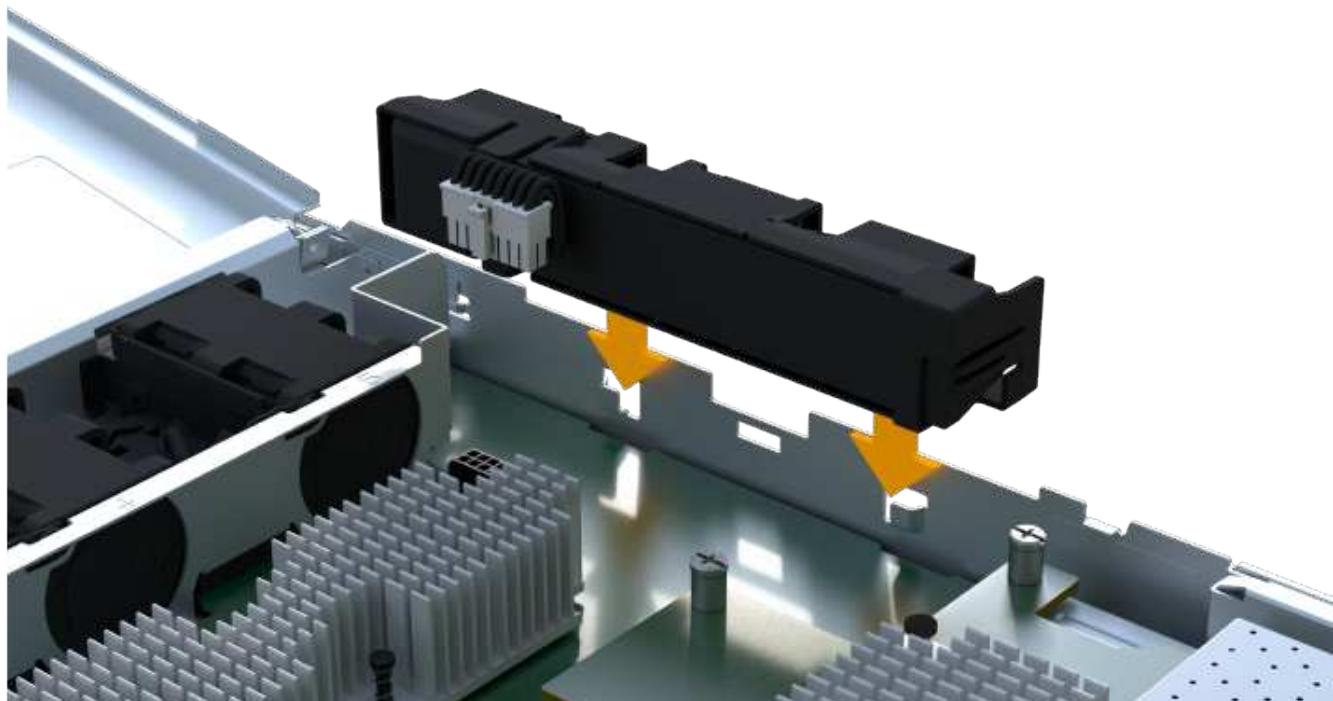
This is a multi-step procedure that requires you to install the following components from the original controller: battery, host interface card, power supply, DIMMs, and fans.

Step 3a: Install battery

Install the battery into the replacement controller canister.

Steps

1. Make sure that you have:
 - The battery from the original controller canister, or a new battery that you ordered.
 - The replacement controller canister.
2. Insert the battery into the controller by lining up the battery casing with the metal latches on the side of the controller.



The battery clicks into place.

3. Plug the battery connector back into the board.

Step 3b: Install the HIC

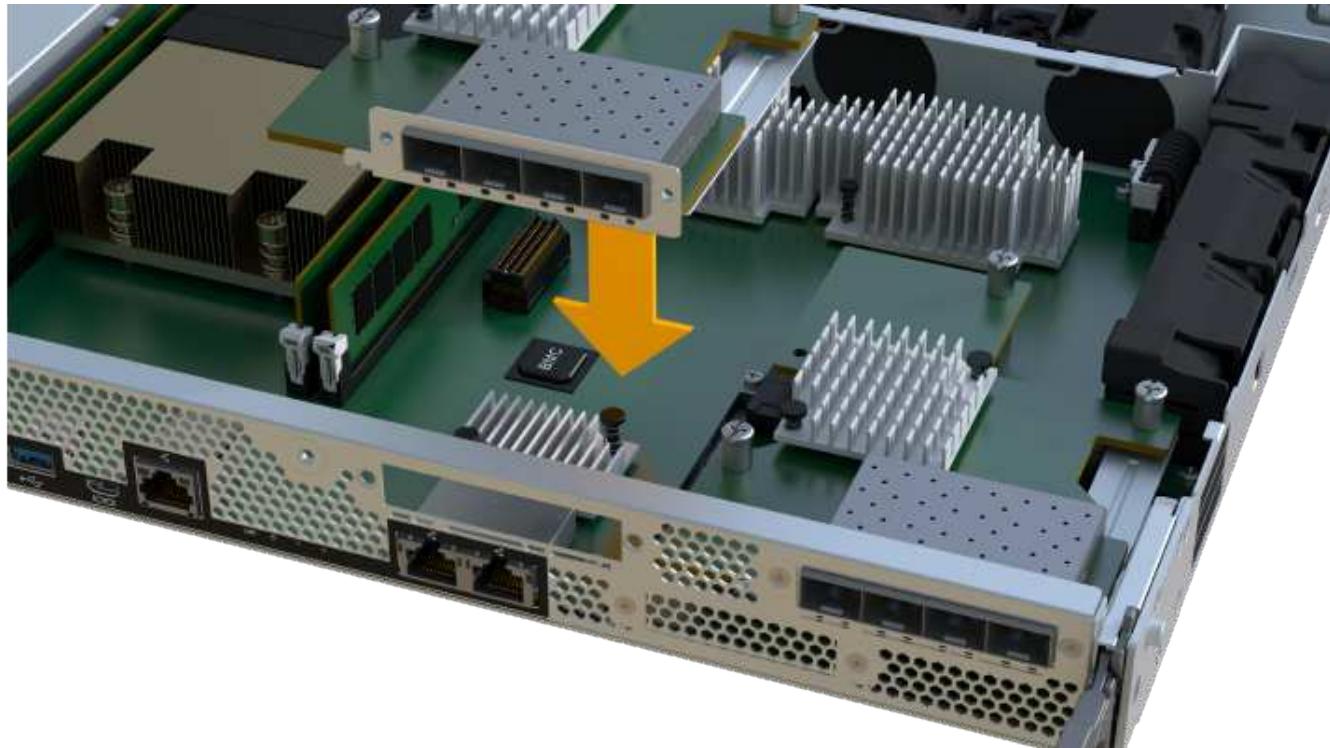
If you removed a HIC from the original controller canister, you must install that HIC in the new controller canister. Otherwise, you can skip this step.

Steps

1. Using a #1 Phillips screwdriver, remove the two screws that attach the blank faceplate to the replacement controller canister, and remove the faceplate.

2. Align the single thumbscrew on the HIC with the corresponding hole on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



The image above is an example; the appearance of your HIC may differ.

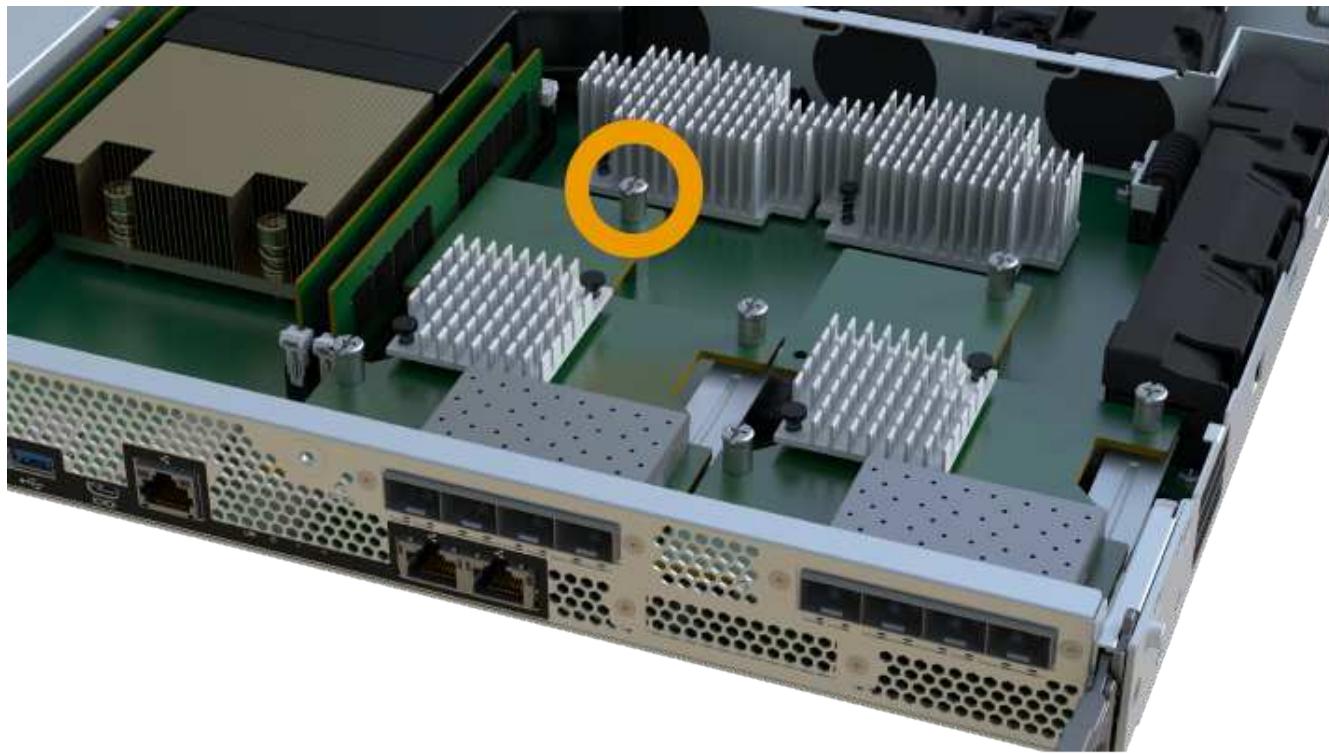
3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage—Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrew.

4. Hand-tighten the HIC thumbscrew.

Do not use a screwdriver, or you might over tighten the screw.



The image above is an example; the appearance of your HIC may differ.

5. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller canister to the new controller canister with the two screws.

Step 3c: Install power supply

Install the power supply into the replacement controller canister.

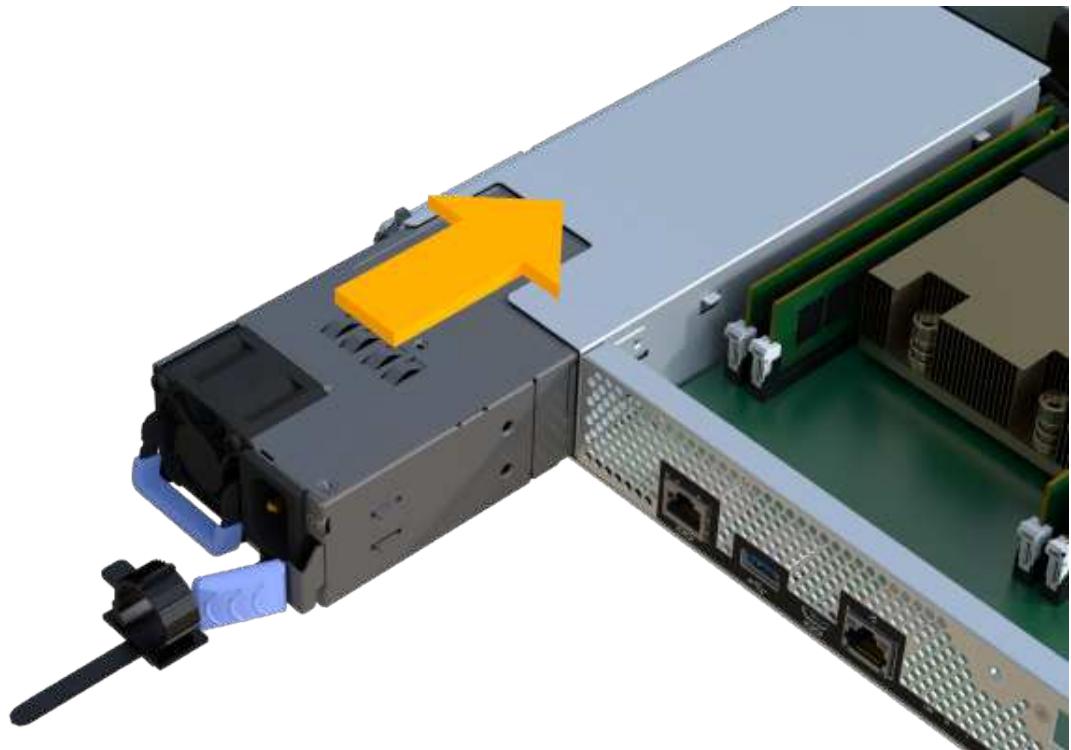
Steps

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system; you can damage the connector.



Step 3d: Install DIMMs

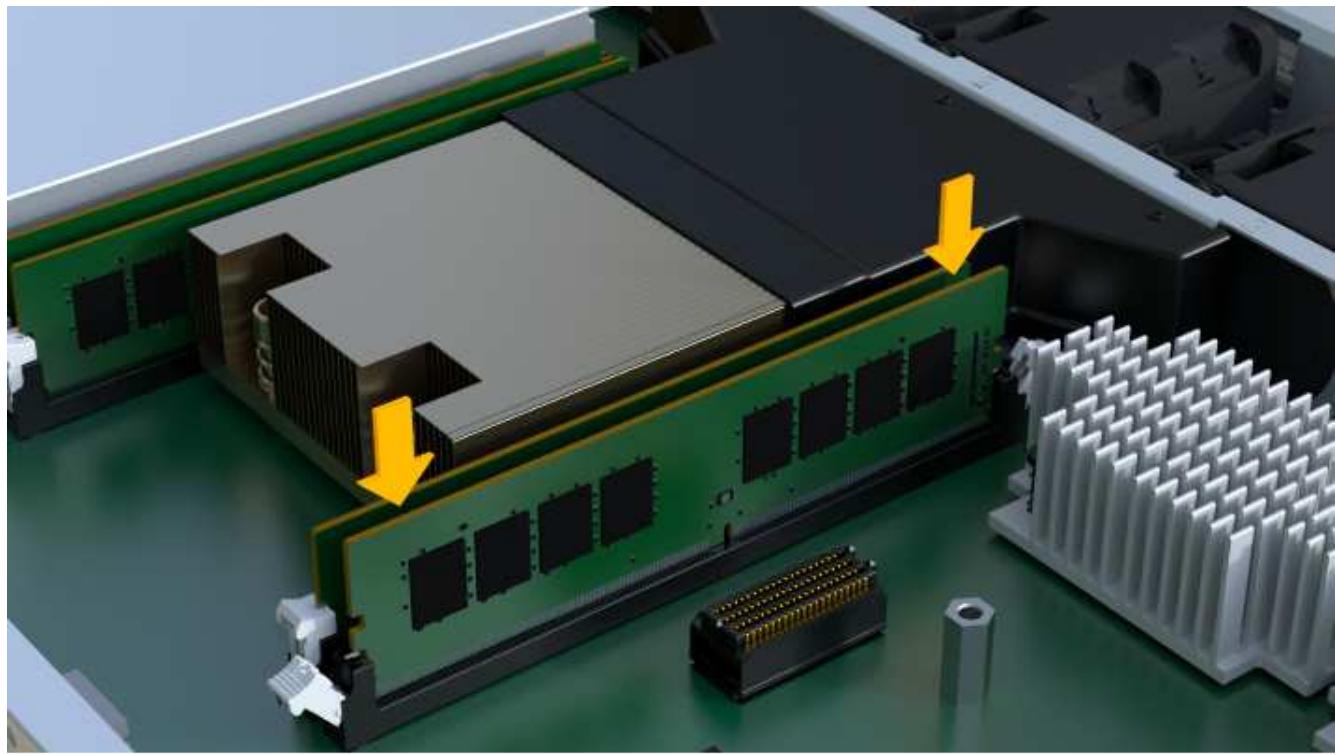
Install the DIMMs into the new controller canister.

Steps

1. Hold the DIMM by the corners, and align it to the slot.

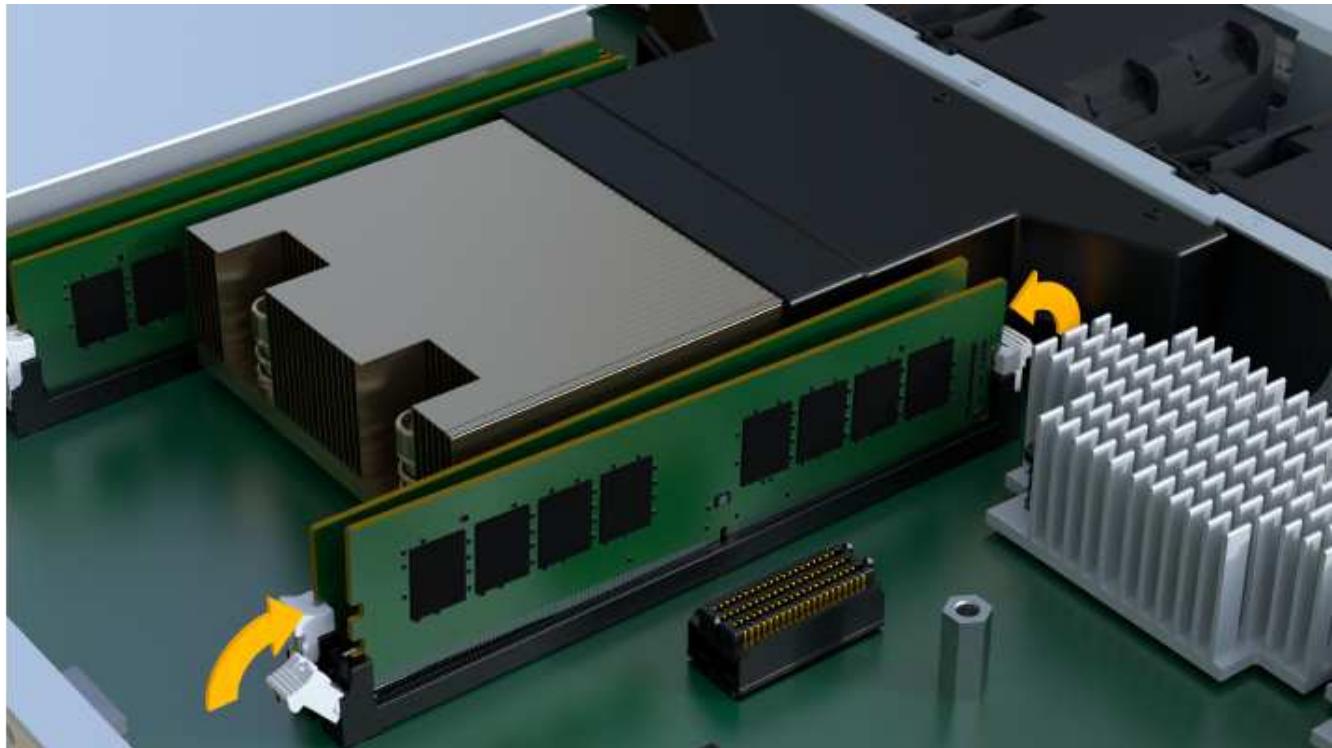
The notch among the pins on the DIMM should line up with the tab in the socket.

2. Insert the DIMM squarely into the slot.



The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

- i Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.
- 3. Push carefully, but firmly, on the top edge of the DIMM until the latches snap into place over the notches at the ends of the DIMM.
- i DIMMs fit tightly. You might need to gently press on one side at a time and secure with each tab individually.

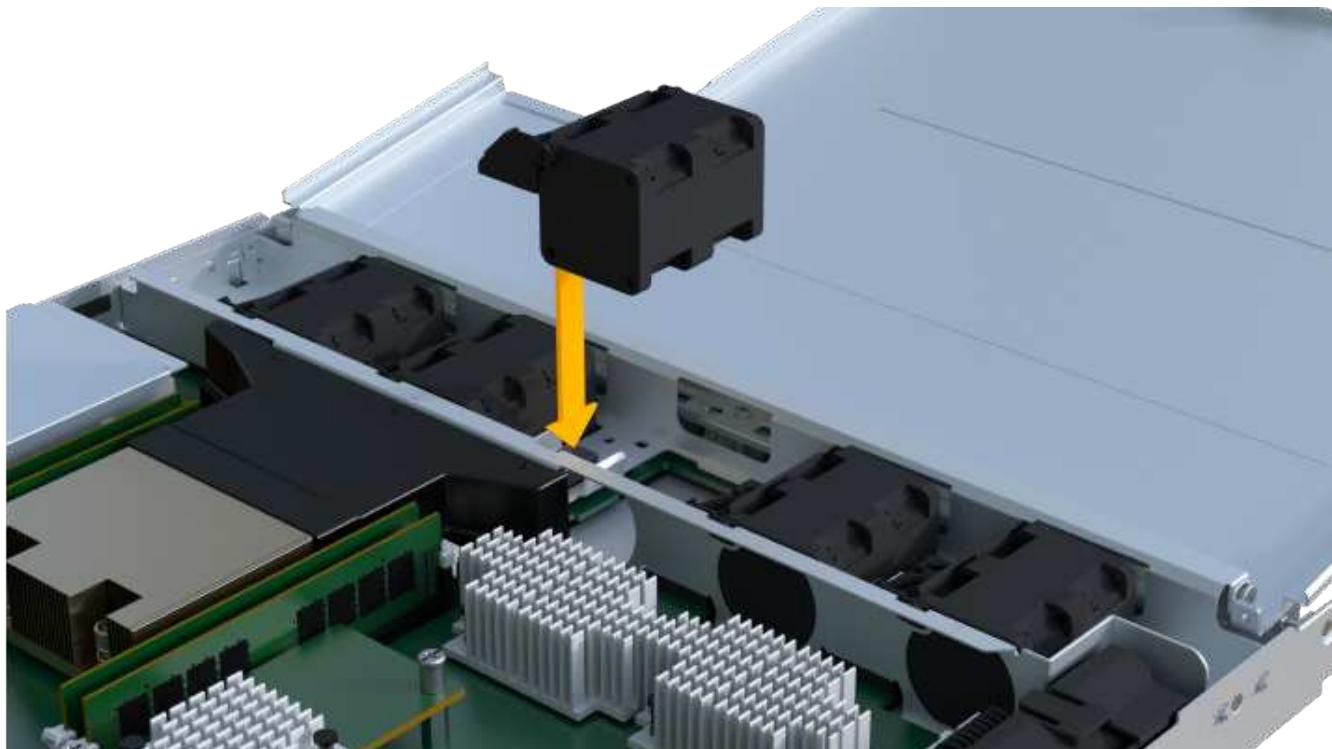


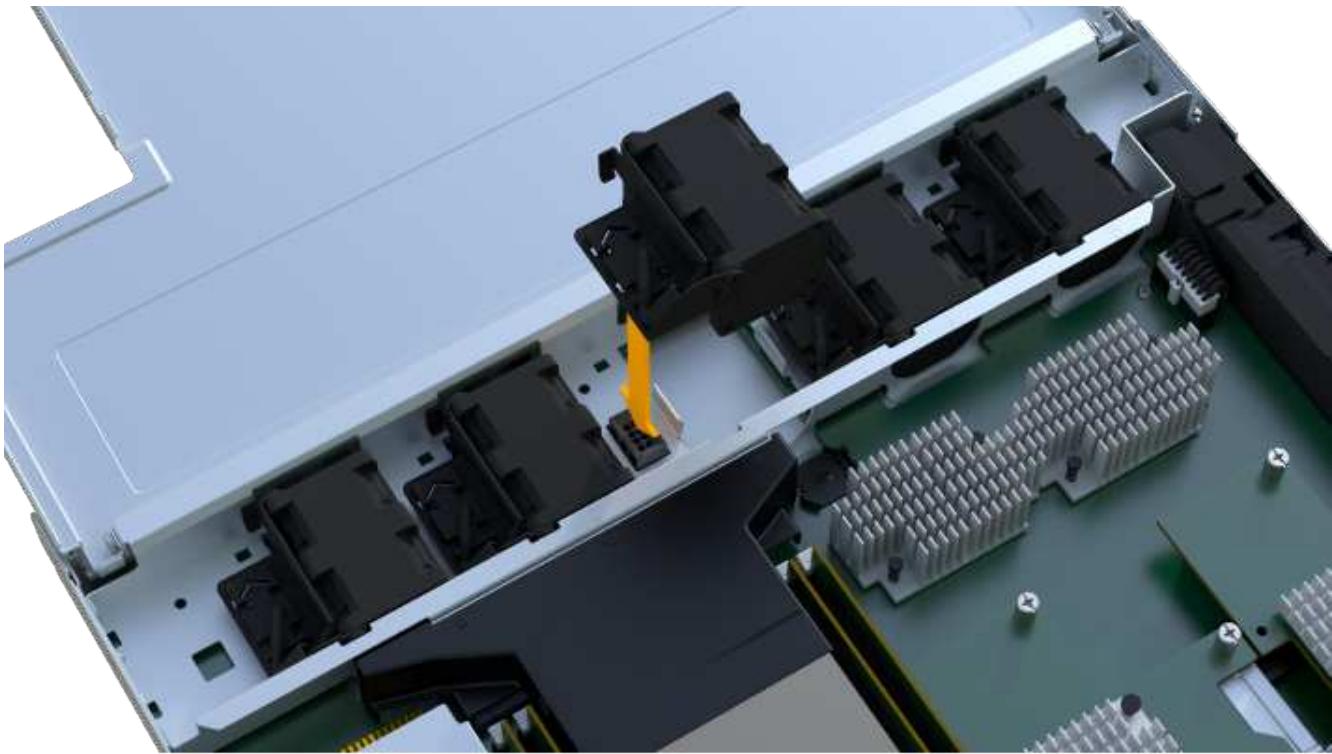
Step 3e: Install fans

Install the fans into the replacement controller canister.

Steps

1. Slide the fan all the way into the replacement controller.





2. Repeat until all fans are installed.

Step 3f: Install new controller canister

Last, install the new controller canister into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



3. Install the SFPs from the original controller in the host ports on the new controller, if they were installed in the original controller, and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

4. If the original controller used DHCP for the IP address, locate the MAC address on the label on the back of the replacement controller. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



If the original controller did not use DHCP for the IP address, the new controller adopts the IP address of the controller you removed.

Step 4: Complete controller replacement

Place the controller online, collect support data, and resume operations.

Steps

1. Place controller online.
 - a. In System Manager, navigate to the Hardware page.
 - b. Select **Show back of controller**.
 - c. Select the replaced controller.
 - d. Select **Place online** from the drop-down list.
2. As the controller boots, check the controller LEDs.

When communication with the other controller is reestablished:

- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.

3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.

- Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
- If volumes are all owned by preferred owner continue to Step 6.
- If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
- If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
- If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.

6. Collect support data for your storage array using SANtricity System Manager.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your controller replacement is complete. You can resume normal operations.

DIMMs

Requirements for replacing an EF300 or EF600 DIMM

Before you replace a DIMM in an EF300 or EF600 storage array, review the requirements and considerations.

You must replace a DIMM when a memory mismatch is present, or you have a failed DIMM. Be sure to verify the configuration of your EF300 or EF600 controller to ensure the correct DIMM size is replaced.



Be aware that the DIMMs in your storage array are fragile; improper handling can lead to damage.

Follow these rules to avoid damaging the DIMMs in your storage array:

- Prevent electrostatic discharge (ESD):
 - Keep the DIMM in the ESD bag until you are ready to install it.
 - Open the ESD bag by hand or cut the top off with a pair of scissors. Do not insert a metal tool or knife into the ESD bag.
 - Keep the ESD bag and any packing materials in case you must return a DIMM later.



Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis.

- Handle DIMMs carefully:
 - Always use two hands when removing, installing, or carrying a DIMM.
 - Never force a DIMM into a shelf, and use gentle, firm pressure to completely engage the latch.
 - Always use approved packaging when shipping DIMMs.
- Avoid magnetic fields. Keep DIMMs away from magnetic devices.

Replace DIMMs in EF300 or EF600

You can replace a DIMM in an EF300 or EF600 array.

About this task

To replace a DIMM, you must verify the cache size of your controller, place the controller offline, remove the controller, remove the DIMMs, and install the new DIMMs in your controller. Then you can bring your controller back online and verify the storage array is working properly.

Before you begin

- Review [Requirements for replacing an EF300 or EF600 DIMM](#).
- Make sure that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.

What you'll need

- A replacement DIMM.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Determine if you need to replace a DIMM

Verify the cache size of your controller before replacing the DIMMs.

Steps

1. Access the Storage Array profile for the controller. From SANtricity System Manager, go to **Support > Support Center**. From the Support Resources page, select **Storage Array Profile**.
2. Scroll down or use the Search field to locate the **Data Cache Module** information.
3. If one of the following is present, note the DIMM's location and continue with remaining procedures in this

section to replace the DIMMs on your controller:

- A failed DIMM, or a DIMM reporting **Data Cache Module** as not optimal.
- A DIMM with a mismatched **Data Cache Module** capacity.

Step 2: Place controller offline

Place the controller offline so you can safely remove and replace the DIMMs.

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a mismatched memory and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which DIMM to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.
 - d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

5. Wait for SANtricity System Manager to update the controller's status to offline.
6. Select **Recheck** from the Recovery Guru, and confirm that the OK to remove field in the Details area displays Yes, indicating that it is safe to remove this component.



Do not begin any other operations until after the status has been updated.

Step 3: Remove controller canister

You remove the failed controller canister so you can replace your DIMMs with new ones.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. Confirm that the Cache Active LED on the back of the controller is off.
5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 4: Remove DIMMs

If there is a memory mismatch present, replace the DIMMs in your controller.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

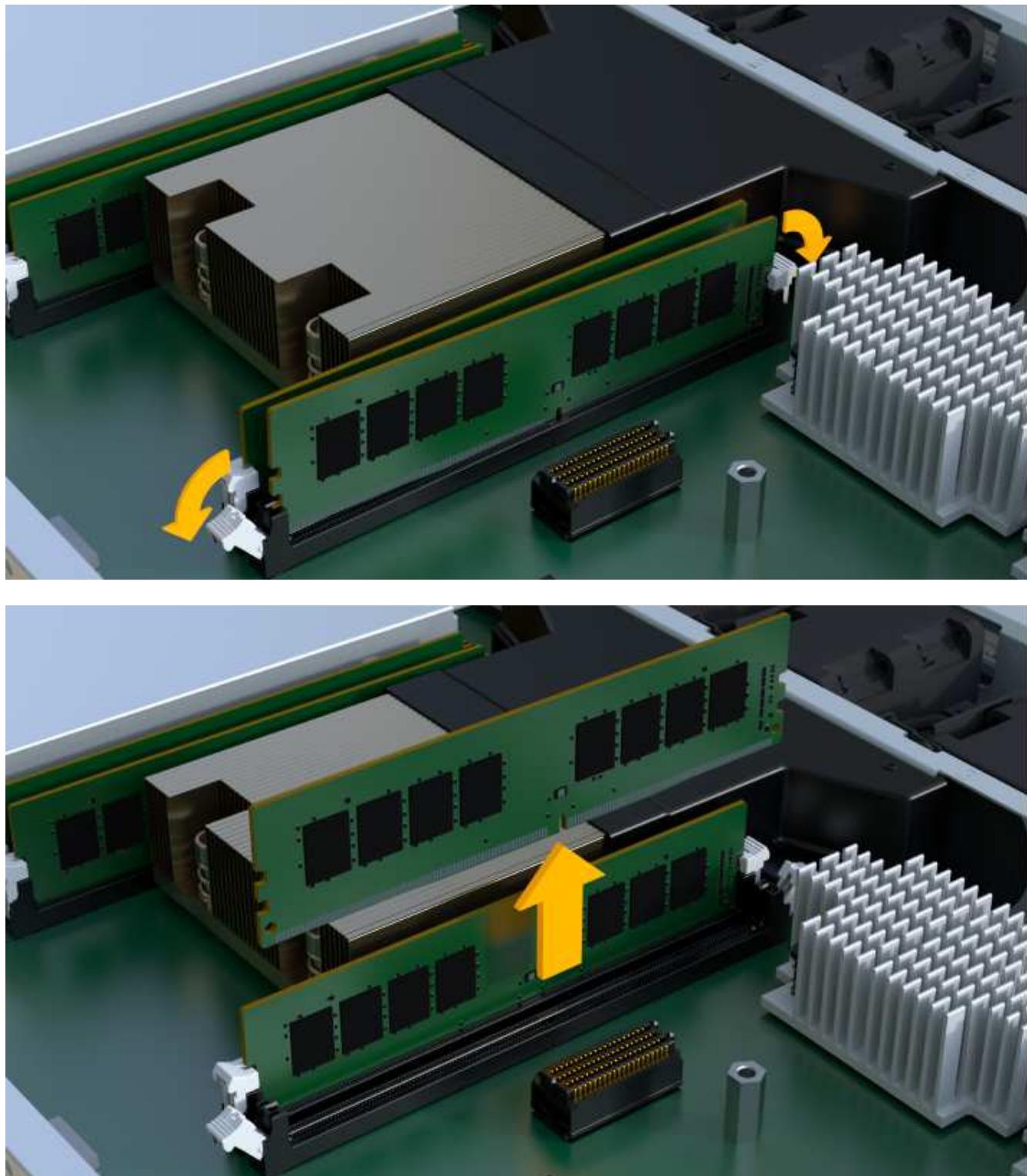
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

3. Locate the DIMMs on your controller.
4. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.



A notch at the bottom of the DIMM helps you align the DIMM during installation.

5. Slowly push apart on the two DIMM ejector tabs on either side of the DIMM to eject the DIMM from its slot, and then slide it out of the slot.



Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

The number and placement of system DIMMs depends on the model of your system.

Step 5: Install new DIMMs

Install a new DIMM to replace the old one.

Steps

1. Hold the DIMM by the corners, and align it to the slot.

The notch among the pins on the DIMM should line up with the tab in the socket.

2. Insert the DIMM squarely into the slot.

The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.

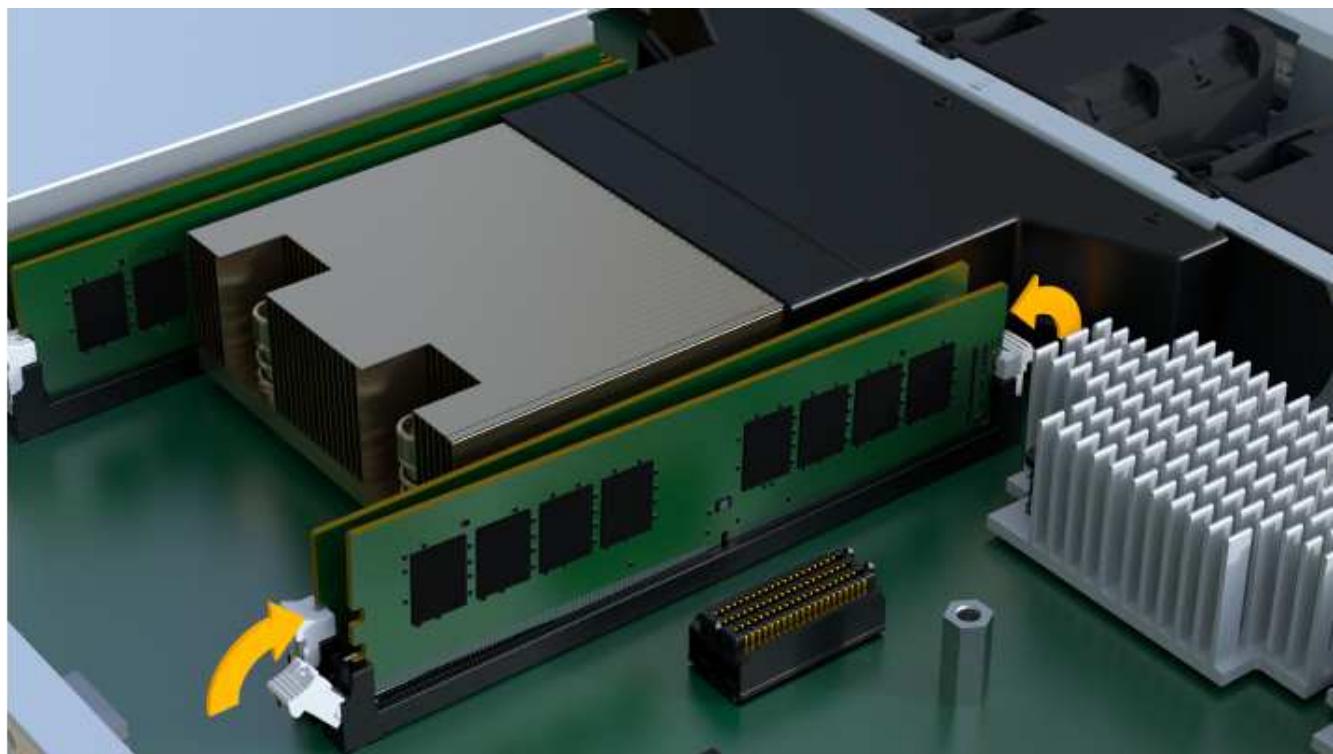


Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

3. Push carefully, but firmly, on the top edge of the DIMM until the latches snap into place over the notches at the ends of the DIMM.



DIMMs fit tightly. You might need to gently press on one side at a time and secure with each tab individually.



Step 6: Reinstall controller canister

After installing the new DIMMs, reinstall the controller canister into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



3. Reconnect all the cables.

Step 7: Complete DIMMs replacement

Place the controller online, collect support data, and resume operations.

Steps

1. Place controller online.
 - a. In System Manager, navigate to the Hardware page.
 - b. Select **Show back of controller**.
 - c. Select the controller with the replaced DIMMs.
 - d. Select **Place online** from the drop-down list.
2. As the controller boots, check the controller LEDs.

When communication with the other controller is reestablished:

- The amber Attention LED remains on.
 - The Host Link LEDs might be on, blinking, or off, depending on the host interface.
3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
 - d. If there is no Recovery Guru present or if following the Recovery Guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your DIMM replacement is complete. You can resume normal operations.

Drives

Requirements for EF300 or EF600 drive replacement

Before replacing a drive in an EF300 or EF600 array, review the requirements and considerations.



Be aware that the drives in your storage array are fragile; improper drive handling is a leading cause of drive failure.

Drive replacement requirements

Follow these rules to avoid damaging the drives in your storage array:

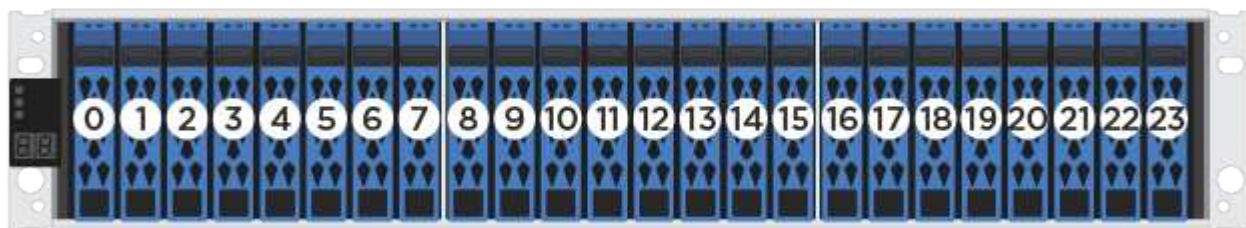
- Prevent electrostatic discharge (ESD):
 - Keep the drive in the ESD bag until you are ready to install it.
 - Open the ESD bag by hand or cut the top off with a pair of scissors. Do not insert a metal tool or knife into the ESD bag.
 - Keep the ESD bag and any packing materials in case you must return a drive later.
 - Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis. If a wrist strap is unavailable, touch an unpainted surface on your storage enclosure chassis before handling the drive.
- Handle drives carefully:
 - Always use two hands when removing, installing, or carrying a drive.
 - Never force a drive into a shelf, and use gentle, firm pressure to completely engage the drive latch.

- Place drives on cushioned surfaces, and never stack drives on top of each other.
 - Do not bump drives against other surfaces.
 - Before removing a drive from a shelf, unlatch the handle and wait 30 seconds for the drive to spin down.
 - Always use approved packaging when shipping drives.
- Avoid magnetic fields. Keep drives away from magnetic devices.

Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry.

Drive staggering in 24-drive controller shelf

Standard 24-drive shelves require drive staggering. The following figure shows how the drives are numbered in each shelf (the shelf's front bezel has been removed).



When inserting fewer than 24 drives into an EF300 or EF600 controller, you must alternate between the two halves of the controller. Beginning with the far left and then moving to the far right, place the drives in one at a time.

The following figure shows how to stagger the drives between the two halves.



Replace drive in an EF300 array

You can replace a drive in an EF300 array.

The EF300 supports SAS expansion with 24-drive and 60-drive shelves. The procedure you follow depends on whether you have a 24-drive shelf or a 60-drive shelf:

- Replace drive in an EF300 (24-drive shelf)
- Replace drive in an EF300 (60-drive shelf)

Replace drive in an EF300 (24-drive shelf)

Follow this procedure to replace a drive in a 24-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O.

Before you begin

- Review drive handling requirements in [Requirements for EF300 or EF600 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static-free work surface.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive (24-drive)

Prepare to replace a drive by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.
 - d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state drive (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within your storage array: From the drive's context menu, select **Turn on locator light**.

The drive's Attention LED (amber) blinks so you can identify which drive to replace.



If you are replacing a drive in a shelf that has a bezel, you must remove the bezel to see the drive LEDs.

Step 2: Remove failed drive (24-drive)

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials.

2. Press the release button on the failed drive.



- For drives in E5724 controller shelves or DE224C drive shelves, the release button is located at the top of the drive.

The cam handle on the drive springs open partially, and the drive releases from the midplane.

3. Open the cam handle, and slide out the drive slightly.

4. Wait 30 seconds.

5. Using both hands, remove the drive from the shelf.

6. Place the drive on an antistatic, cushioned surface away from magnetic fields.

7. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive (24-drive)

You install a new drive to replace the failed one. Install the replacement drive as soon as possible after removing the failed drive. Otherwise, there is a risk that the equipment might overheat.

Steps

1. Open the cam handle.
2. Using two hands, insert the replacement drive into the open bay, firmly pushing until the drive stops.
3. Slowly close the cam handle until the drive is fully seated in the midplane and the handle clicks into place.

The green LED on the drive comes on when the drive is inserted correctly.



Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement (24-drive)

Confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced.

When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.

- Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
- Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
- Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.

2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.

3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.

5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace drive in an EF300 (60-drive shelf)

Follow this procedure to replace a drive in a 60-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O operations.

Before you begin

- Review drive handling requirements in [Requirements for EF300 or EF600 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive (60-drive)

Prepare to replace a drive by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.
 - d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state disk (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within the storage array.
 - a. If the shelf has a bezel, remove it so you can see the LEDs.
 - b. From the drive's context menu, select **Turn on locator light**.

The drive drawer's Attention LED (amber) blinks so you can open the correct drive drawer to identify which drive to replace.



(1) Attention LED

- c. Unlatch the drive drawer by pulling on both levers.

- d. Using the extended levers, carefully pull the drive drawer out until it stops.
- e. Look at the top of the drive drawer to find the Attention LED in front of each drive.



(1) *Attention LED light on for the drive on the top right side*

The drive drawer Attention LEDs are on the left side in front of each drive, with an attention icon on the drive handle just behind the LED.



(1) Attention icon

(2) Attention LED

Step 2: Remove failed drive (60-drive)

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials for the next time you need to send a drive back.

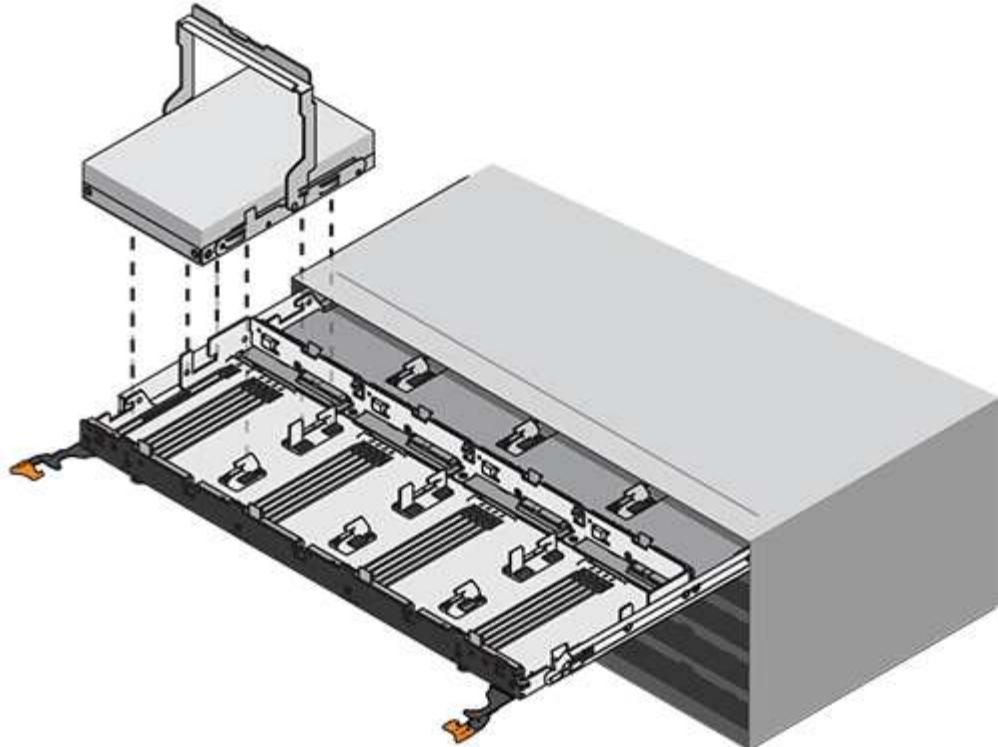
2. Release the drive drawer levers from the center of the appropriate drive drawer by pulling both towards the sides of the drawer.
3. Carefully pull on the extended drive drawer levers to pull out the drive drawer to its full extension without removing it from the enclosure.
4. Gently pull back the orange release latch that is in front of the drive you want to remove.

The cam handle on the drive springs open partially, and the drive is released from the drawer.



(1) *Orange release latch*

5. Open the cam handle, and lift out the drive slightly.
6. Wait 30 seconds.
7. Use the cam handle to lift the drive from the shelf.



8. Place the drive on an antistatic, cushioned surface away from magnetic fields.
9. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive (60-drive)

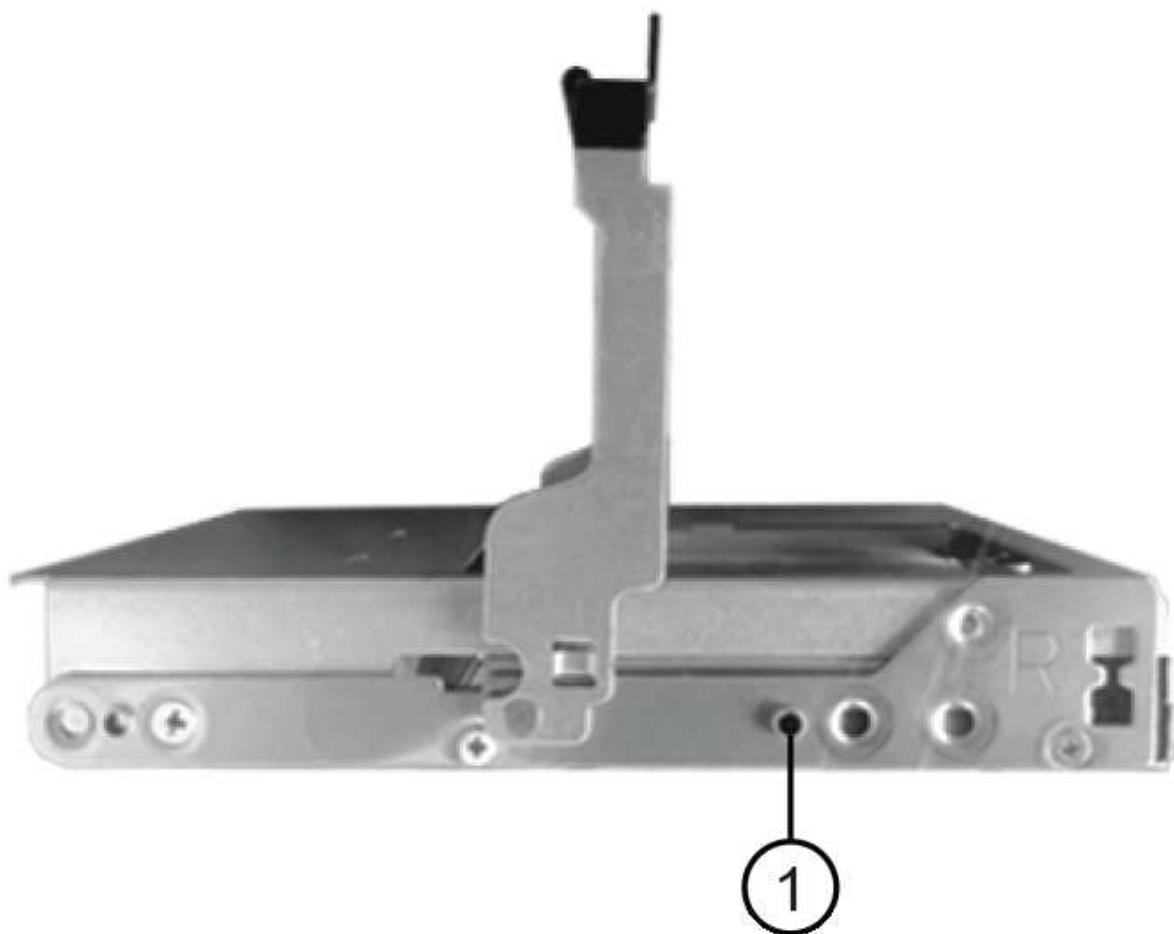
Install a new drive to replace the failed one.



Possible loss of data access — When pushing the drive drawer back into the enclosure, never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

Steps

1. Raise the cam handle on the new drive to vertical.
2. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.



(1) Raised button on the right side of the drive carrier

3. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.
4. Carefully push the drive drawer back into the enclosure. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.
5. Close the drive drawer by pushing both levers towards the center.

The green Activity LED for the replaced drive on the front of the drive drawer comes on when the drive is inserted correctly.

Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement (60-drive)

Confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced. (When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.)
 - Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
 - Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
 - Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.
2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.
5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace drive in an EF600 array

You can replace a drive in an EF600 array.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O.

Before you begin

- Review [Requirements for EF300 or EF600 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static-free work surface.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive

Prepare for drive replacement by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.
 - d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state disk (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within your storage array: From the drive's context menu, select **Turn on locator light**.

The drive's Attention LED (amber) blinks so you can identify which drive to replace.



If you are replacing a drive in a shelf that has a bezel, you must remove the bezel to see the drive LEDs.

Step 2: Remove drive

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials.

2. Press the black release button on the failed drive.

The latch on the drive springs partially opens, and then the drive releases from the controller.

3. Open the cam handle, and slide out the drive slightly.
4. Wait 30 seconds.
5. Using both hands, remove the drive from the shelf.



6. Place the drive on an antistatic, cushioned surface away from magnetic fields.
7. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive

Install a new drive to replace the failed one. You should install the replacement drive as soon as possible after removing the failed drive.

Steps

1. Open the cam handle.
2. Using two hands, insert the replacement drive into the open bay, firmly pushing until the drive stops.
3. Slowly close the cam handle until the drive is fully seated in the midplane and the handle clicks into place.

The green LED on the drive comes on when the drive is inserted correctly.



Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement

Complete the drive replacement to confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced. (When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.)
 - Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
 - Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
 - Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.

2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.
5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Fans

Requirements for EF300 or EF600 fan replacement

Before replacing a failed fan in an EF300 or EF600 array, review the following requirements.

- You have a replacement fan that is supported for your controller shelf or drive shelf model.
- You have an ESD wristband, or you have taken other antistatic precautions.



If the Recovery Guru indicates that it is not OK to remove the fan, contact technical support.

Replace an EF300 or EF600 fan

You can replace a fan in an EF300 or EF600 array.

About this task

Each EF300 and EF600 controller shelf or drive shelf includes five fans. If a fan fails, you must replace it as soon as possible to ensure that the shelf has adequate cooling.

What you'll need

- A replacement fan.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To

open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller offline

Place the controller canister offline so you can safely replace the failed fan.

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a fan and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which fan to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.
 - d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

5. Wait for SANtricity System Manager to update the controller's status to offline.
6. Select **Recheck** from the Recovery Guru, and confirm that the **OK to remove** field in the Details area displays Yes, indicating that it is safe to remove this component.



Do not begin any other operations until after the status has been updated.

Step 2: Remove controller canister

Remove the controller canister so you can replace the failed fan with a new one.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.

3. Disconnect all the cables from the controller canister.



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

4. Confirm that the Cache Active LED on the back of the controller is off.
5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 3: Remove failed fan

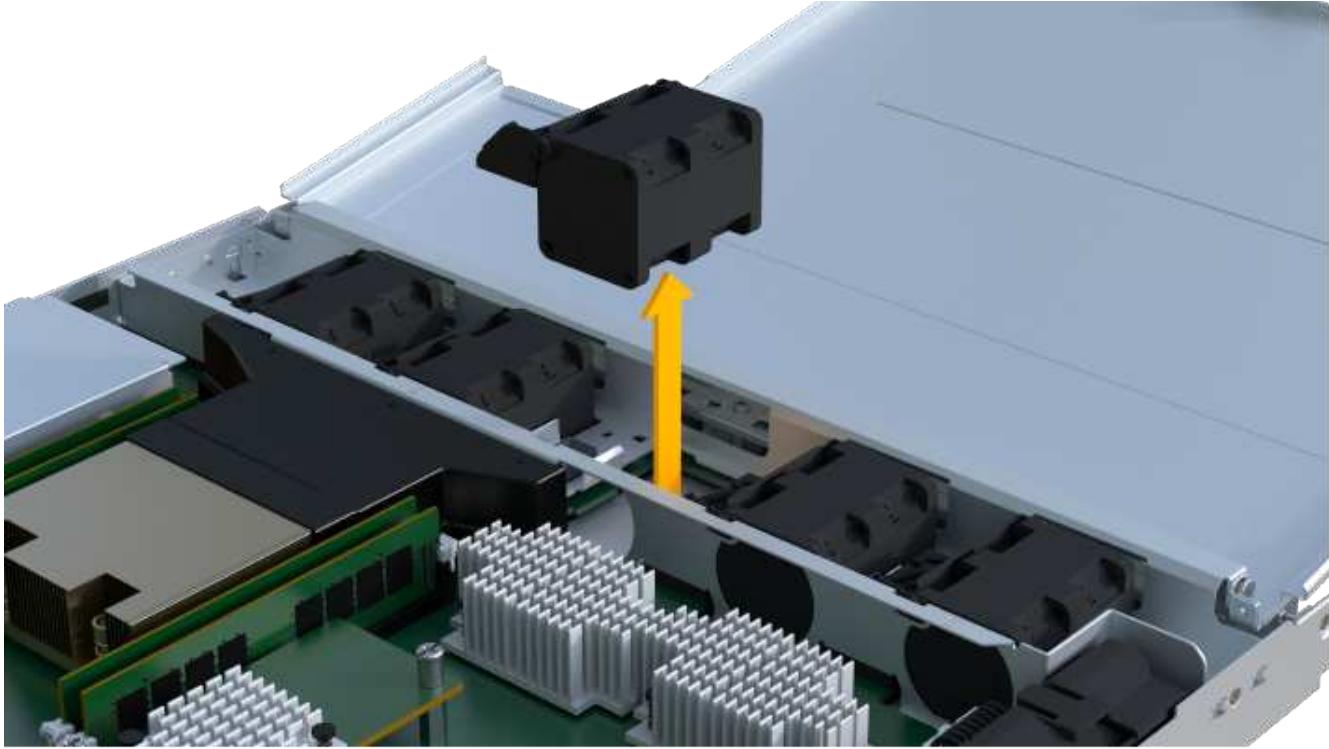
You remove a failed fan so you can replace it with a new one.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

3. Gently lift the failed fan from the controller.

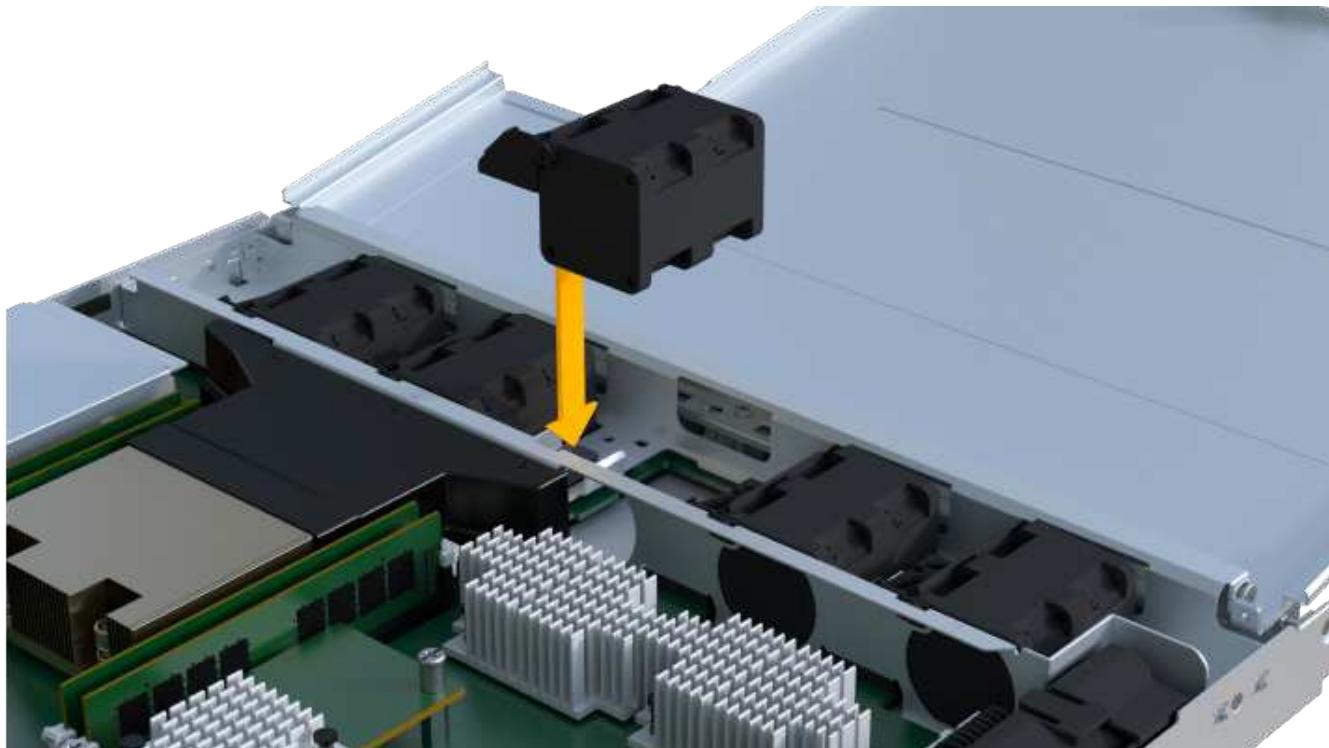


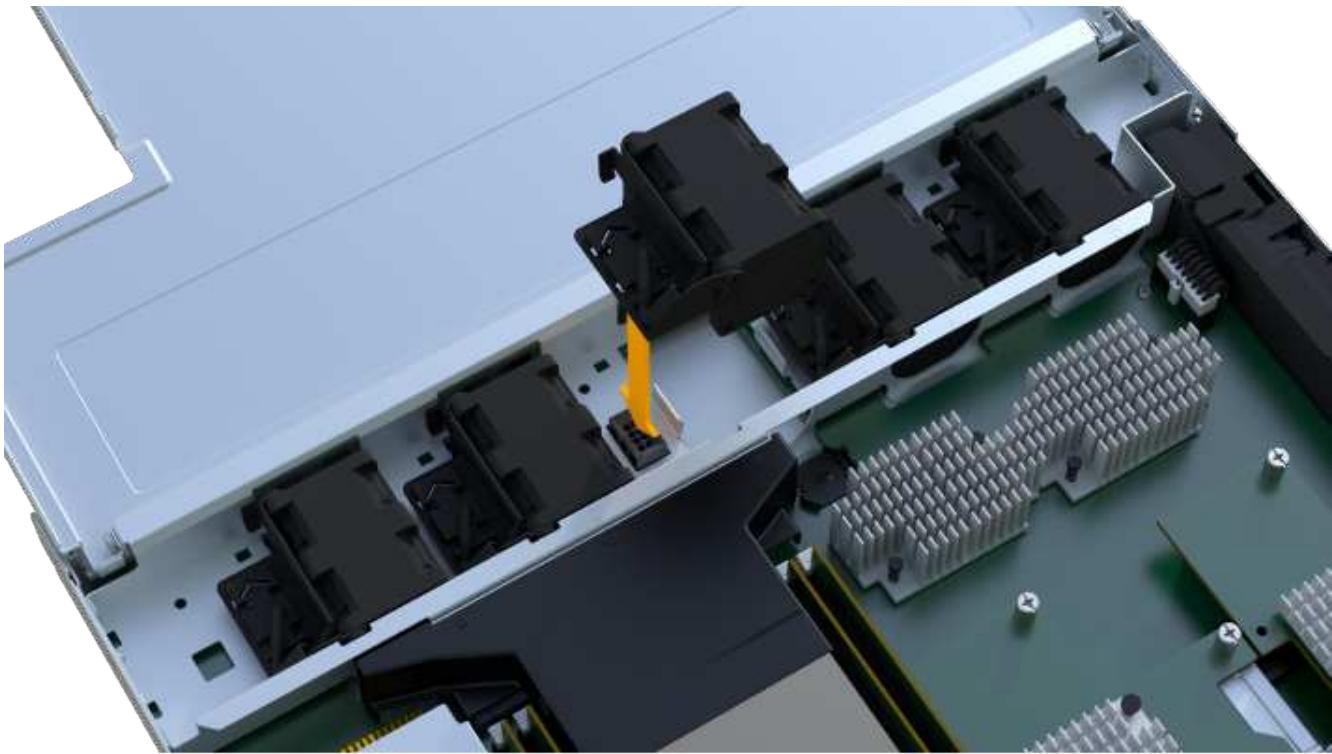
Step 4: Install new fan

Install a new fan to replace the failed one.

Steps

1. Slide the replacement fan all the way into the shelf.





Step 5: Reinstall controller canister

After installing the new fan, reinstall the controller canister into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



Step 6: Complete fan replacement

Place the controller online, collect support data, and resume operations.

1. Place controller online.
 - a. In System Manager, navigate to the hardware page.
 - b. Select **Show back of controller**.
 - c. Select the controller with the replaced fan.
 - d. Select **Place online** from the drop-down list.
2. As the controller boots, check the controller LEDs.

When communication with the other controller is reestablished:

- The amber Attention LED remains on.
 - The Host Link LEDs might be on, blinking, or off, depending on the host interface.
3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
 - d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
 - e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your fan replacement is complete. You can resume normal operations.

Host interface cards

Requirements for EF300 or EF600 HIC upgrades

Before upgrading or replacing a host interface card (HIC) in a EF300 or EF600 array, review the following requirements.

- You have scheduled a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure. Because both controllers must have the same HIC configuration when they are powered on, the power must be off when you change HIC configuration. The presence of mismatched HICs causes the controller with the replacement HIC to lock down when you bring it online.
- You have all cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- You have an ESD wristband, or you have taken other antistatic precautions.
- You have a #1 Phillips screwdriver.
- You have labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)
- Some HIC replacements or upgrades might require a host port protocol conversion. Follow the instructions in the [Change host protocol for an EF300 or EF600](#) for this requirement.

- EF300 controllers must have HIC port 2 filled with a HIC for host connectivity.

Add host interface card (HIC) to an EF600

You can add a host interface card (HIC) to an EF600 controller. This addition increases the number of host ports in your storage array.

About this task

This procedure applies only to EF600 controller shelves, and involves the following steps:

- You must power off the storage array, install the HIC, and reapply power.
- You must repeat all steps to remove the second controller, install the HICs for the second controller, and reinstall the second controller before reapplying power to the controller shelf.

Before you begin

- Review [Requirements for EF300 or EF600 HIC upgrades](#).
- Schedule a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure. Because both controllers must have the same HIC configuration when they are powered on, the power must be off when you install HICs.

What you'll need

- Two HICs that are compatible with your controllers.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- A #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

 **Possible loss of data access** — Never install a HIC in an EF600 controller canister if that HIC was designed for another E-Series controller. In addition, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Step 1: Place controller shelf offline

Place the controller shelf offline so you can safely add the HICs.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

3. 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.



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, the host application might lose access to the data because the storage is not accessible.

4. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

5. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
6. Power down the controller shelf.
 - a. Label and then unplug both power cables from controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can add the new HIC.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. If the HIC ports use SFP+ transceivers, remove them.

Depending on what type of HIC you are adding to, you might be able to reuse these SFPs.

5. Confirm that the Cache Active LED on the back of the controller is off.

6. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



7. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



8. Place the controller canister on a flat, static-free surface.

Step 3: Add the new HIC

Install the HIC to increase the number of host ports in your storage array.



Possible loss of data access — Never install a HIC in an EF600 controller canister if that HIC was designed for another E-Series controller. In addition, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

3. Using a #1 Phillips screwdriver, remove the two screws that attach the HIC faceplate to the controller canister, and remove the faceplate.
4. Align the single thumbscrew on the HIC with the corresponding hole on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

5. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrew.



The image above is an example of an EF600, the appearance of your HIC may differ.

6. Hand-tighten the HIC thumbscrew.

Do not use a screwdriver, or you might over tighten the screws.

7. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller canister to the new controller canister with the two screws.

Step 4: Reinstall the controller canister

Reinstall the controller canister into the controller shelf after installing the HIC.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



3. If removed, install the SFPs into the new HIC and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

Step 5: Complete HIC addition

Place the controller online, collect support data, and resume operations.

Steps

1. Place controller online.
 - a. Plug in power cables.

2. As the controller boots, check the controller LEDs.
 - The amber Attention LED remains on.
 - The Host Link LEDs might be on, blinking, or off, depending on the host interface.
3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.
5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
 - d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
 - e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

The process of adding a host interface card in your storage array is complete. You can resume normal operations.

Upgrade EF300 or EF600 host interface card (HIC)

You can upgrade a host interface card (HIC) to increase the number of host ports or to change host protocols.

About this task

- When you upgrade HICs, you must power off the storage array, upgrade the HICs, and reapply power.
- When upgrading HICs in an EF300 or EF600 controller repeat all steps to remove the second controller, upgrade the second controller's HICs, and reinstall the second controller before reapplying power to the

controller shelf.

Before you begin

- Review [Requirements for EF300 or EF600 HIC upgrades](#).
- Schedule a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure. Because both controllers must have the same HIC configuration when they are powered on, the power must be off when you install HICs.

What you'll need

- Two HICs that are compatible with your controllers.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- Labels to identify each cable that is connected to the controller canister.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

 **Possible loss of data access** — Never install a HIC in an EF300 or EF600 controller canister if that HIC was designed for another E-Series controller. In addition, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Step 1: Place controller shelf offline

Place the controller shelf offline so you can safely upgrade the HICs.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

3. 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.



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, the host application might lose access to the data because the storage is not accessible.

4. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

5. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
6. Power down the controller shelf.
 - a. Label and then unplug both power cables from controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can upgrade the new HIC.

Steps

1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



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

3. If the HIC ports use SFP+ transceivers, remove them.

Depending on what type of HIC you are upgrading to, you might be able to reuse these SFPs.

4. Confirm that the Cache Active LED on the back of the controller is off.
5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 3: Remove the HIC

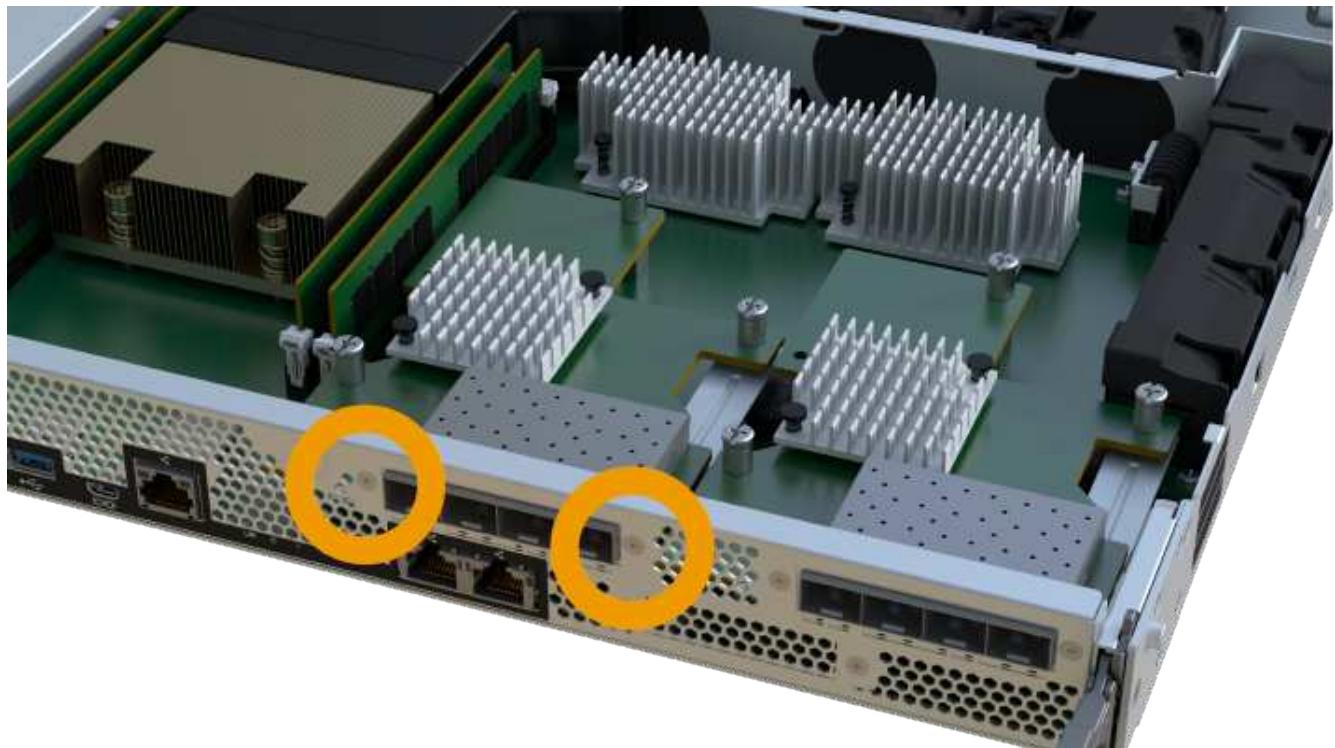
Remove the original HIC so you can replace it with an upgraded one.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

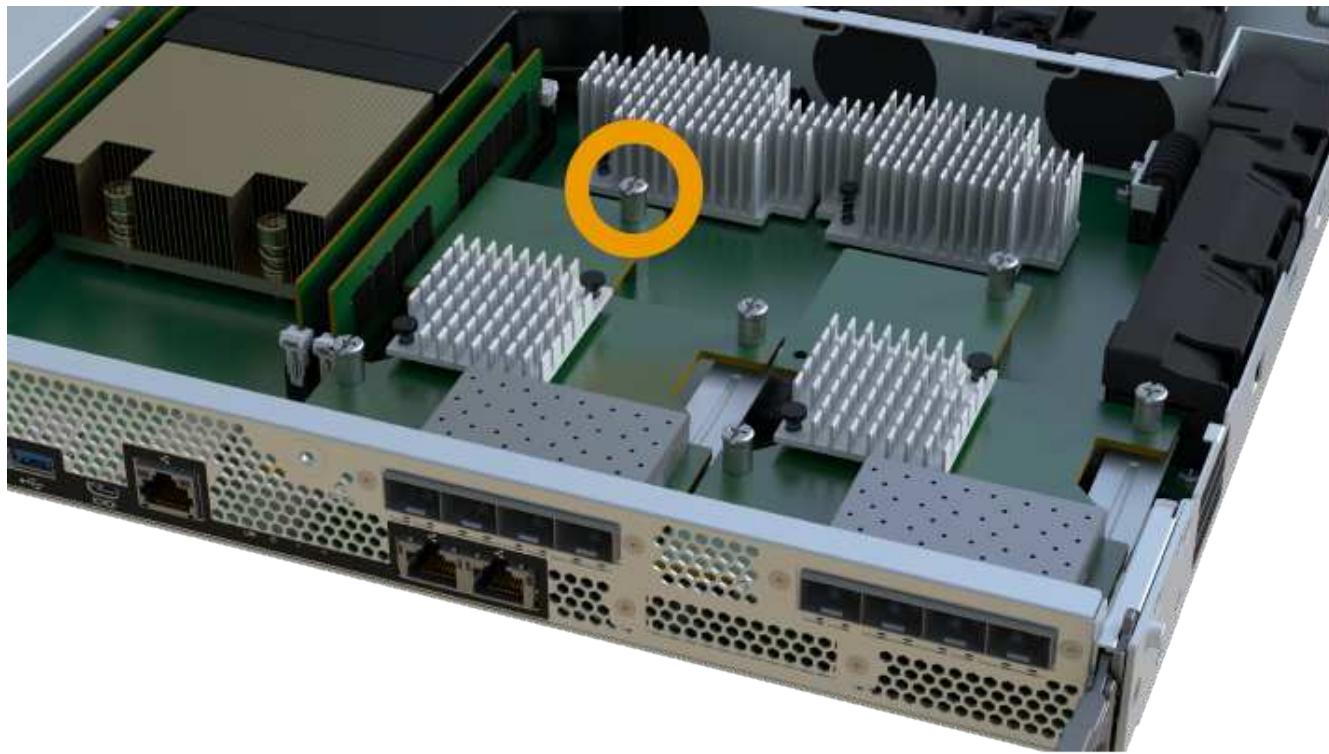
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

3. Using a Phillips screwdriver, remove the two screws that attach the HIC faceplate to the controller canister.



The image above is an example, the appearance of your HIC may differ.

4. Remove the HIC faceplate.
5. Using your fingers or a Phillips screwdriver, loosen the single thumbscrew that secure the HIC to the controller card.



The HIC comes with three screw locations on the top, but is secured with only one.

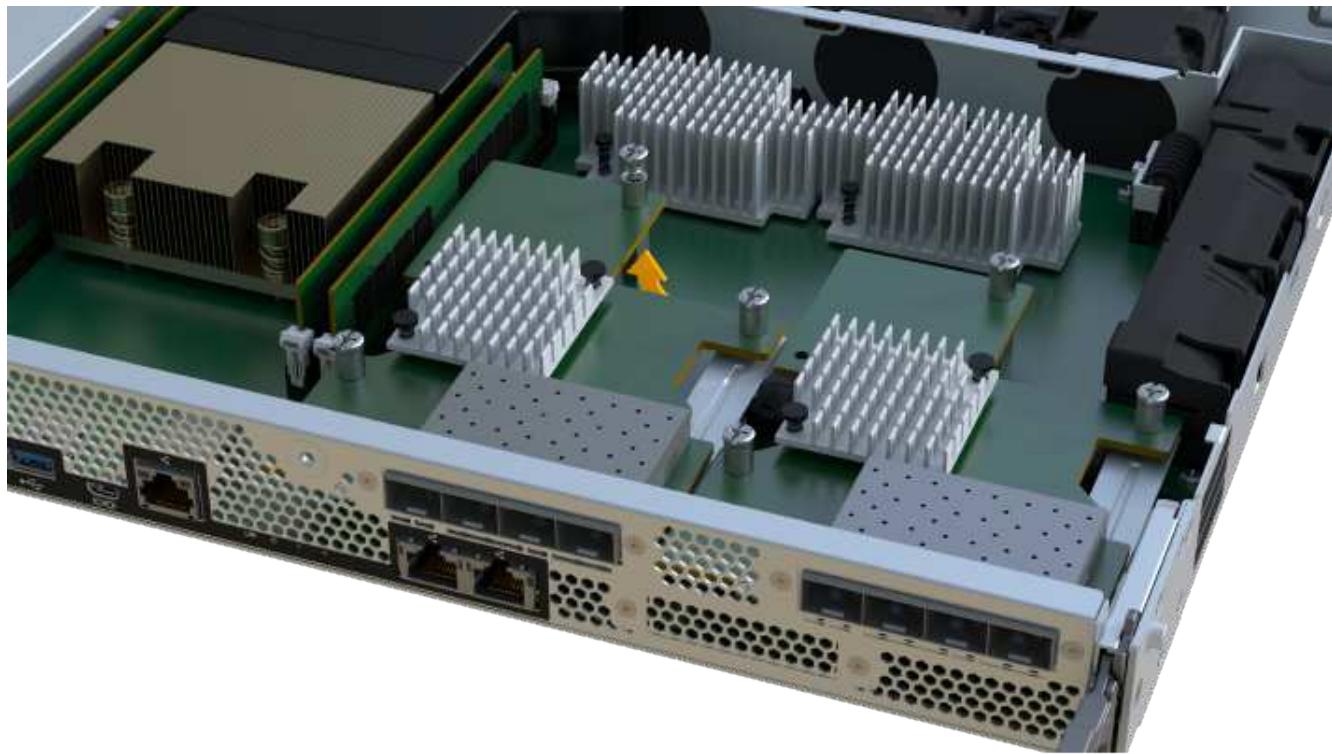


The image above is an example, the appearance of your HIC may differ.

6. Carefully detach the HIC from the controller card by lifting the card up and out of the controller.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



The image above is an example, the appearance of your HIC may differ.

7. Place the HIC on a flat, static-free surface.

Step 4: Upgrade the HIC

After removing the old HIC, you install the new one.

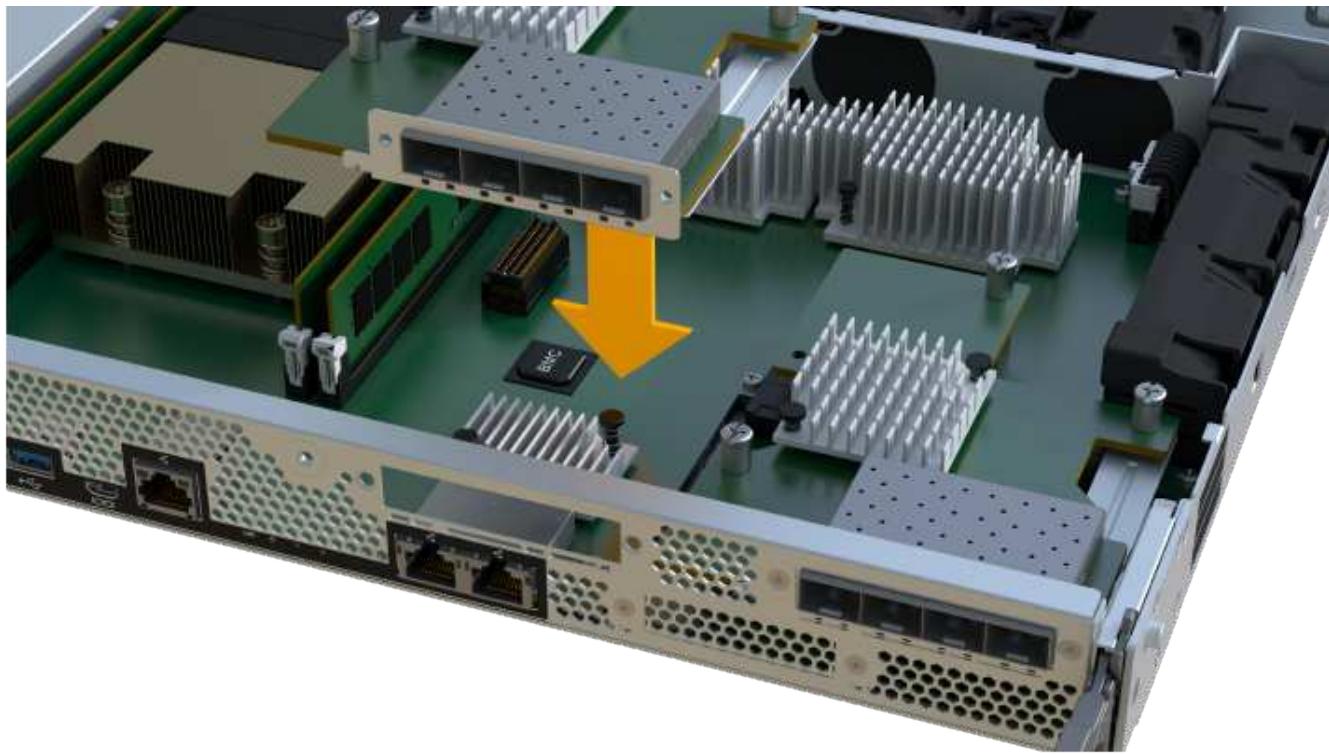


Possible loss of data access — Never install a HIC in an EF300 or EF600 controller canister if that HIC was designed for another E-Series controller. In addition, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Align the single thumbscrew on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



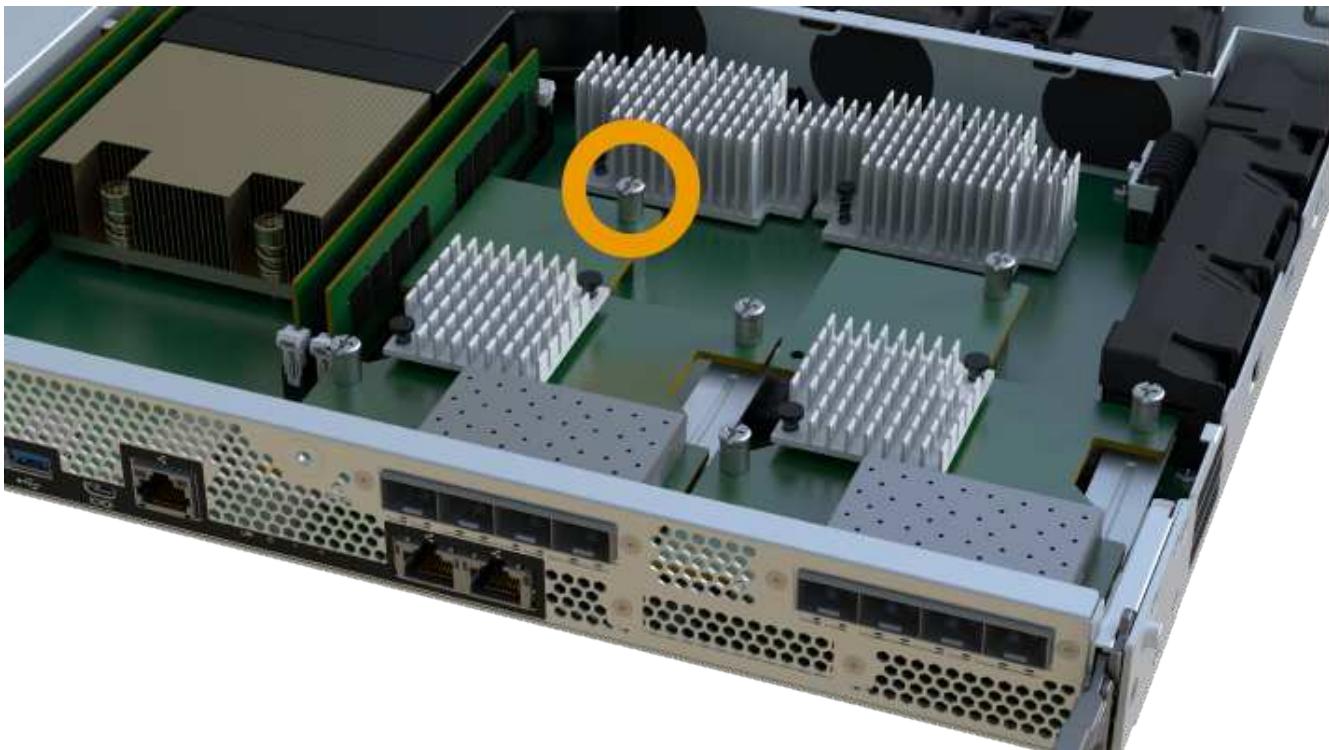
The image above is an example, the appearance of your HIC may differ.

3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage—Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrew.

4. Hand-tighten the HIC thumbscrew.





The image above is an example; the appearance of your HIC may differ.



Do not use a screwdriver, or you might over tighten the screws.

- Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original HIC with the three screws.

Step 5: Reinstall controller canister

After upgrading the HIC, reinstall the controller canister into the controller shelf.

Steps

- Lower the cover on the controller canister and secure the thumbscrew.
- While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



- If removed, install the SFPs into the new HIC and reconnect all the cables. If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

Step 6: Complete the HIC upgrade

Place the controller online, collect support data, and resume operations.

Steps

- Place controller online.

- a. Plug in power cables.
2. As the controller boots, check the controller LEDs.
 - The amber Attention LED remains on.
 - The Host Link LEDs might be on, blinking, or off, depending on the host interface.
3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
 - d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
 - e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

The process of upgrading a host interface card in your storage array is complete. You can resume normal operations.

Replace failed host interface card (HIC) in EF300 or EF600

Follow this procedure to replace a failed host interface card (HIC) in an EF300 or EF600 array.

About this task

When you replace a failed HIC, you must power off the storage array, replace the HIC, and reapply power.

Before you begin

- Review [Requirements for EF300 or EF600 HIC upgrades](#).
- Schedule a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure. Because both controllers must have the same HIC configuration when they are powered on, the power must be off when you install HICs.

What you'll need

- HICs that are compatible with your controllers.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- Labels to identify each cable that is connected to the controller canister.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

 **Possible loss of data access** — Never install a HIC in an EF300 or EF600 controller canister if that HIC was designed for another E-Series controller. In addition, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Step 1: Place the controller offline

Place the affected controller offline so you can safely replace the HICs.

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which battery to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.

d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

5. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

6. Select **Recheck** from the Recovery Guru, and confirm that the OK to remove field in the Details area displays Yes, indicating that it is safe to remove this component.

Step 2: Remove controller canister

Remove the controller canister so you can replace the failed host interface card.

Steps

1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



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

3. If the HIC ports use SFP+ transceivers, remove them.

Depending on what type of HIC you are upgrading to, you might be able to reuse these SFPs.

4. Confirm that the Cache Active LED on the back of the controller is off.
5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 3: Remove the HIC

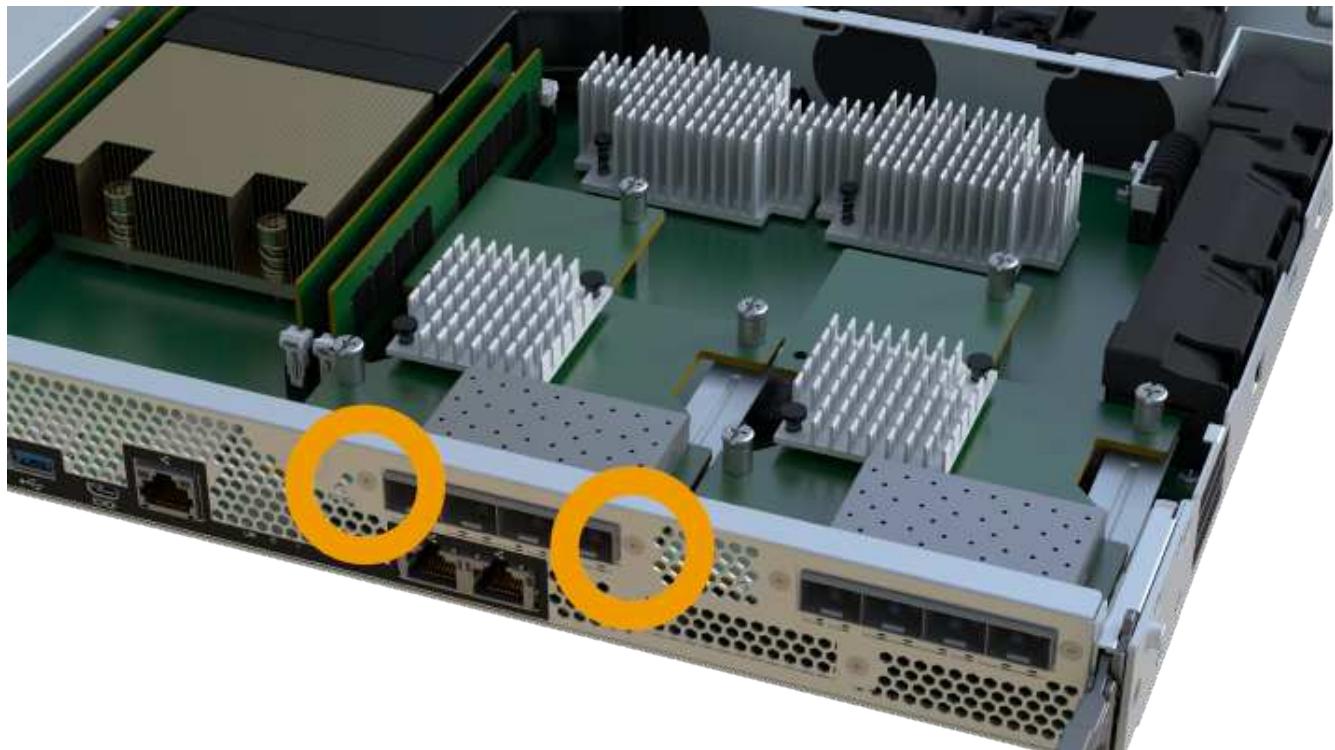
Remove the original HIC so you can replace it with an upgraded one.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.

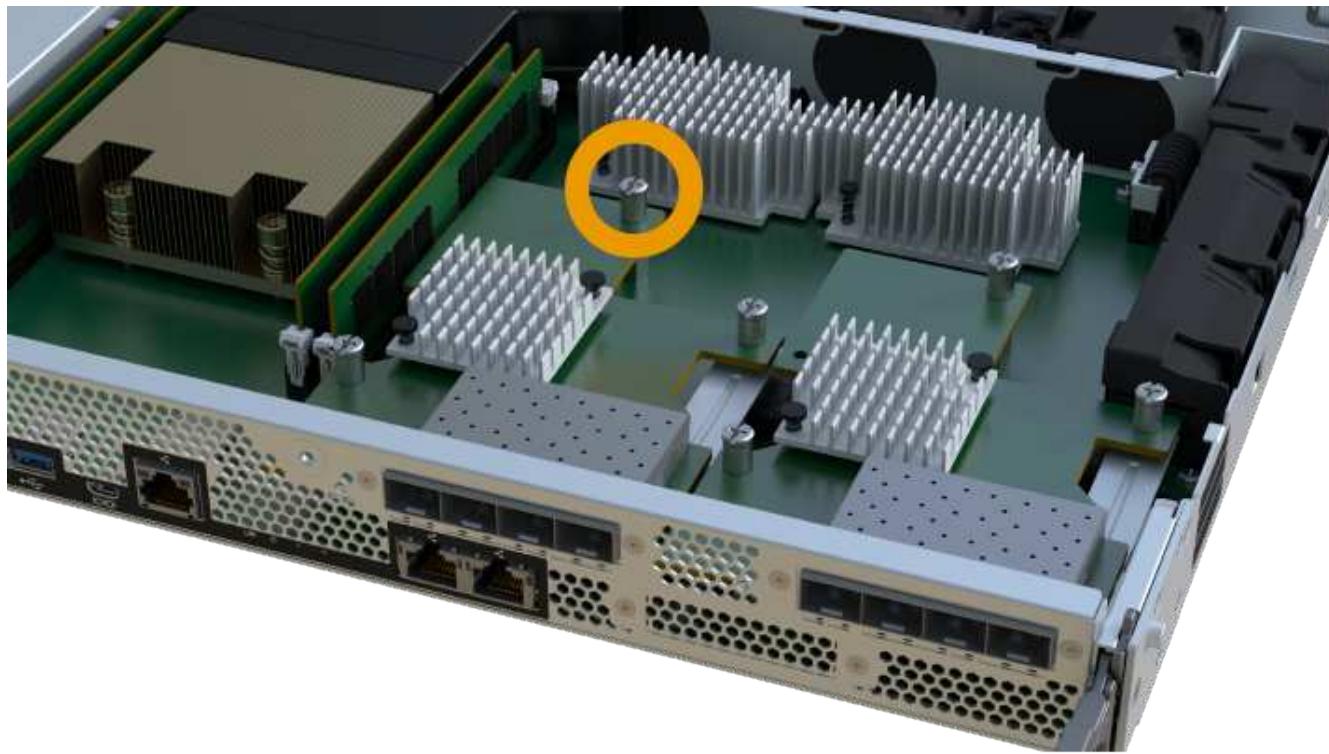
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

3. Using a Phillips screwdriver, remove the two screws that attach the HIC faceplate to the controller canister.



The image above is an example; the appearance of your HIC may differ.

4. Remove the HIC faceplate.
5. Using your fingers or a Phillips screwdriver, loosen the single thumbscrew that secure the HIC to the controller card.



The HIC comes with three screw locations on the top, but is secured with only one.

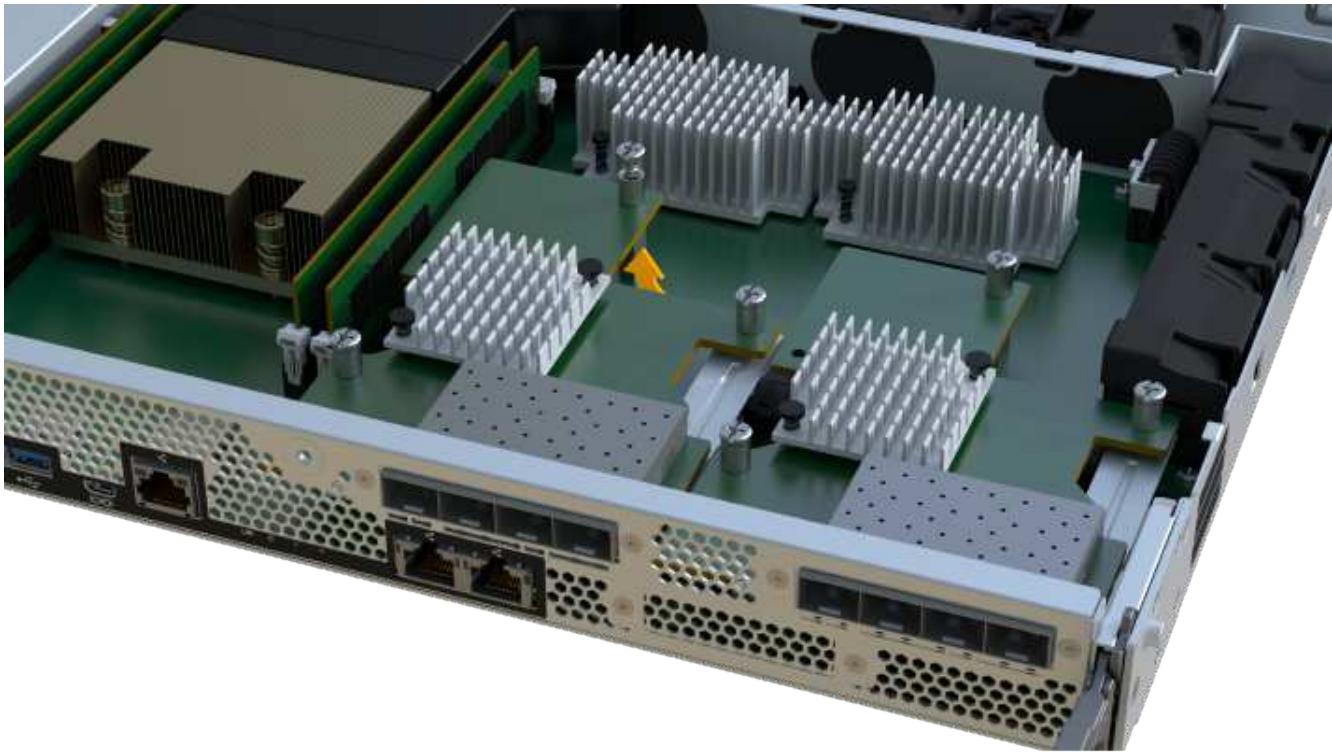


The image above is an example; the appearance of your HIC may differ.

6. Carefully detach the HIC from the controller card by lifting the card up and out of the controller.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



The image above is an example; the appearance of your HIC may differ.

7. Place the HIC on a flat, static-free surface.

Step 4: Replace the HIC

After removing the old HIC, install a new HIC.



Possible loss of data access — Never install a HIC in an EF300 or EF600 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Steps

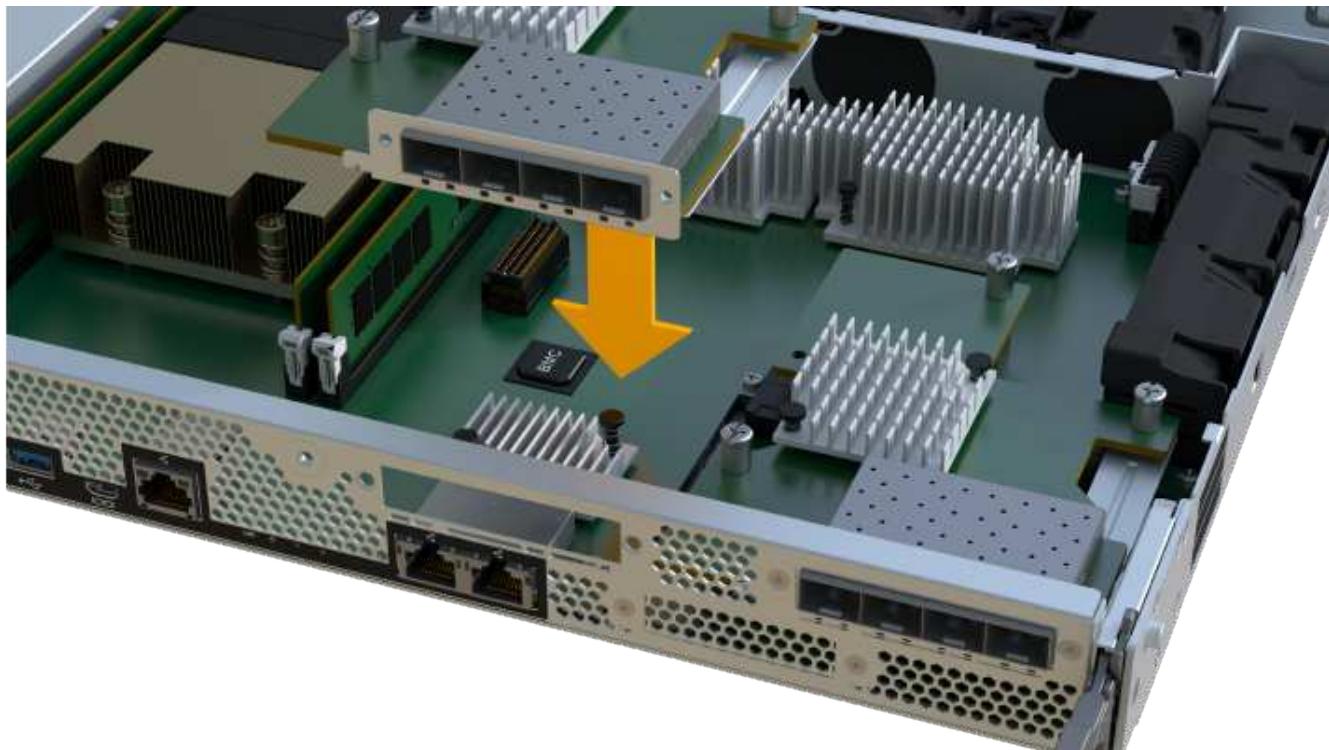
1. Unpack the new HIC and the new HIC faceplate.
2. Align the single thumbscrew on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrew.



The image above is an example; the appearance of your HIC may differ.

4. Hand-tighten the HIC thumbscrew.

Do not use a screwdriver, or you might over tighten the screws.

5. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original HIC with the three screws.

Step 5: Reinstall controller canister

After replacing the HIC, reinstall the controller canister into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



3. Install the SFPs into the new HIC and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

Step 6: Complete HIC replacement

Place the controller online, collect support data, and resume operations.

Steps

1. Place controller online.
 - a. In System Manager, navigate to the hardware page.
 - b. Select **Show back of controller**.
 - c. Select the controller with the replaced host interface card.
 - d. Select **Place online** from the drop-down list.
2. As the controller boots, check the controller LEDs.

When communication with the other controller is reestablished:

- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.

3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.

- a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
- b. If volumes are all owned by preferred owner continue to Step 6.
- c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute volumes**.
- d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
- e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.

6. Collect support data for your storage array using SANtricity System Manager.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your host interface card replacement is complete. You can resume normal operations.

Host port protocol conversion

Requirements for EF300 or EF600 host protocol conversion

Before converting the host protocol for an EF300 or EF600 array, review the following requirements.

- You have scheduled a downtime maintenance window for this procedure.
- You must stop host I/O operations when you perform the conversion. You cannot access data on the storage array until you have successfully completed the conversion.
- You are using out-of-band management. (You cannot use in-band management to complete this procedure.)
- You have obtained the necessary hardware for the conversion, which may include a new set of HICs and/or SFPs. Your NetApp Sales Representative can help you determine what hardware you need and help you order the correct parts.
- The dual-protocol SFP transceivers support 16Gb and 8Gb FC, as well as 10Gb iSCSI. Therefore, you may not need to change SFPs if you have the dual-protocol and are simply switching between FC and iSCSI or vice versa.
- Some host port protocol conversions may require a host interface card addition, or upgrade.

Change host protocol for an EF300 or EF600

Follow this procedure to change the host port protocol in an EF300 or EF600 array. This procedure applies only to host interface cards (HICs) using either Infiniband (IB) or Fibre Channel (FC).

Step 1: Obtain the feature pack key

To obtain the feature pack key, you need the serial number from the controller shelf, a Feature Activation Code, and the Feature Enable Identifier for the storage array.

Steps

1. Locate the serial number.
 - a. From SANtricity System Manager, select **Support > Support Center**.
 - b. With the **Support Resources** tab selected, scroll to the **View top storage array properties** section.
 - c. Locate the **Chassis Serial Number**, and copy this value to a text file.

View top storage array properties

| | |
|--|----------------------------------|
| Storage array world-wide identifier (ID): | 600A0980006CEF9B00000000574DB18C |
| Chassis serial number: | 1142FG00061 |
| Number of shelves: | 2 |
| Number of drives: | 41 |
| Drive media types: | HDD |
| Number of controllers: | 2 |
| Controller board ID: | 2806 |

2. Locate the **feature pack submodel ID**.

- a. From the SANtricity System Manager, select **Support**.
- b. Select the **Support Center** tile.
- c. On the Support Resources tab, locate and select the **Storage Array Profile** link.
- d. Type **feature pack submodel ID** in the text box, and click **Find**.
- e. Locate the feature pack submodel ID for the starting configuration.

Storage Array Profile



Feature pack submodel ID

Find

Results: 1 of 1

Feature pack submodel ID: 318

Additional feature information

Snapshot groups allowed per base volume (see note below): 4
Volume assignments per host or host cluster: 256

Note: If a volume is a member of a snapshot consistency group, that membership (member volume) counts against both the snapshot group limit and the volume assignment limit.

FIRMWARE INVENTORY

Storage Array

| | |
|---|--------------------------|
| Report Date: | 2/13/17 4:56:33 PM UTC |
| Storage Array Name: | LDAPandCLI-Cfg04-Arapaho |
| Current SANtricity OS Software Version: | 88.40.39.74.001 |
| Management Software Version: | 11.40.0010.0051 |
| Controller Firmware Version: | 88.40.39.74 |
| Supervisor Software Version: | 88.40.39.74 |
| IOM (ESM) Version: | 81.40.0G00.0006 |
| Current NVSRAM Version: | N280X-840834-402 |
| Staged SANtricity OS Software Version: | None |
| Staged NVSRAM Version: | None |

- Using the feature pack submodel ID, locate the corresponding Controller submodel ID for the starting configuration and find the Feature Activation Code for the desired ending configuration within the following table. Then, copy that Feature Activation Code to a text file.

| Starting configuration | | Ending configuration | | Feature Activation Code |
|------------------------|----------------------------|------------------------|-----------|-------------------------|
| Controller submodel ID | HIC ports | Controller submodel ID | HIC ports | |
| 443 | NVMe/FC or NVMe/RoCE | 444 | NVMe/IB | DH5-HB4-ZK9QH |
| | | 448 | FC | 7HZ-EB4-ZHAYW |
| | | 491 | iSER/IB | 0H1-675-Z5SII |
| | | 492 | SRP/IB | NHD-V75-ZB6ZX |
| | | | | |
| 444 | NVMe/FC or NVMe/IB | 443 | NVMe/RoCE | YH3-XB4-ZJRIZ |
| | | 448 | FC | 2HU-BB4-ZFCG5 |
| | | 491 | iSER/IB | 2H3-P75-Z6AQG |
| | | 492 | SRP/IB | 5HG-G75-ZDNEZ |
| | | | | |

| Starting configuration | | Ending configuration | | Feature Activation Code |
|------------------------|---------|----------------------|----------------------------|-------------------------|
| 448 | FC | 443 | NVMe/FC or NVMe/RoCE | JHX-UB4-ZGTP1 |
| | | 444 | NVMe/FC or NVMe/IB | LHS-RB4-ZDV29 |
| | | 491 | iSER/IB | FH6-975-Z7Q7H |
| | | 492 | SRP/IB | 0HI-Z75-ZE4L5 |
| 491 | iSER/IB | 443 | NVMe/FC or NVMe/RoCE | MHQ-M85-ZIJNT |
| | | 444 | NVMe/FC or NVMe/IB | 4HS-685-ZJZ1U |
| | | 448 | FC | YHU-P85-ZLHCX |
| | | 465 | FC/PTL | AHX-985-ZMXMI |
| | | 492 | SRP/IB | ZHZ-S85-ZNF4J |
| 492 | SRP/IB | 443 | NVMe/FC or NVMe/RoCE | EH3-C85-Z0V93 |
| | | 444 | NVMe/FC or NVMe/IB | BH5-V85-ZQDQJ |
| | | 448 | FC | 1H8-F85-ZRT1V |
| | | 465 | FC/PTL | 1HA-Y85-ZSB7S |
| | | 491 | iSER/IB | KHD-I85-ZUSMI |
| | | 492 | SRP | NHL-J75-ZFL3W |
| 465 | FC/PTL | 491 | iSER | 6H8-S75-Z98FH |
| | | 492 | SRP | NHL-J75-ZFL3W |

| Starting configuration | | Ending configuration | | Feature Activation Code |
|-------------------------------|-----------|-----------------------------|-------------------------|--------------------------------|
| 516 | NVMe/RoCE | 517 | NVMe/IB | LHF-285-ZV9YZ |
| | | 518 | FC | IHI-L85-ZXQEP |
| | | 519 | iSER/IB | RHK-585-ZY7P5 |
| | | 520 | FC-PTL | NHN-095-ZZ0XF |
| | | 521 | SRP/IB | GHP-895-Z25BD |
| 517 | NVMe/IB | 516 | NVMe/RoCE | 7HS-R95-Z3M06 |
| | | 518 | FC | UHU-B95-Z43X2 |
| | | 519 | FC-PTL | 8HX-U95-Z5K6F |
| | | 520 | iSER/IB | UHZ-E95-Z71LH |
| | | 521 | SRP/IB | SH2-X95-Z8IVS |
| 518 | FC | 516 | NVMe/FC or NVMe/RoCE | UH5-H95-Z9Z58 |
| | | 517 | NVMe/FC or NVMe/IB | XH7-195-ZBGJC |
| | | 519 | FC-PTL | FHA-K95-ZCXX0 |
| | | 520 | iSER/IB | JHC-595-ZDE3X |
| | | 521 | SRP/IB | 0HF-095-ZFVFN |

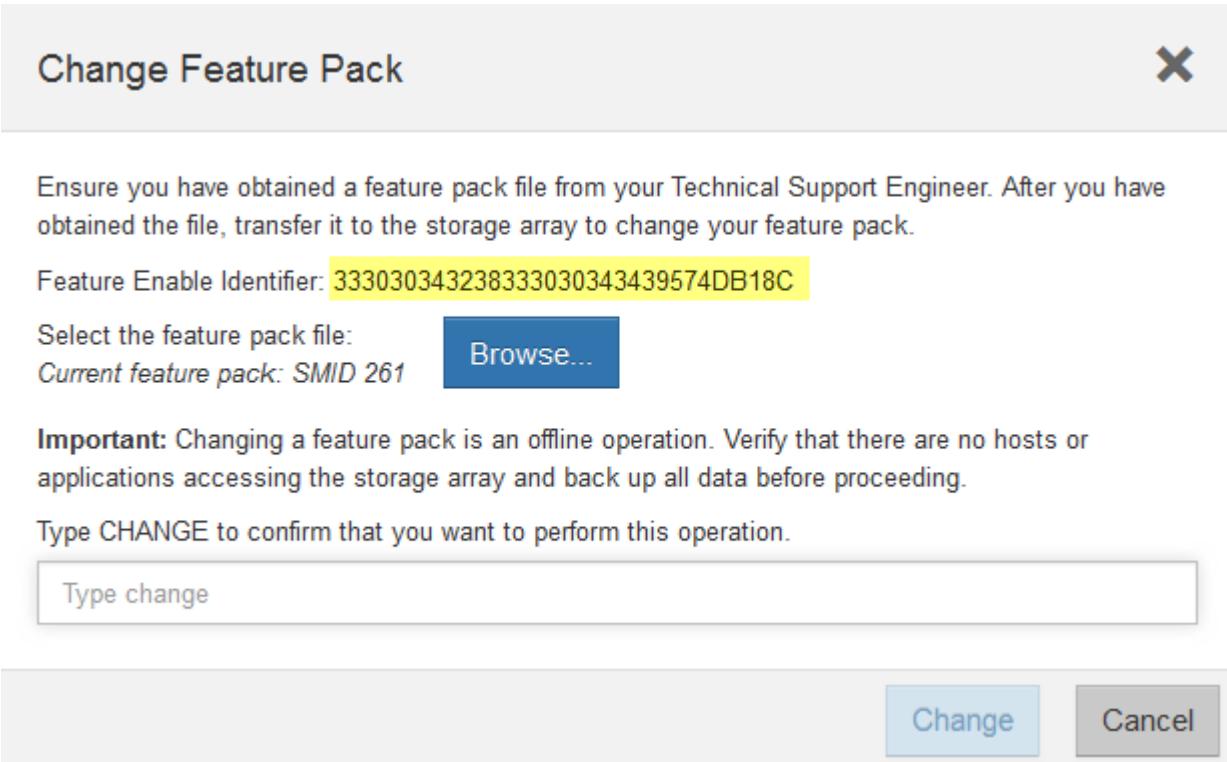
| Starting configuration | | Ending configuration | | Feature Activation Code |
|------------------------|---------|----------------------|----------------------|-------------------------|
| 519 | FC-PTL | 516 | NVMe/FC or NVMe/RoCE | YHH-895-ZGCXS |
| | | 517 | NVMe/FC or NVMe/IB | 2HK-R95-ZHT83 |
| | | 518 | FC | 1HM-BA5-ZJALA |
| | | 520 | iSER/IB | YHP-UA5-ZKRXA |
| | | 521 | SRP/IB | MHR-EA5-ZL83V |
| 520 | iSER/IB | 516 | NVMe/FC or NVMe/RoCE | HHU-XA5-ZNPLT |
| | | 517 | NVMe/FC or NVMe/IB | YHW-HA5-Z07QK |
| | | 518 | FC | WHZ-1A5-ZPN4U |
| | | 519 | FC/PTL | 7H2-KA5-ZR5C3 |
| | | 521 | SRP | 3H5-4A5-ZSLVX |
| 521 | SRP/IB | 516 | NVMe/FC or NVMe/RoCE | 1H7-NA5-ZT31W |
| | | 517 | NVMe/FC or NVMe/IB | XHA-7A5-ZVJGC |
| | | 518 | FC | KHC-QA5-ZW1P3 |
| | | 519 | FC/PTL | CHE-AA5-ZXH2F |
| | | 520 | iSER/IB | SHH-TA5-ZZYHS |



If your controller submodel ID is not listed, contact [NetApp Support](#).

4. In System Manager, locate the Feature Enable Identifier.
 - a. Go to **Settings > System**.
 - b. Scroll down to **Add-ons**.
 - c. Under **Change Feature Pack**, locate the **Feature Enable Identifier**.

- d. Copy and paste this 32-digit number to a text file.



5. Go to [NetApp License Activation: Storage Array Premium Feature Activation](#), and enter the information required to obtain the feature pack.

- Chassis Serial Number
- Feature Activation Code
- Feature Enable Identifier

NOTE: The Premium Feature Activation web site includes a link to “Premium Feature Activation Instructions.” Do not attempt to use those instructions for this procedure.

6. Choose whether to receive the key file for the feature pack in an email or download it directly from the site.

Step 2: Stop host I/O

Stop all I/O operations from the host before converting the protocol of the host ports.

You cannot access data on the storage array until you successfully complete the conversion.

Steps

1. 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.



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.

2. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

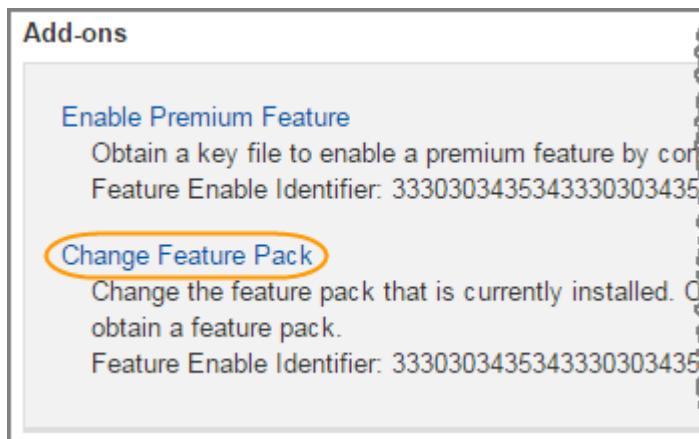
3. From the Home page of SANtricity System Manager, select **View Operations in Progress**.
4. Wait for all operations to complete before continuing with the next step.

Step 3: Change the feature pack

Change the feature pack to convert the host protocol of your host ports.

Steps

1. From SANtricity System Manager, select **Settings > System**.
2. Under **Add-ons**, select **Change Feature Pack**.



3. Click **Browse**, and then select the feature pack you want to apply.
4. Type **CHANGE** in the field.
5. Click **Change**.

The feature pack migration begins. Both controllers automatically reboot twice to allow the new feature pack to take effect. The storage array returns to a responsive state after the reboot is complete.

6. Confirm the host ports have the protocol you expect.
 - a. From SANtricity System Manager, select **Hardware**.
 - b. Click **Show back of shelf**.
 - c. Select the graphic for either Controller A or Controller B.
 - d. Select **View settings** from the context menu.
 - e. Select the **Host Interfaces** tab.
 - f. Click **Show more settings**.

What's next?

Go to [Complete host protocol conversion](#).

Complete host protocol conversion for an EF300 or EF600

After you apply the feature pack key to convert the protocol, you must configure the host to use the appropriate protocol.

For step-by-step instructions, see the guide appropriate for your system:

- [Linux express configuration](#)
- [VMware express configuration](#)
- [Windows express configuration](#)

Specific settings might vary. Check the [NetApp Interoperability Matrix](#) for specific instructions and additional recommended settings for your solution.

Power supplies

Requirements for EF300 or EF600 power supply replacement

Before replacing a power supply in an EF300 or EF600 array, review the following requirements.

- You must have a replacement power supply that is supported for your controller shelf or drive shelf model.
- You must have an ESD wristband, or you have taken other antistatic precautions.

Replace an EF300 or EF600 power supply

You can replace a power supply when it fails in your EF300 or EF600 controller.

If a power supply fails, you must replace it as soon as possible so the controller shelf has a redundant power source.

Before you begin

- Review the details in the Recovery Guru to confirm that there is an issue with the power supply. Select **Recheck** from the Recovery Guru to ensure no other items must be addressed first.
- Check that the amber Attention LED on the power supply is on, indicating that the power supply or its integrated fan has a fault.

What you'll need

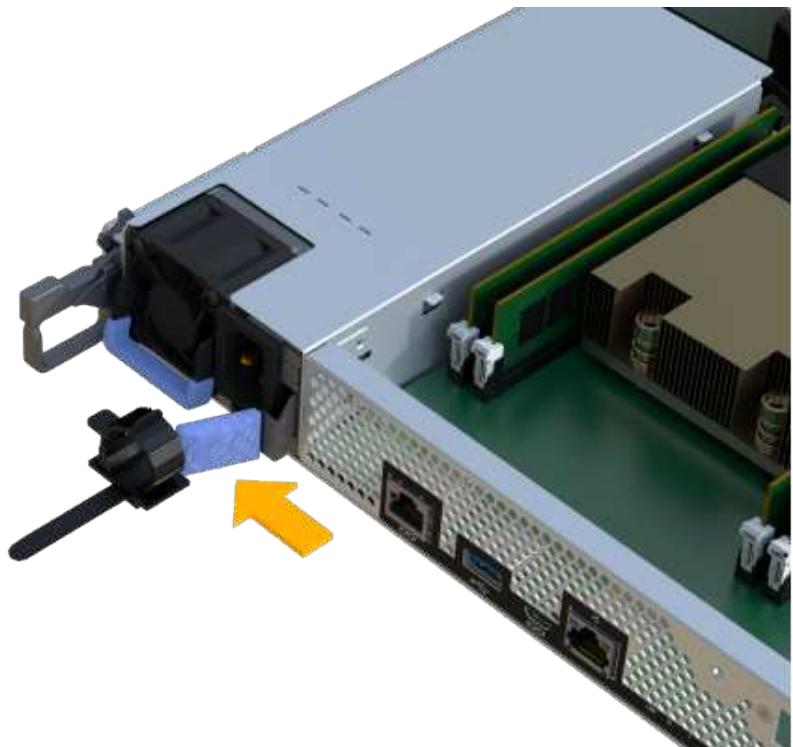
- A replacement power supply that is supported for your controller shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Remove failed power supply

Remove a failed power supply so you can replace it with a new one.

Steps

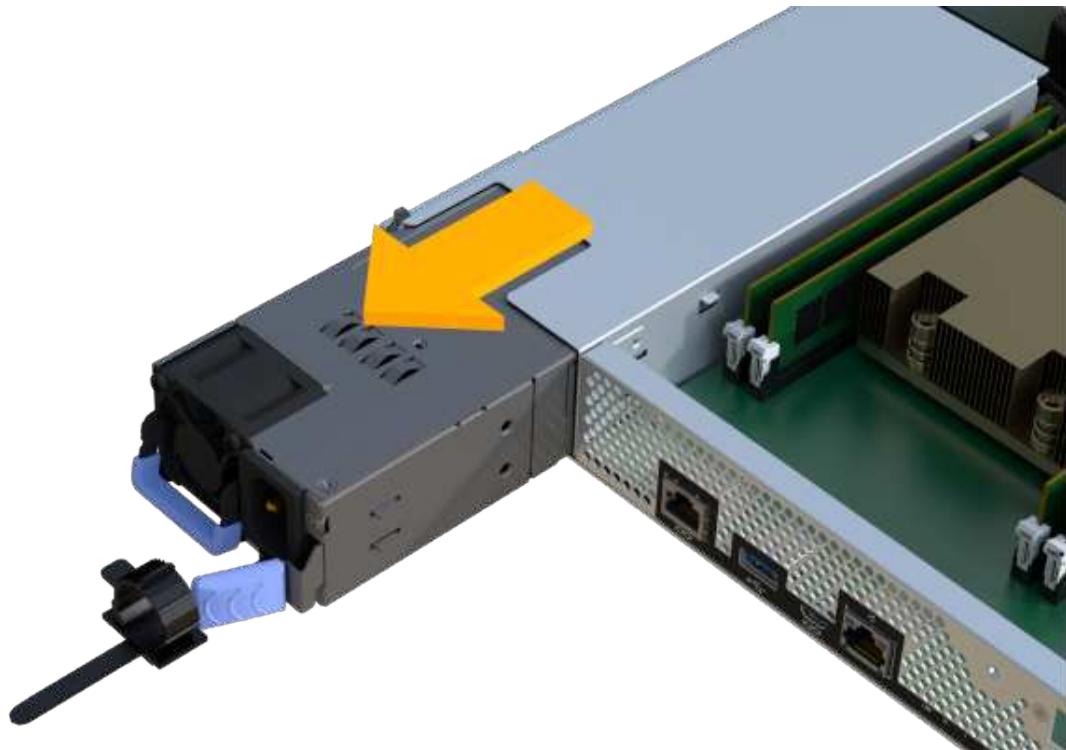
1. Unpack the new power supply, and set it on a level surface near the drive shelf.
Save all packing materials for use when returning the failed power supply.
2. Disconnect the power cables:
 - a. Open the power cord retainer, and then unplug the power cord from the power supply.
 - b. Unplug the power cord from the power source.
3. Locate the tab to the right of the power supply and press it towards the power supply unit.



4. Locate the handle on the front of the power supply.
5. Use the handle to slide the power supply straight out of the system.



When removing a power supply, always use two hands to support its weight.



Step 2: Install new power supply and complete the replacement

After removing the failed power supply, install a new one.

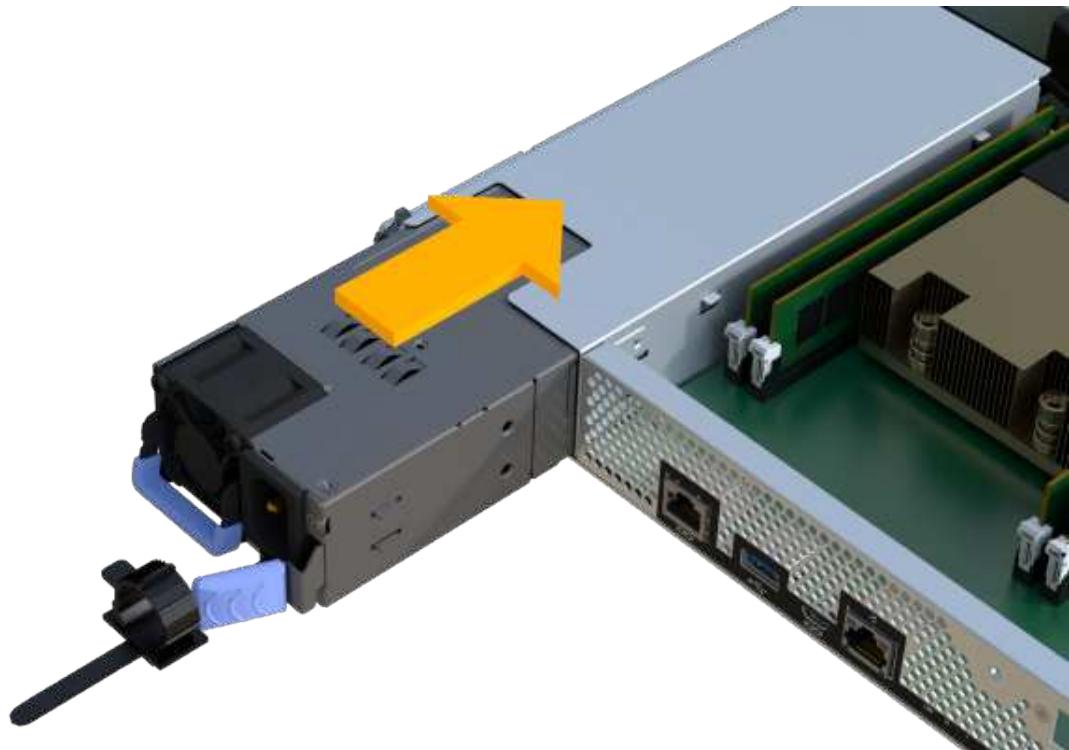
Steps

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system; you can damage the connector.



2. Confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

3. From SANtricity System Manager, click **Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

What's next?

Your power supply replacement is complete. You can resume normal operations.

SAS expansion cards

Requirements for EF300 SAS expansion card replacement

If you plan to add a SAS expansion card to an EF300, review the following requirements.

- You must follow the [Install and set up EF300 and EF600 storage systems](#) to set up your controller.
- You must update your firmware to the latest version. To update your firmware, follow the instructions in the [Upgrading SANtricity OS](#).
- You must schedule a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure.
- You have an ESD wristband, or you have taken other antistatic precautions.

- You have a #1 Phillips screwdriver.
- You have labels to identify each cable that is connected to the controller canister.
- You have a management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)
- EF300 controllers may have a SAS expansion card installed in port 1 to allow for drive tray expansion.
- To cable your SAS expansion, see [Cabling E-Series hardware](#) for instructions.

Add SAS expansion card to EF300

You can add a SAS expansion card to an EF300 controller to allow for drive tray expansion.

About this task

When you add a SAS expansion card, you must power off the storage array, install the new SAS expansion card, and reapply power.

Before you begin

- Review [Requirements for EF300 SAS expansion card replacement](#).
- You must schedule a downtime maintenance window for this procedure. You cannot access data on the storage array until you have successfully completed this procedure.

What you'll need

- A SAS expansion card that is compatible with your controller.
- An ESD wristband, or you have taken other antistatic precautions.
- A flat, static free work area.
- A #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller shelf offline

Place the controller shelf offline so you can safely add the SAS expansion card.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Configuration Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

3. 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.



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, the host application might lose access to the data because the storage is not accessible.

4. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

5. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
6. Power down the controller shelf.
 - a. Label and then unplug both power cables from controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can add the new SAS expansion card.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. Confirm that the Cache Active LED on the back of the controller is off.
5. Squeeze the handles on either side of the controller, and pull back until it releases from the shelf.



6. Using two hands and the handles, slide the controller canister out of the shelf. When the front of the controller is free of the enclosure, use two hands to pull it out completely.



Always use two hands to support the weight of a controller canister.



7. Place the controller canister on a flat, static-free surface.

Step 3: Add the new SAS expansion card

Install the SAS expansion card to allow for drive tray expansion.



On an EF300 controller shelf, a SAS expansion card may only be installed in port 1.

Steps

1. Remove the controller canister's cover by unscrewing the single thumbscrew and lifting the lid open.
2. Confirm that the green LED inside the controller is off.
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.
3. Using a #1 Phillips screwdriver, remove the two screws that attach the faceplate to the controller canister, and remove the faceplate.
4. Align the single thumbscrew on the SAS expansion card with the corresponding hole on the controller, and align the connector on the bottom of the expansion card with the expansion card interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the SAS expansion card or on the top of the controller card.

5. Carefully lower the SAS expansion card into place, and seat the expansion card connector by pressing gently on the expansion card.
6. Hand-tighten the SAS expansion card thumbscrew.

Do not use a screwdriver, or you might over tighten the screws.

7. Using a #1 Phillips screwdriver, attach the faceplate you removed from the original controller canister to the new controller canister with the two screws.

Step 4: Reinstall the controller canister

After installing the new SAS expansion card, reinstall the controller canister into the controller shelf.

Steps

1. Lower the cover on the controller canister and secure the thumbscrew.
2. While squeezing the controller handles, gently slide the controller canister all the way into the controller shelf.



The controller audibly clicks when correctly installed into the shelf.



Step 5: Complete SAS expansion card addition

Place the controller online, collect support data, and resume operations.

Steps

1. Plug in power cables to place the controller online.
2. As the controller boots, check the controller LEDs.
 - The amber Attention LED remains on.
 - The Host Link LEDs might be on, blinking, or off, depending on the host interface.
3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS is installed.

As needed, install the latest version.

5. Verify that all volumes have been returned to the preferred owner.
 - a. Select **Storage > Volumes**. From the **All Volumes** page, verify that volumes are distributed to their preferred owners. Select **More > Change ownership** to view volume owners.
 - b. If volumes are all owned by preferred owner continue to Step 6.
 - c. If none of the volumes are returned, you must manually return the volumes. Go to **More > Redistribute**

- volumes.
- d. If only some of the volumes are returned to their preferred owners after auto-distribution or manual distribution you must check the Recovery Guru for host connectivity issues.
 - e. If there is no Recovery Guru present or if following the recovery guru steps the volumes are still not returned to their preferred owners contact support.
6. Collect support data for your storage array using SANtricity System Manager.
- a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.



To cable your SAS expansion, see [Cabling E-Series hardware](#) for instructions.

What's next?

The process of adding a SAS expansion card in your storage array is complete. You can resume normal operations.

E2800

Maintain E2800 hardware

For the E2800 storage system, you can perform maintenance procedures on the following components.

Batteries

Each controller canister includes a battery that preserves cached data if the AC power fails.

Controllers

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

Canisters

Canisters consist of three different types: power-fan canisters (power supplies) that supply a redundant power source and adequate cooling in a 12-drive or 24-drive controller shelf or drive shelf; power canisters that are used for power redundancy in a 60-drive controller shelf or drive shelf; and fan canisters that are used for cooling the 60-drive controller shelf or drive shelf.

Drives

A drive is an electromagnetic mechanical device that provides the physical storage media for data.

Host interface cards (HICs)

A host interface card (HIC) can optionally be installed within a controller canister. The E2800 controller includes built-in host ports on the controller card itself, as well as host ports on the optional HIC. Host ports that

are built into the controller are called baseboard host ports. Host ports that are built into the HIC are called HIC ports.

Host port protocol

You can convert the protocol of a host to a different protocol so that compatibility and communication can be established.

Batteries

Requirements for E2800 battery replacement

Before you replace an E2800 battery, review the requirements and considerations.

Each controller canister includes a battery that preserves cached data if the AC power fails.

Recovery Guru alerts

If the Recovery Guru in SANtricity System Manager reports one of following statuses, you must replace the affected battery:

- Battery Failed
- Battery Replacement Required

From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.

Procedure overview

To protect your data, you must replace a failed battery as soon as possible.

The following is an overview of the steps required to replace a battery in an E2800 controller:

1. Prepare for replacement, following the appropriate steps for a duplex or simplex configuration.
2. Remove the controller canister.
3. Remove the failed battery.
4. Install the new battery.
5. Re-install the controller canister.
6. Complete the replacement, following the appropriate steps for a duplex or simplex configuration.

Duplex or simplex configuration

The steps to replace a battery depend on whether you have one or two controllers, as follows:

| If your storage array has... | You must... |
|------------------------------|--|
| Two controllers (duplex) | <ol style="list-style-type: none"> 1. Take the controller offline. 2. Remove the controller canister. 3. Replace the battery. 4. Replace the controller canister. 5. Bring the controller online. |
| One controller (simplex) | <ol style="list-style-type: none"> 1. Stop host I/O operations. 2. Power down the controller shelf. 3. Remove the controller canister. 4. Replace the battery. 5. Replace the controller canister. 6. Apply power to the controller shelf. |

Requirements for replacing a battery

If you plan to replace a failed battery, you must have:

- A replacement battery.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Prepare to replace E2800 battery

The steps to prepare for battery replacement depend on whether you have a duplex configuration (two controllers) or a simplex configuration (one controller).

- For duplex configurations, see [Place controller offline \(duplex\)](#).
- For simplex configurations, see [Power down the controller shelf \(simplex\)](#).

Before you begin

- Verify that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.
- Review the [Requirements for E2800 battery replacement](#).

Place controller offline (duplex)

If you have a duplex configuration, you must place the affected controller offline so you can safely remove the failed battery. The controller that you are not placing offline must be online (in the optimal state).



Perform this task only if your storage array has two controllers (duplex configuration).

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which battery to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

4. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

5. If the controller is not already offline, take it offline now using SANtricity System Manager.

- From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.
 - d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

- Alternatively, you can take the controllers offline by using the following CLI commands:

For controller A: set controller [a] availability=offline

For controller B: set controller [b] availability=offline

6. Wait for SANtricity System Manager to update the controller's status to offline.
7. Go to [Remove E2800 controller canister](#).



Do not begin any other operations until after the status has been updated.

Power down the controller shelf (simplex)

If you have a simplex configuration, power down the controller shelf so you can safely remove the failed battery.



Perform this task only if your storage array has one controller (simplex configuration).

Steps

1. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

2. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

3. Ensure that no I/O operations are occurring between the storage array and all connected hosts. For example, you can perform these steps:
 - 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. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

5. From the home page of SANtricity System Manager, select **View Operations in Progress**.
6. Confirm that all operations have completed before continuing with the next step.
7. Turn off both power switches on the controller shelf.
8. Wait for all LEDs on the controller shelf to turn off.
9. Go to [Remove E2800 controller canister](#).

Remove E2800 controller canister

You need to remove the controller canister from the controller shelf, so you can remove the battery.

When you remove a controller canister, you must disconnect all cables. Then, you can slide the controller canister out of the controller shelf.

What you'll need

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

Steps

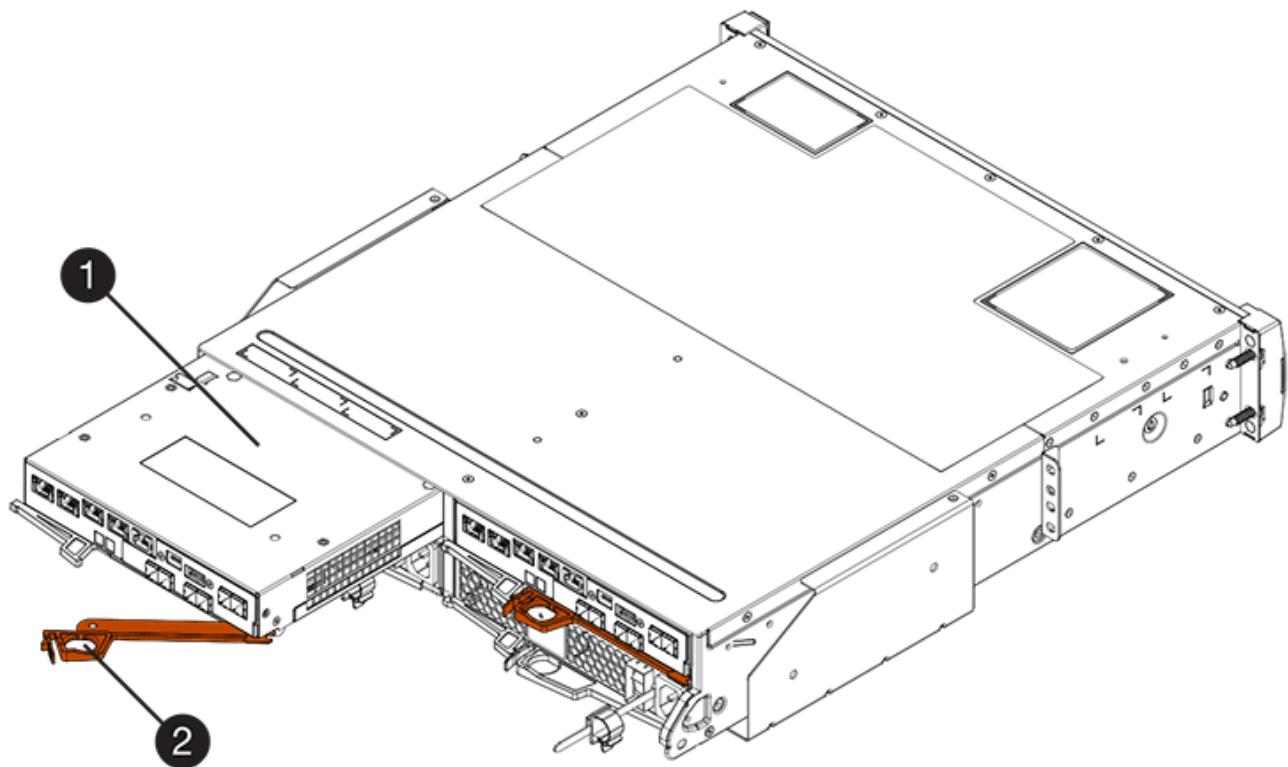
1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. If the host ports on the controller canister use SFP+ transceivers, leave them installed.
5. Confirm that the Cache Active LED on the back of the controller is off.
6. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

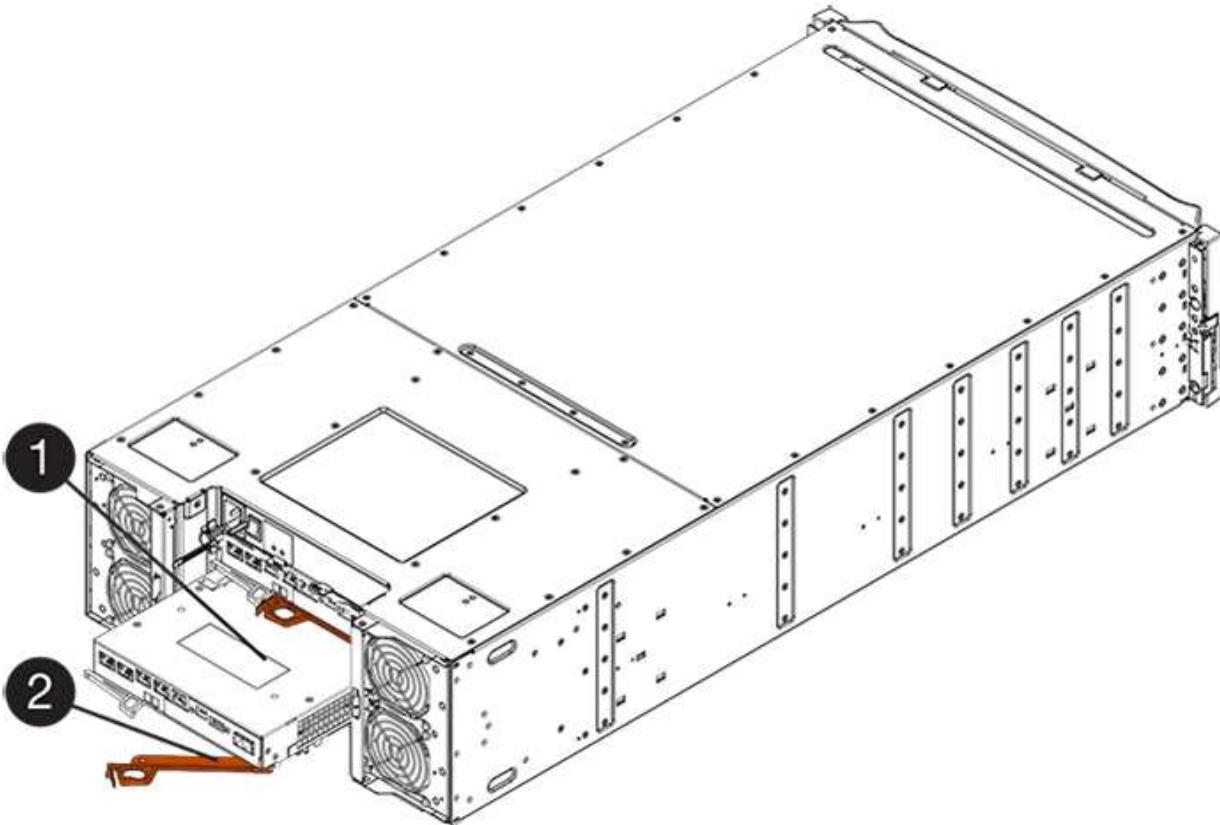
The following figure is an example of an E2812 controller shelf, E2824 controller shelf, or EF280 flash array:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

7. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E2812 controller shelf, E2824 controller shelf or EF280 flash array, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

8. Turn the controller canister over, so that the removable cover faces up.
9. Place the controller canister on a flat, static-free surface.
10. Go to [Remove failed E2800 battery](#).

Remove failed E2800 battery

After removing the controller canister from the controller shelf, you can remove the battery.

Steps

1. Remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

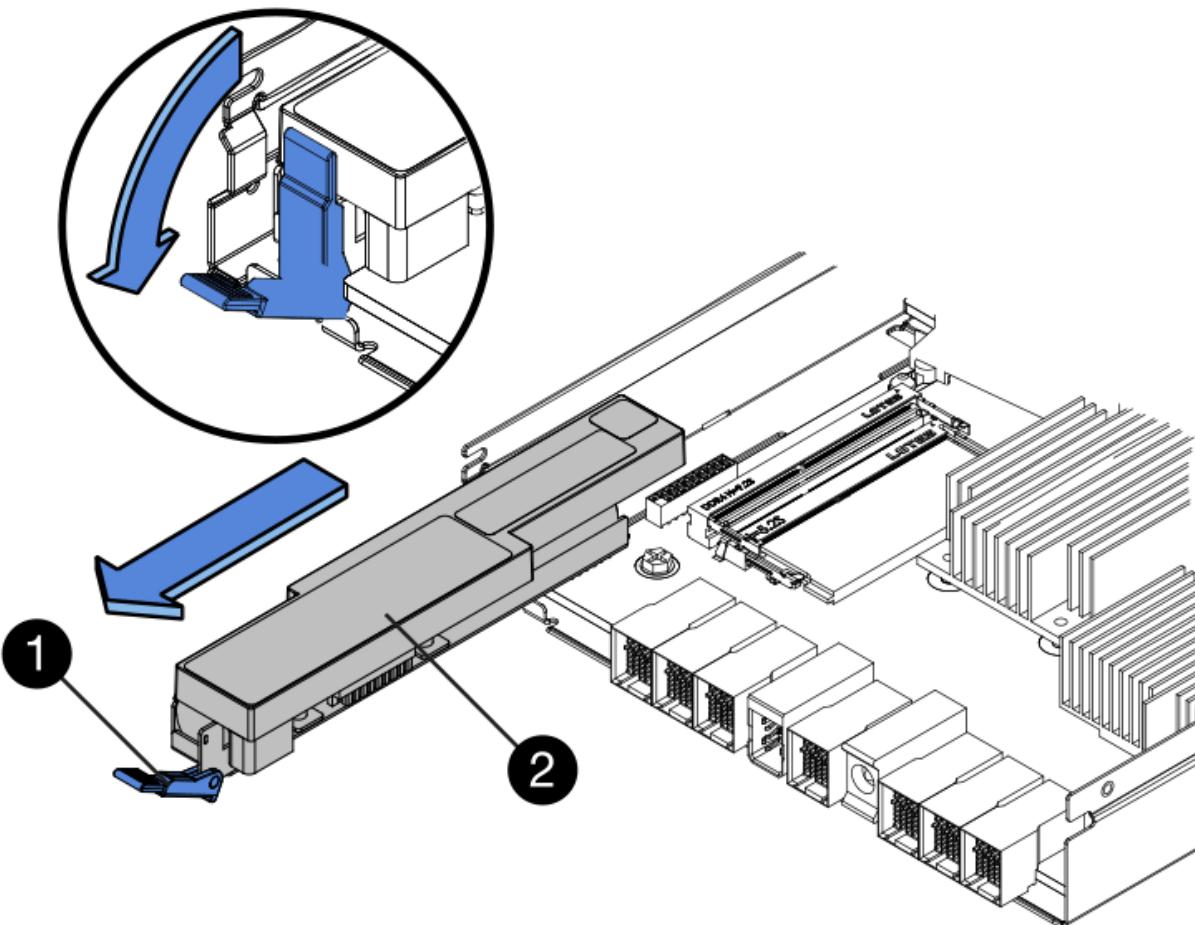
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active

(2) Battery

3. Locate the blue release latch for the battery.
4. Unlatch the battery by pushing the release latch down and away from the controller canister.



(1) Battery release latch

(2) Battery

5. Lift up on the battery, and slide it out of the controller canister.
6. Follow the appropriate procedures for your location to recycle or dispose of the failed battery.



To comply with International Air Transport Association (IATA) regulations, never ship a lithium battery by air unless it is installed within the controller shelf.

7. Go to [Install new battery](#).

Install new E2800 battery

After removing the failed battery, you can install the new one.

What you'll need

- The replacement battery.
- A flat, static-free surface.

Steps

1. Unpack the new battery, and set it on a flat, static-free surface.



To comply with IATA safety regulations, replacement batteries are shipped with a state of charge (SoC) of 30 percent or less. When you reapply power, keep in mind that write caching will not resume until the replacement battery is fully charged and it has completed its initial learn cycle.

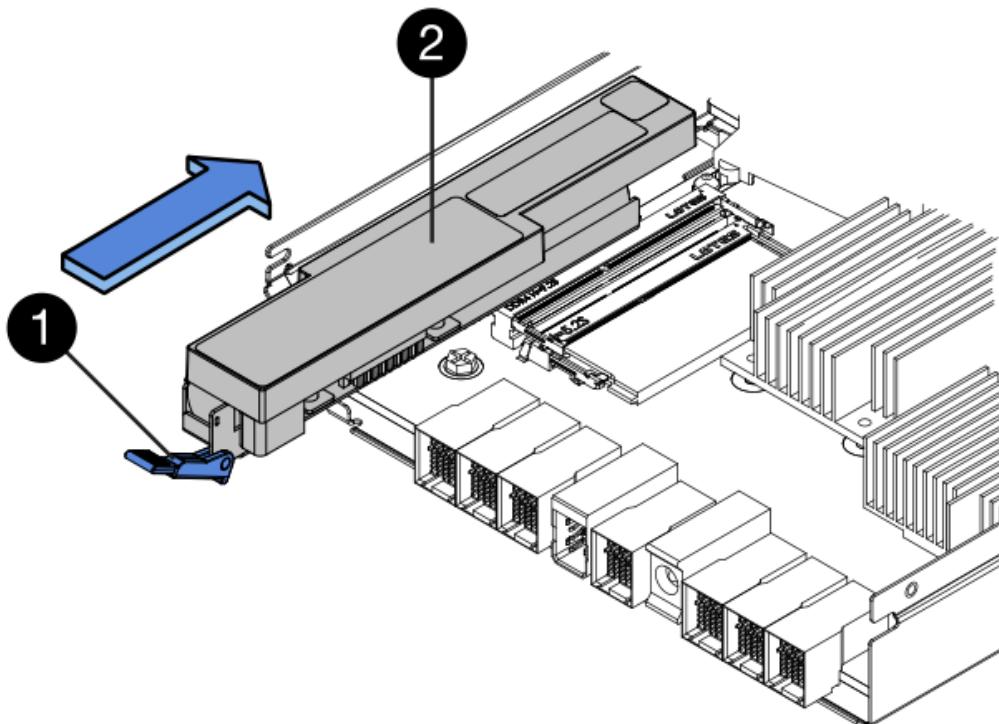
2. Orient the controller canister so that the slot for the battery faces toward you.

3. Insert the battery into the controller canister at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller canister and slide the top of the battery beneath the small alignment pin on the left side of the canister.

4. Move the battery latch up to secure the battery.

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



(1) Battery release latch

(2) Battery

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



Possible hardware damage — The metal flange at the front of the battery must be completely inserted into the slot on the controller canister (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage to the controller when you apply power.

- **Correct** — The battery's metal flange is completely inserted in the slot on the controller:



- ° **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



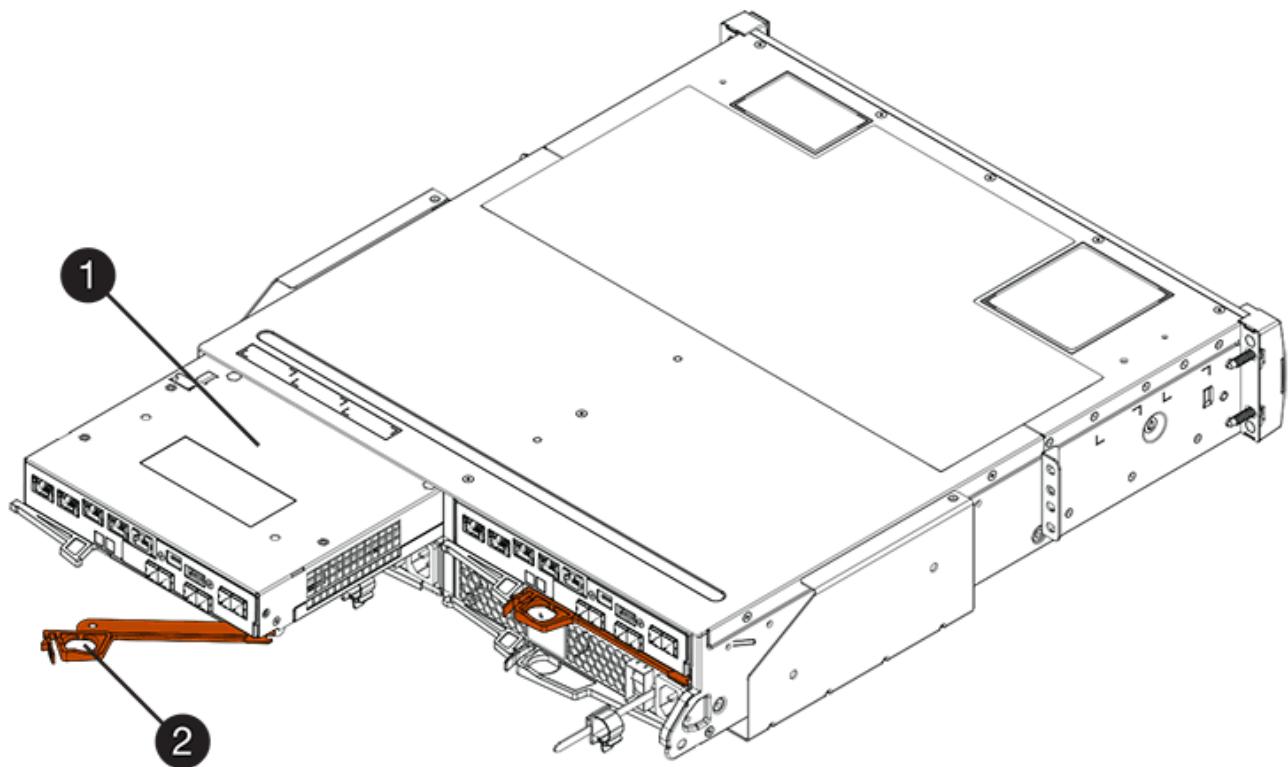
6. Go to [Re-install E2800 controller canister](#).

Re-install E2800 controller canister

Reinstall the controller canister into the controller shelf after installing the new battery.

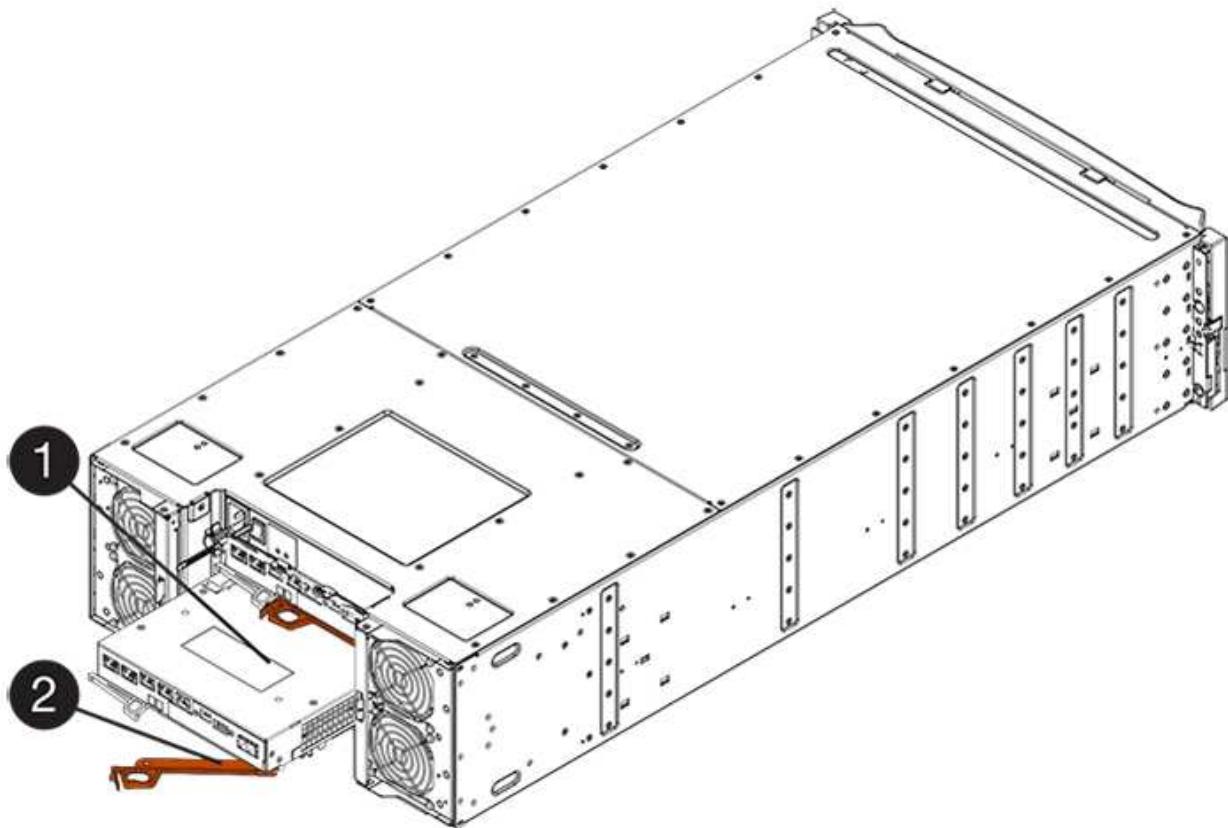
Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle



(1) Controller canister

(2) Cam handle

4. Move the cam handle to the left to lock the controller canister in place.
5. Reconnect all the cables.
6. Go to [Complete E2800 battery replacement](#).

Complete E2800 battery replacement

The steps to complete battery replacement depend on whether you have a duplex configuration (two controllers) or a simplex configuration (one controller).

- For duplex configurations, see [Place controller online \(duplex\)](#).
- For simplex configurations, see [Power up controller \(simplex\)](#).

Place controller online (duplex)

Place the controller online to confirm the storage array is working correctly. Then, you can collect support data and resume operations.



Perform this task only if your storage array has two controllers.

Steps

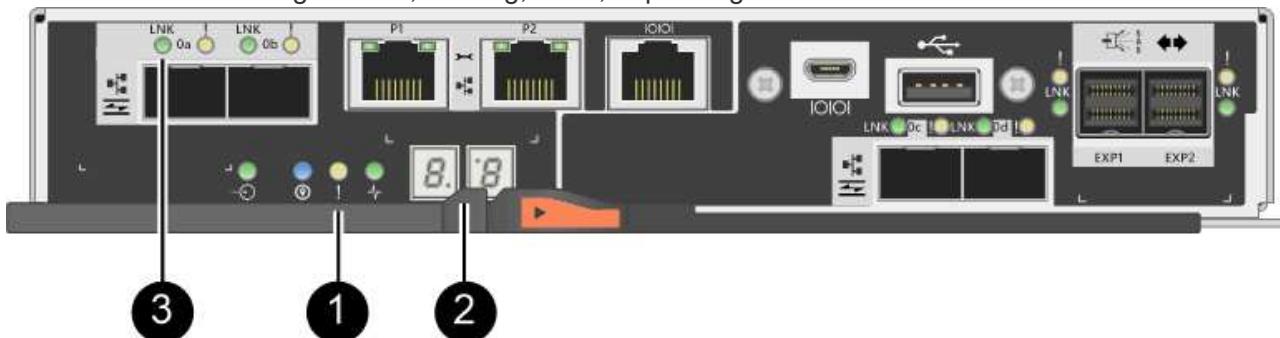
1. As the controller boots, check the controller LEDs and the seven-segment display.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS, OL, blank** to indicate that the controller is offline.
- The amber Attention LED remains lit.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) Attention LED (amber)

(2) Seven-segment display

(3) Host Link LEDs

2. Bring the controller online using SANtricity System Manager.
 - From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf**.
 - c. Select the controller you want to place online.
 - d. Select **Place Online** from the context menu, and confirm that you want to perform the operation.

The system places the controller online.

- Alternatively, you can bring the controller back online by using the following CLI commands:

For controller A: set controller [a] availability=online;

For controller B: set controller [b] availability=online;

3. When the controller is back online, confirm that its status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the battery and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the battery.



If you cannot resolve the problem, contact technical support.

4. If needed, collect support data for your storage array using SANtricity System Manager.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your battery replacement is complete. You can resume normal operations.

Power up controller (simplex)

Power up the controller shelf to confirm that it is working correctly. Then, you can collect support data and resume operations.



Perform this task only if your storage array has one controller.

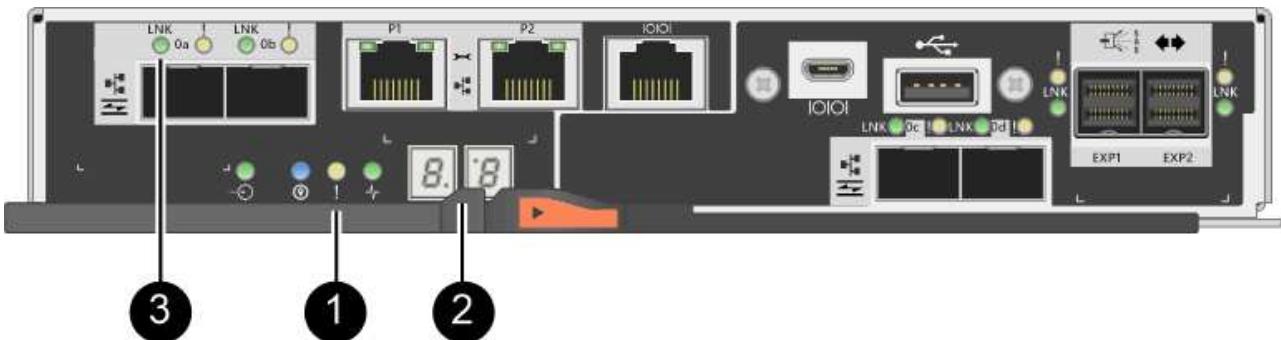
Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.

- The seven-segment display shows the repeating sequence **OS**, **Sd**, **blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
- The amber Attention LED on the controller turns on and then turns off, unless there is an error.
- The green Host Link LEDs turn on.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Attention LED (amber)

(2) Seven-segment display

(3) Host Link LEDs

3. Confirm that the controller's status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the battery and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the battery.



If you cannot resolve the problem, contact technical support.

4. If needed, collect support data for your storage array using SANtricity System Manager.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your battery replacement is complete. You can resume normal operations.

Controllers

Requirements for E2800 controller replacement

Before you replace or add an E2800 controller, review the requirements and considerations.

Each controller canister contains a controller card, a battery, and an optional host interface card (HIC). You can add a second controller to a simplex configuration or replace a failed controller.

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.)

Requirements for adding second controller

You can add a second controller canister to the simplex version of the following controller shelves:

- E2812 controller shelf
- E2824 controller shelf
- EF280 flash array

The figures show an example controller shelf before adding a second controller (one controller canister and a controller blank) and after adding a second controller (two controller canisters).



The figures show example controller canisters; the host ports on your controller canisters might be different.

Before you add a second controller, you must have:

- A new controller canister with the same part number as the currently installed controller canister.
- A new HIC that is identical to the HIC in the currently installed controller canister (only necessary if the currently installed controller canister includes a host interface card).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new controller ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- Multipath driver installed on the host so that you can use both controllers. Refer to the [Linux express](#)

[configuration](#), [Windows express configuration](#), or [VMware express configuration](#) for instructions.

- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- Labels to identify the new cables.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Optionally, you can use the command line interface (CLI) to perform some of the procedures. If you do not have access to the CLI, you can do one of the following:

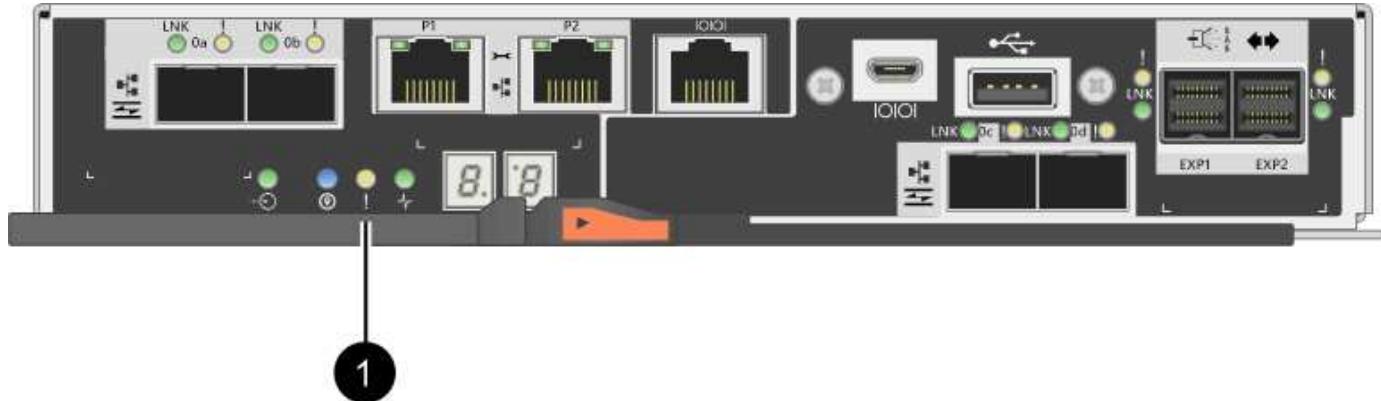
- For **SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
- For **SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Requirements for replacing controller

When you replace a failed controller canister, you must remove the battery and HIC, if one is installed, from the original controller canister, and install them in the replacement controller canister.

You can determine if you have a failed controller canister in two ways:

- The Recovery Guru in SANtricity System Manager directs you to replace the controller canister.
- The amber Attention LED on the controller canister is on, indicating that the controller has a fault.



(1) Attention LED



The figure shows an example controller canister; the host ports on your controller canister might be different.

Before you replace a controller, you must have:

- A replacement controller canister with the same part number as the controller canister you are replacing.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.

- #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Optionally, you can use the command line interface (CLI) to perform some of the procedures. If you do not have access to the CLI, you can do one of the following:

- **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
- **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Duplex configuration requirements

If the controller shelf has two controllers (duplex configuration), you can replace a controller canister while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:

- The second controller canister in the shelf has Optimal status.
- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.

Simplex configuration requirements

If you have only one controller canister (simplex configuration), data on the storage array will not be accessible until you replace the controller canister. You must stop host I/O operations and power down the storage array.

Add second controller canister in E2800

You can add a second controller canister in the E2800 array.

About this task

This task describes how to add a second controller canister to the simplex version of either a E2812 controller shelf, E2824 controller shelf, or EF280 flash array. This procedure is also referred to as a simplex-to-duplex conversion, which is an online procedure. You can access data on the storage array while you perform this procedure.

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.)

What you'll need

- A new controller canister with the same part number as the currently installed controller canister. (See step 1 to verify the part number.)
- A new HIC that is identical to the HIC in the currently installed controller canister (only necessary if the currently installed controller canister includes a host interface card).
- An ESD wristband, or take other antistatic precautions.

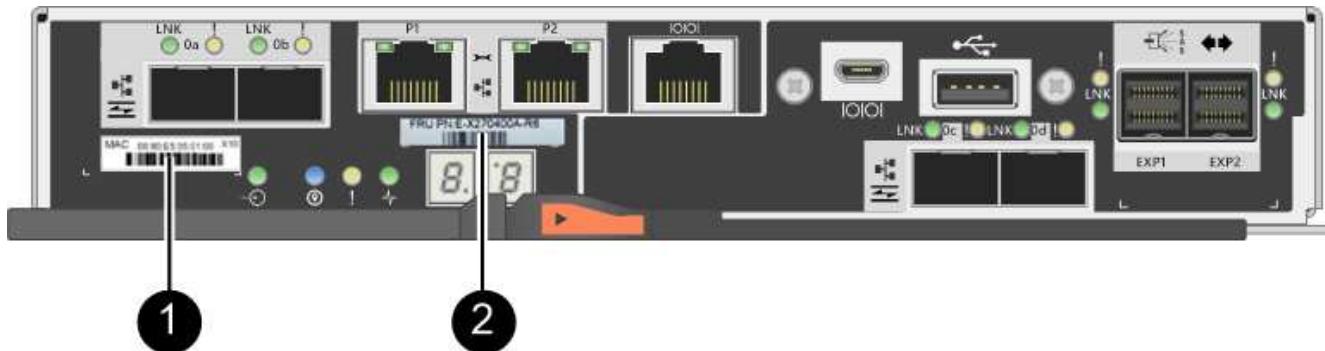
- A #1 Phillips screwdriver.
- Labels to identify the new cables. For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new controller ports.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Verify the new controller's part number

Confirm that the new controller has the same part number as the currently installed controller.

Steps

1. Unpack the new controller canister, and set it on a flat, static-free surface.
2. Locate the MAC address and FRU part number labels on the back of the controller canister.



(1) MAC address: The MAC address for management port 1 ("P1"). If you used DHCP to obtain the original controller's IP address, you will need this address to connect to the new controller.

(2) FRU part number: This number must match the replacement part number for the currently installed controller.

3. From SANtricity System Manager, locate the replacement part number for the installed controller canister.
 - Select **Hardware**.
 - Locate the controller shelf, which is marked with the controller icon .
 - Click the controller icon.
 - Select the controller, and click **Next**.
 - On the **Base** tab, make a note of the **Replacement Part Number** for the controller.
4. Confirm that the replacement part number for the installed controller is the same as the FRU part number for the new controller.



Possible loss of data access — If the two part numbers are not the same, do not attempt this procedure. In addition, if the original controller canister includes a host interface card (HIC), you must install an identical HIC into the new controller canister. The presence of mismatched controllers or HICs will cause the new controller to lock down when you bring it online.

Step 2: Install host interface card

If the currently installed controller includes a HIC, you must install the same model of host interface card (HIC) in the second controller canister.

Steps

1. Unpack the new HIC, and confirm it is identical to the existing HIC.



Possible loss of data access — The HICs installed in the two controller canisters must be identical. If the replacement HIC is not identical to the HIC you are replacing, do not attempt this procedure. The presence of mismatched HICs will cause the new controller to lock down when it comes online.

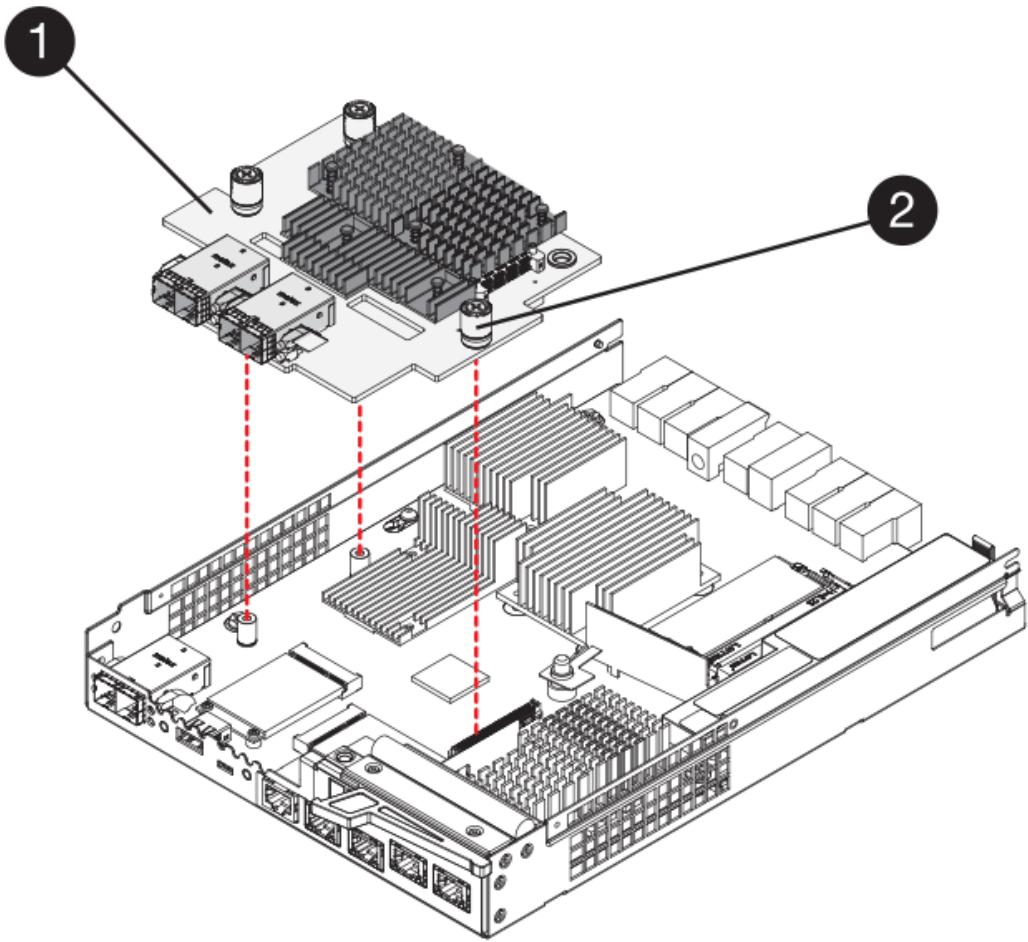
2. Turn the new controller canister over, so that the cover faces up.
3. Press the button on the cover, and slide the cover off.
4. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the controller canister, and remove the faceplate.
5. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

6. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



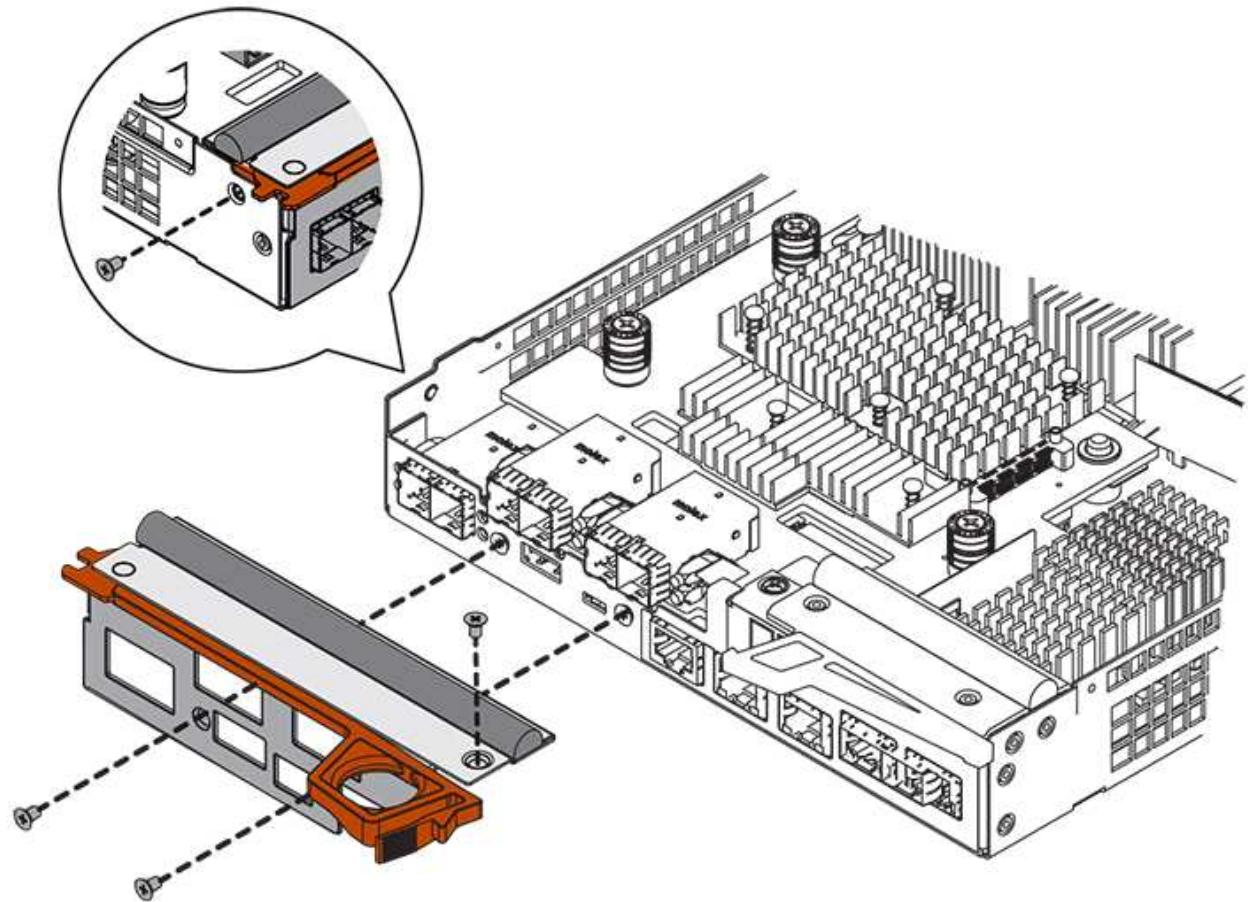
(1) *Host interface card*

(2) *Thumbscrews*

7. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

8. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.



9. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
10. Set the controller canister aside until you are ready to install it.

Step 3: Collect support data

Collect support data before and after replacing a component to ensure you can send a full set of logs to technical support in case the replacement does not resolve the problem.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Collect support data for your storage array using SANtricity System Manager.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

3. 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.



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.

Step 4: Change configuration to duplex

Before adding a second controller to the controller shelf, you must change the configuration to duplex by installing a new NVSRAM file and using the command line interface to set the storage array to duplex. The duplex version of the NVSRAM file is included with the download file for SANtricity OS Software (controller firmware).

Steps

1. Download the latest NVSRAM file from the NetApp Support site to your management client.
 - a. From SANtricity System Manager, select **Support > Upgrade Center**. In the area labeled “SANtricity OS Software upgrade,” click **NetApp SANtricity OS Downloads**.
 - b. From the NetApp Support site, select **E-Series SANtricity OS Controller software**.
 - c. Follow the online instructions to select the version of NVSRAM you want to install, and then complete the file download. Be sure to select the duplex version of the NVSRAM (the file has “D” near the end of its name).

The file name will be similar to: **N290X-830834-D01.dlp**

2. Upgrade the files using SANtricity System Manager.



Risk of data loss or risk of damage to the storage array — Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

You can cancel the operation during the pre-upgrade health check, but not during transferring or activating.

- From SANtricity System Manager:
 - a. Under **SANtricity OS Software upgrade**, click **Begin Upgrade**.
 - b. Next to **Select Controller NVSRAM file**, click **Browse**, and then select the NVSRAM file you downloaded.
 - c. Click **Start**, and then confirm that you want to perform the operation.

The upgrade begins and the following occurs:

- The pre-upgrade health check begins. If the pre-upgrade health check fails, use the Recovery Guru or contact technical support to resolve the problem.
- The controller files are transferred and activated. The time required depends on your storage array configuration.

- The controller reboots automatically to apply the new settings.
- Alternatively, you can use the following CLI command to perform the upgrade:

```
download storageArray NVSRAM file="filename"  
healthCheckMeOverride=FALSE;
```

In this command, `filename` is the file path and the file name for duplex version of the Controller NVSRAM file (the file with “D” in its name). Enclose the file path and the file name in double quotation marks (""). For example:

```
file="C:\downloads\N290X-830834-D01.dlp"
```

3. (Optional) To see a list of what was upgraded, click **Save Log**.

The file is saved in the Downloads folder for your browser with the name, **latest-upgrade-log-timestamp.txt**.

- After upgrading controller NVSRAM, verify the following in SANtricity System Manager:
 - Go to the Hardware page, and verify that all components appear.
 - Go to the Software and Firmware Inventory dialog box (go to **Support > Upgrade Center**, and then click the link for **Software and Firmware Inventory**). Verify the new software and firmware versions.
 - When you upgrade controller NVSRAM, any custom settings that you have applied to the existing NVSRAM are lost during the process of activation. You must apply the custom settings to the NVSRAM again after the process of activation is complete.
4. Change the storage array setting to duplex using CLI commands. To use CLI, you can either open a command prompt if you downloaded the CLI package or you can open the Enterprise Management Window (EMW) if you have Storage Manager installed.
- From a command prompt:
 - a. Use the following command to switch the array from simplex to duplex:

```
set storageArray redundancyMode=duplex;
```

- b. Use the following command to reset the controller.

```
reset controller [a];
```

- From the EMW interface:
 - a. Select the storage array.
 - b. Select **Tools > Execute Script**.
 - c. Type the following command in the text box.

```
set storageArray redundancyMode=duplex;
```

- d. Select **Tools > Verify and Execute**.
- e. Type the following command in the text box.

```
reset controller [a];
```

- f. Select **Tools > Verify and Execute**.

After the controller reboots, an “alternate controller missing” error message is displayed. This message indicates that controller A has been successfully converted to duplex mode. This message persists until you install the second controller and connect the host cables.

Step 5: Remove the controller blank

Remove the controller blank before you install the second controller. A controller blank is installed in controller shelves that have only one controller.

Steps

1. Squeeze the latch on the cam handle for the controller blank until it releases, and then open the cam handle to the right.
2. Slide the blank controller canister out of the shelf and set it aside.

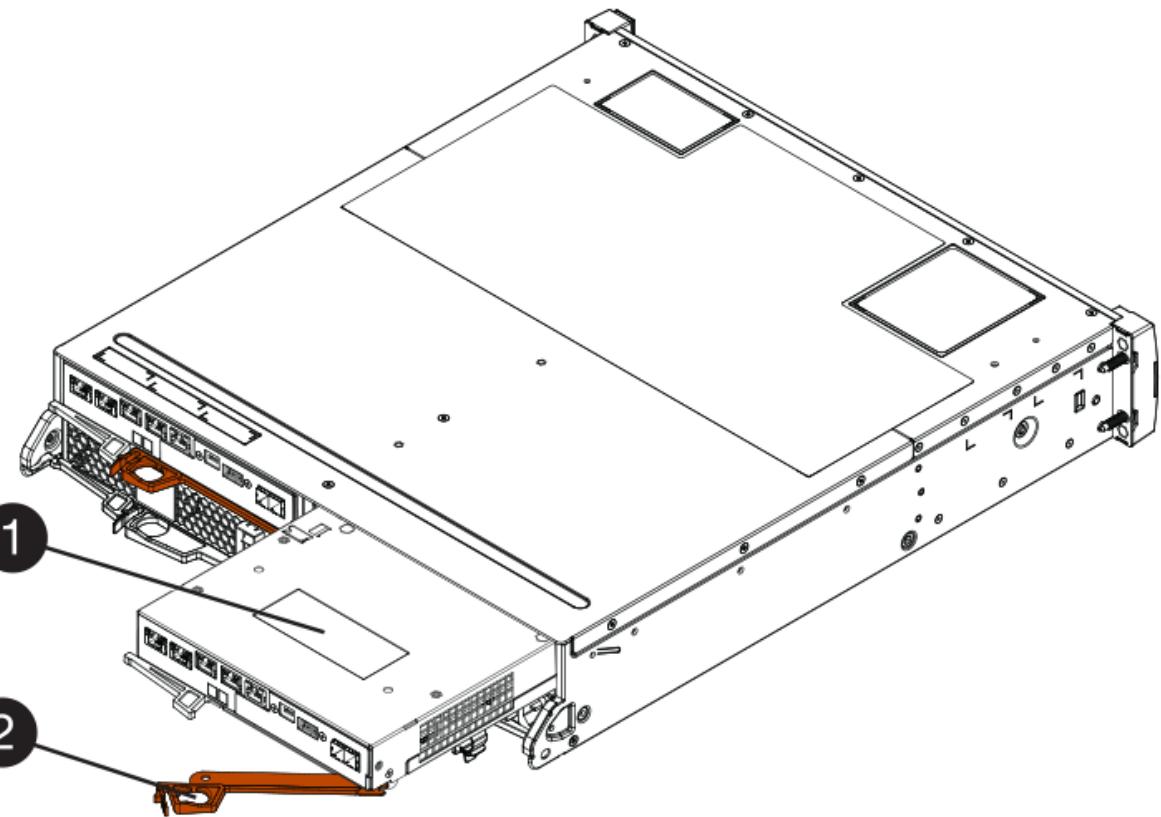
When you remove the controller blank, a flap swings into place to block the empty bay.

Step 6: Install second controller canister

Install a second controller canister to change a simplex configuration to a duplex configuration.

Steps

1. Turn the controller canister over, so that the removable cover faces down.
2. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle

3. Move the cam handle to the left to lock the controller canister in place.
4. Insert any SFP+ transceivers, and connect cables to the new controller.

Step 7: Complete adding a second controller

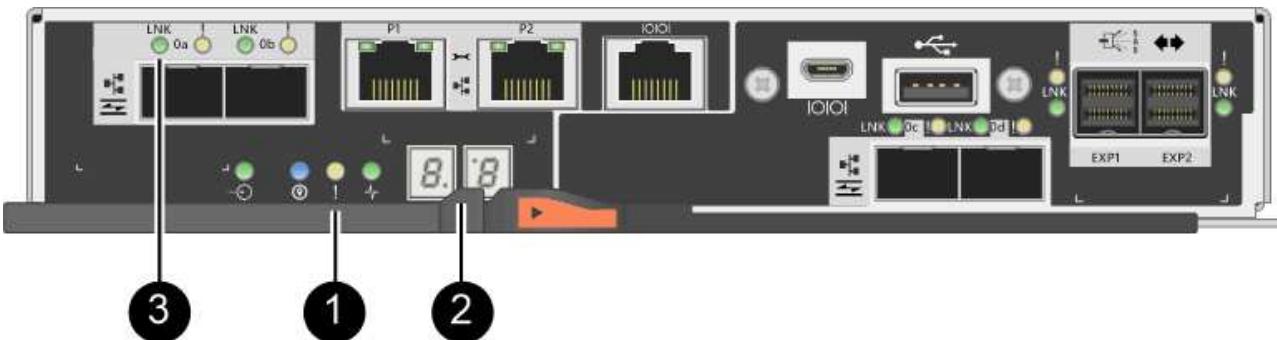
Complete the process of adding a second controller by confirming that it is working correctly, reinstall the duplex NVRAM file, distribute volumes between the controllers, and collect support data.

Steps

1. As the controller boots, check the controller LEDs and the seven-segment display.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS**, **OL**, **blank** to indicate that the controller is offline.
- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) *Attention LED (amber)*

(2) *Seven-segment display*

(3) *Host Link LEDs*

- Check the codes on the controller's seven-segment display as it comes online. If the display shows one of the following repeating sequences, immediately remove the controller.

- **OE, L0, blank** (mismatched controllers)
- **OE, L6, blank** (unsupported HIC)



Possible loss of data access — If the controller you just installed shows one of these codes, and the other controller is reset for any reason, the second controller could also lock down.

- Update the array's settings from simplex to duplex with the following CLI command:

```
set storageArray redundancyMode=duplex;
```

- From SANtricity System Manager, confirm that the controller's status is Optimal.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

- Reinstall the duplex version of the NVSRAM file using SANtricity System Manager.

This step ensures that both controllers have an identical version of this file.



Risk of data loss or risk of damage to the storage array — Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.



You must install SANtricity OS software when you install a new NVSRAM file using SANtricity System Manager. If you already have the latest version of SANtricity OS software, you must reinstall that version.

- If necessary, download the latest version of the SANtricity OS software from the NetApp Support site.
- In System Manager, go to the Upgrade Center.

- c. Under **SANtricity OS Software upgrade**, click **Begin Upgrade**.
- d. Click **Browse**, and select the SANtricity OS software file.
- e. Click **Browse**, and select the Controller NVSRAM file.
- f. Click **Start**, and confirm that you want to perform the operation.

The transfer of control operation begins.

6. After the controllers reboot, optionally distribute volumes between controller A and the new controller B.
 - a. Select **Storage > Volumes**.
 - b. From the All Volumes tab, select **More > Change Ownership**.
 - c. Type the following command in the text box: change ownership

The Change Ownership button is enabled.

- d. For each volume you want to redistribute, select **Controller B** from the **Preferred Owner** list.

Change Volume Ownership

X

Changing a volume's preferred controller while an application is using it will cause I/O errors UNLESS:

- The volumes are not in use, or
- There is a multi-path driver installed on all hosts using these volumes.

| Volume | Preferred Owner | Current Owner |
|--------|---|---------------|
| 3 | Controller B Controller A Controller B Controller C | Controller A |
| SQL_16 | Controller A Controller B Controller B Controller C | Controller B |
| SQL_15 | Controller A Controller B Controller C | Controller A |
| SQL_17 | Controller B Controller A Controller C | Controller B |

Type CHANGE OWNERSHIP to confirm that you want to perform this operation.

Change Ownership
Cancel

e. Click **Change Ownership**.

When the process is complete, the Change Volume Ownership dialog shows the new values for **Preferred Owner** and **Current Owner**.

7. Collect support data for your storage array using SANtricity System Manager.

a. Select **Support > Support Center > Diagnostics**.

b. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

The process of adding a second controller is complete. You can resume normal operations.

Replace controller in E2800 duplex configuration

You can replace a controller canister in a duplex (two-controller) configuration, for the following controller shelves:

- E2812 controller shelf
- E2824 controller shelf
- E2860 controller shelf
- EF280 flash array

About this task

Each controller canister contains a controller card, a battery, and an optional host interface card (HIC). When you replace a controller canister, you must remove the battery and HIC, if one is installed, from the original controller canister, and install them in the replacement controller canister.

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.)

What you'll need

- A replacement controller canister with the same part number as the controller canister you are replacing. (See step 1 to verify the part number.)
- An ESD wristband, or you have taken other antistatic precautions.
- #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace controller (duplex)

Prepare to replace the controller by verifying that the replacement controller canister has the correct FRU part

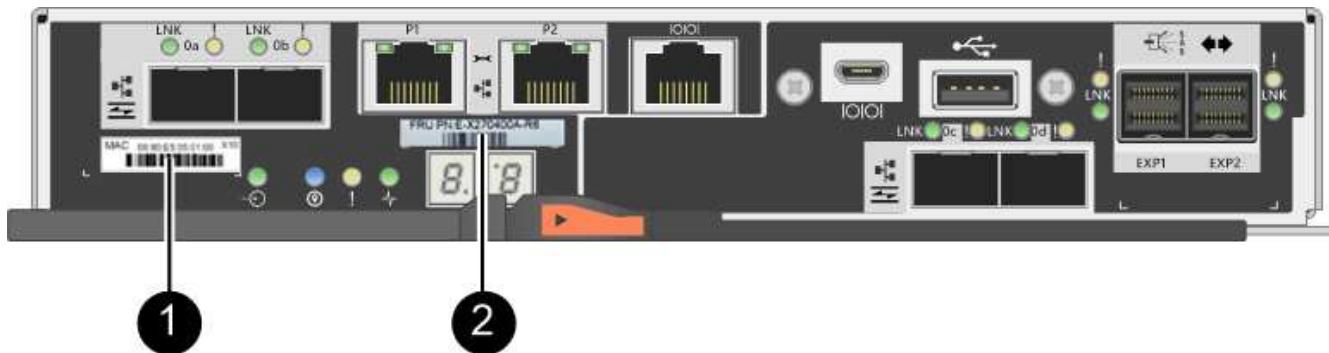
number, backing up the configuration, and collecting support data. If the controller is still online, you must take it offline.

Steps

1. Unpack the new controller canister, and set it on a flat, static-free surface.

Save the packing materials to use when shipping the failed controller canister.

2. Locate the MAC address and FRU part number labels on the back of the controller canister.



(1) MAC address: The MAC address for management port 1 ("P1"). If you used DHCP to obtain the original controller's IP address, you need this address to connect to the new controller.

(2) FRU part number: This number must match the replacement part number for the currently installed controller.

3. From SANtricity System Manager, locate the replacement part number for the controller canister you are replacing.

When a controller has a fault and needs to be replaced, the replacement part number is displayed in the Details area of the Recovery Guru. If you need to find this number manually, follow these steps:

- Select **Hardware**.
 - Locate the controller shelf, which is marked with the controller icon
 - Click the controller icon.
 - Select the controller, and click **Next**.
 - On the **Base** tab, make a note of the **Replacement Part Number** for the controller.
4. Confirm that the replacement part number for the failed controller is the same as the FRU part number for the replacement controller.



Possible loss of data access — If the two part numbers are not the same, do not attempt this procedure. In addition, if the failed controller canister includes a host interface card (HIC), you must install that HIC into the new controller canister. The presence of mismatched controllers or HICs will cause the new controller to lock down when you bring it online.

5. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - Select **Support > Support Center > Diagnostics**.
 - Select **Collect Configuration Data**.
 - Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

6. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

7. If the controller is not already offline, take it offline now using SANtricity System Manager.

- From SANtricity System Manager:
 - Select **Hardware**.
 - If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - Select the controller that you want to place offline.
 - From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

- Alternatively, you can take the controllers offline by using the following CLI commands:

For controller A: set controller [a] availability=offline

For controller B: set controller [b] availability=offline

8. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

9. Select **Recheck** from the Recovery Guru, and confirm that the **OK to remove** field in the Details area displays **Yes**, indicating that it is safe to remove this component.

Step 2: Remove failed controller (duplex)

Replace the failed canister with a new one.

Step 2a: Remove controller canister (duplex)

Remove the failed controller canister so you can replace it with a new one.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



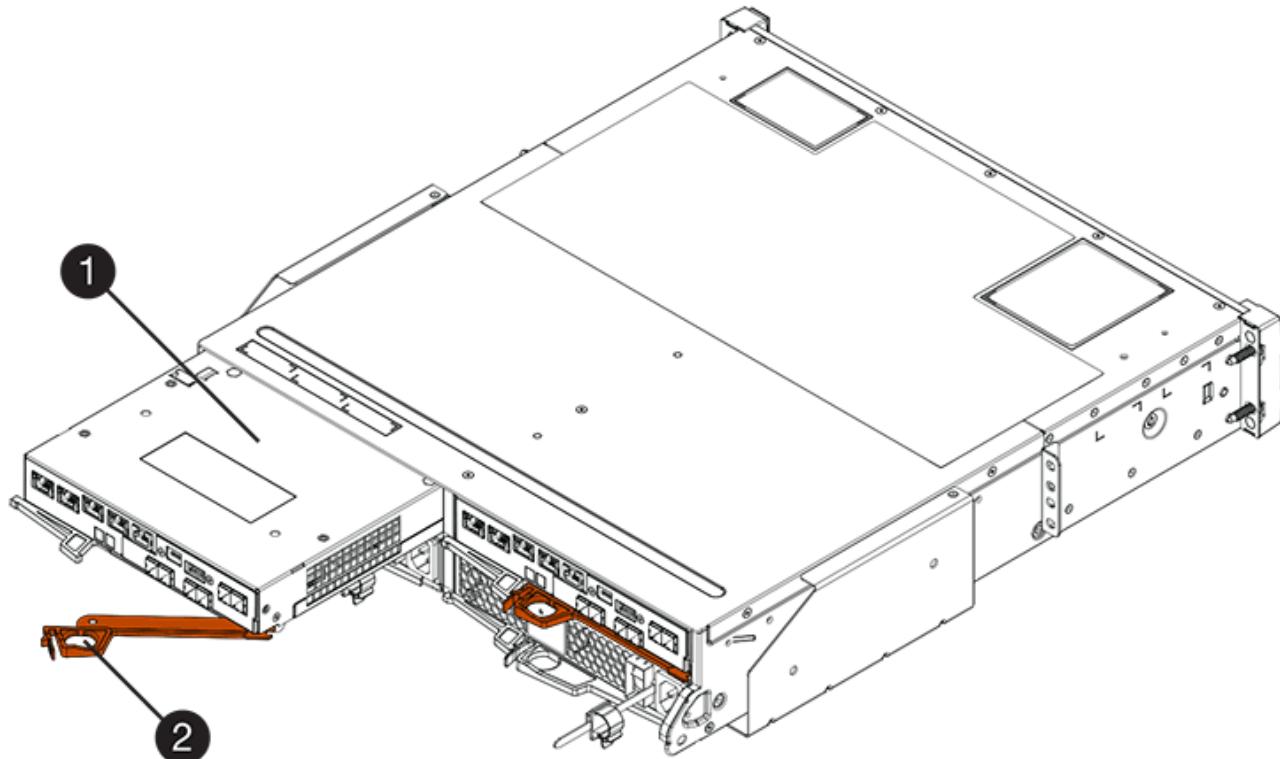
To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

4. If the controller canister has a HIC that uses SFP+ transceivers, remove the SFPs.

Because you must remove the HIC from the failed controller canister, you must remove any SFPs from the HIC ports. However, you can leave any SFPs installed in the baseboard host ports. When you reconnect the cables, you can move those SFPs to the new controller canister.

5. Confirm that the Cache Active LED on the back of the controller is off.
6. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

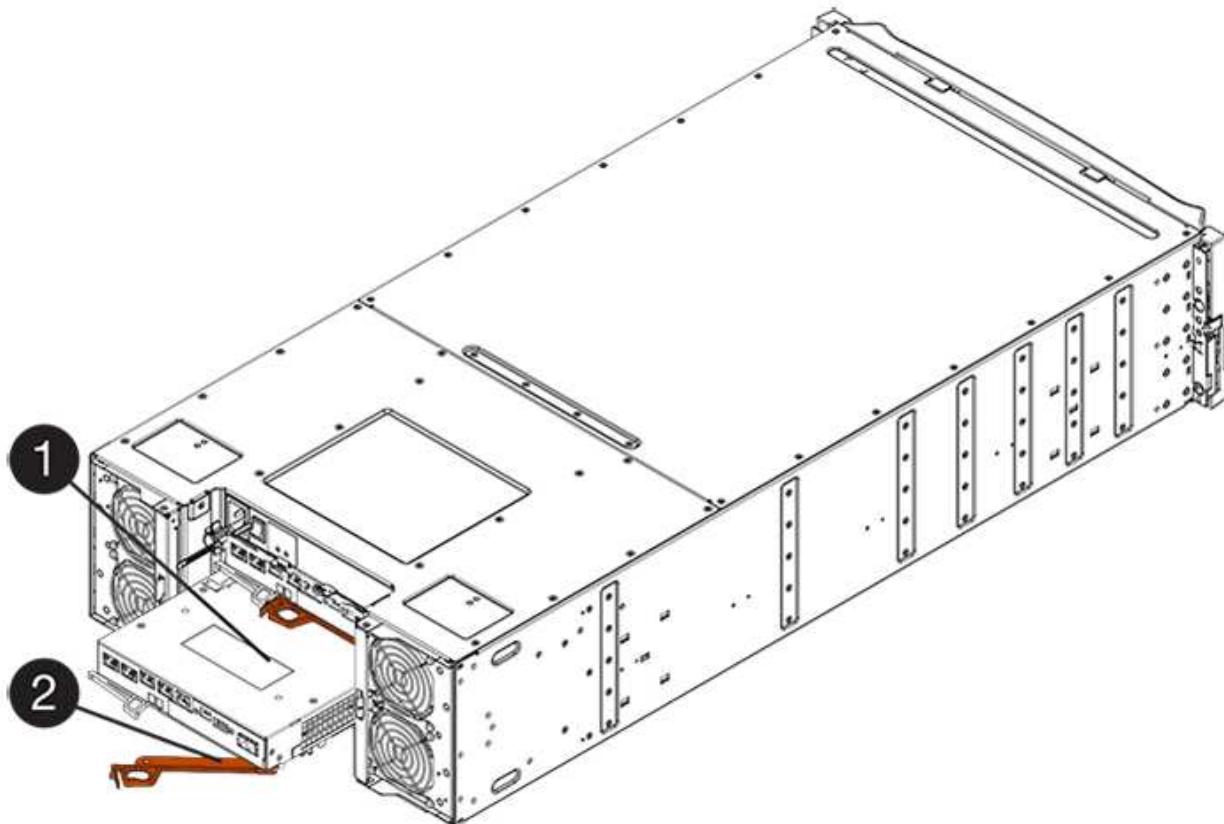
The following figure is an example of an E2812 controller shelf, E2824 controller shelf, or EF280 flash array:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

7. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E2812 controller shelf, E2824 controller shelf, or EF280 flash array, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

8. Turn the controller canister over, so that the removable cover faces up.

9. Place the controller canister on a flat, static-free surface.

Step 2b: Remove battery (duplex)

Remove the battery so you can install the new controller.

Steps

1. Remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

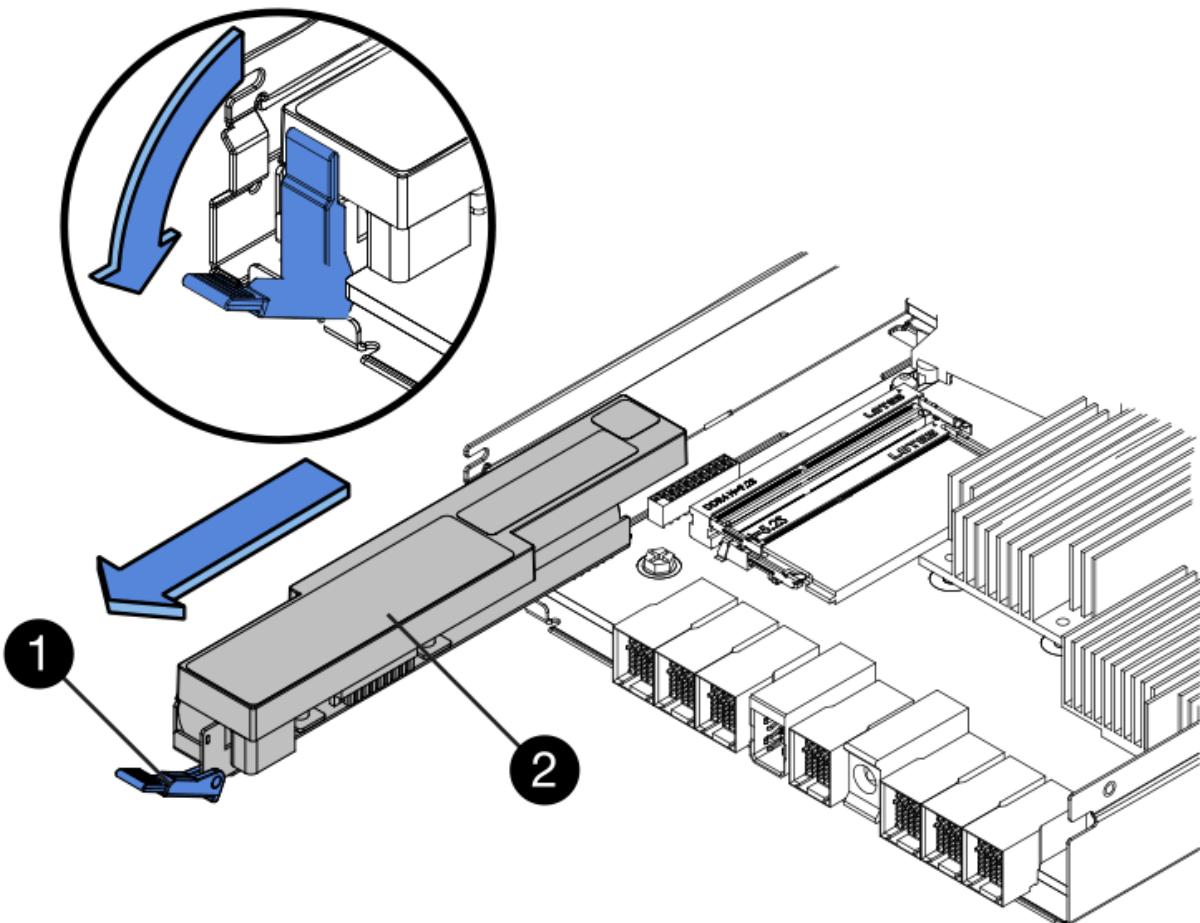
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active LED

(2) Battery

3. Locate the blue release latch for the battery.
4. Unlatch the battery by pushing the release latch down and away from the controller canister.



(1) *Battery release latch*

(2) *Battery*

5. Lift up on the battery, and slide it out of the controller canister.

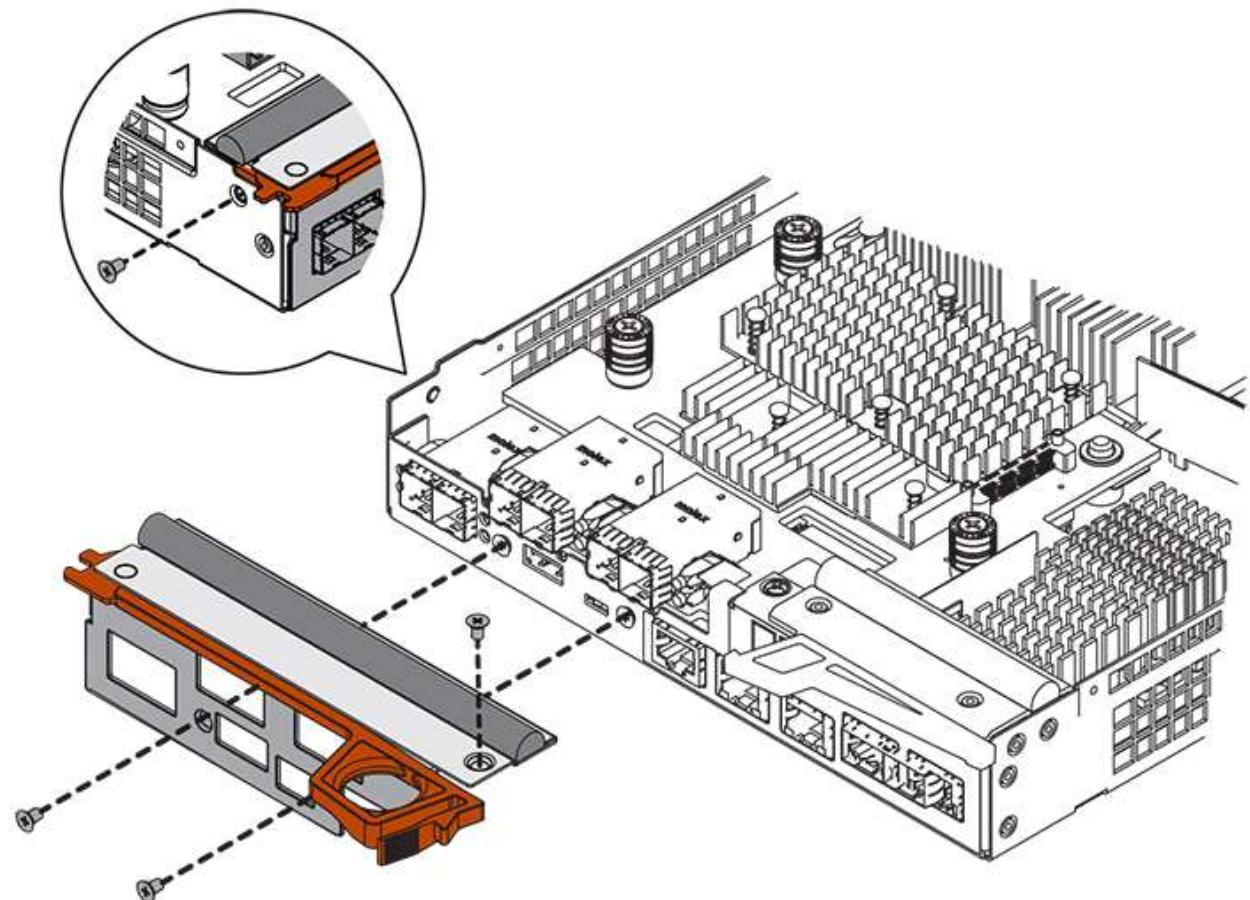
Step 2c: Remove host interface card (duplex)

If the controller canister includes a host interface card (HIC), you must remove the HIC from the original controller canister, so you can reuse it in the new controller canister.

Steps

1. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller canister.

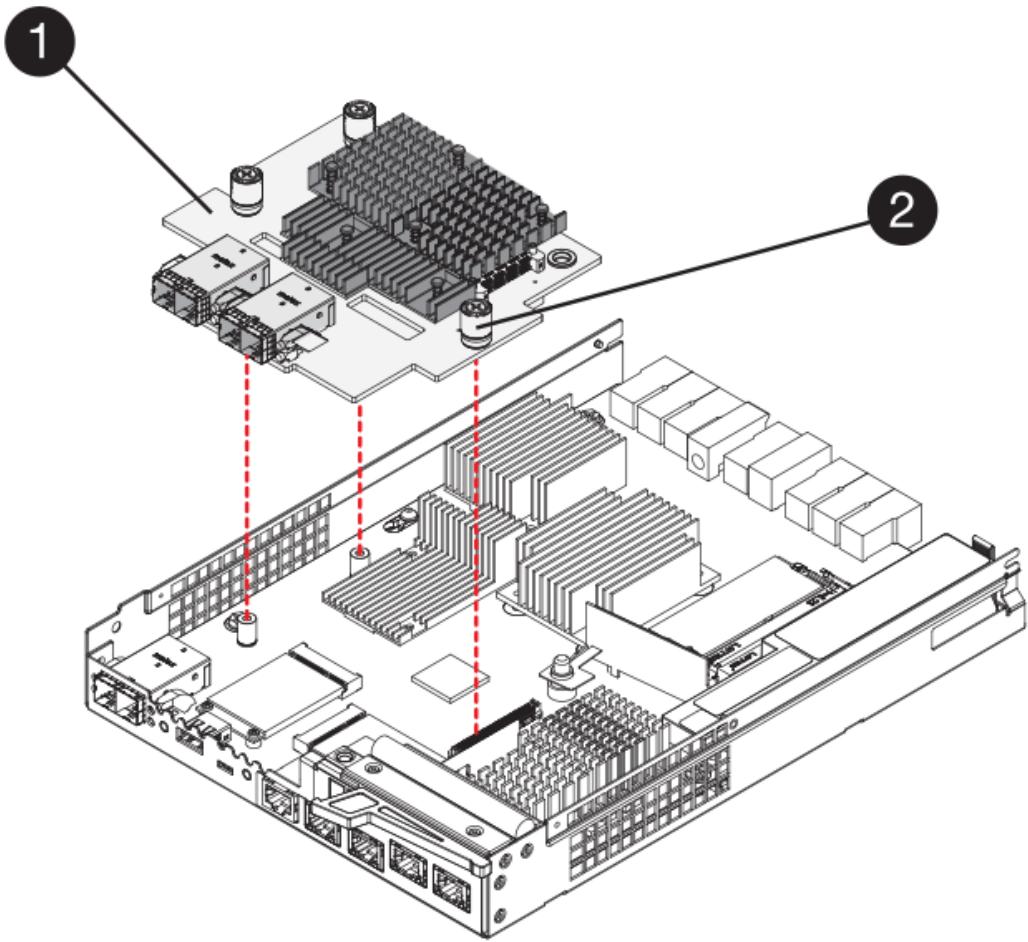
There are four screws: one on the top, one on the side, and two on the front.



2. Remove the HIC faceplate.
3. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
4. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



(1) *Host interface card (HIC)*

(2) *Thumbscrews*

5. Place the HIC on a static-free surface.

Step 3: Install new controller (duplex)

Install a new controller canister to replace the failed one. Perform this task only if your storage array has two controllers (duplex configuration).

Step 3a: Install battery (duplex)

You must install the battery into the replacement controller canister. You can install the battery that you removed from the original controller canister or install a new battery that you ordered.

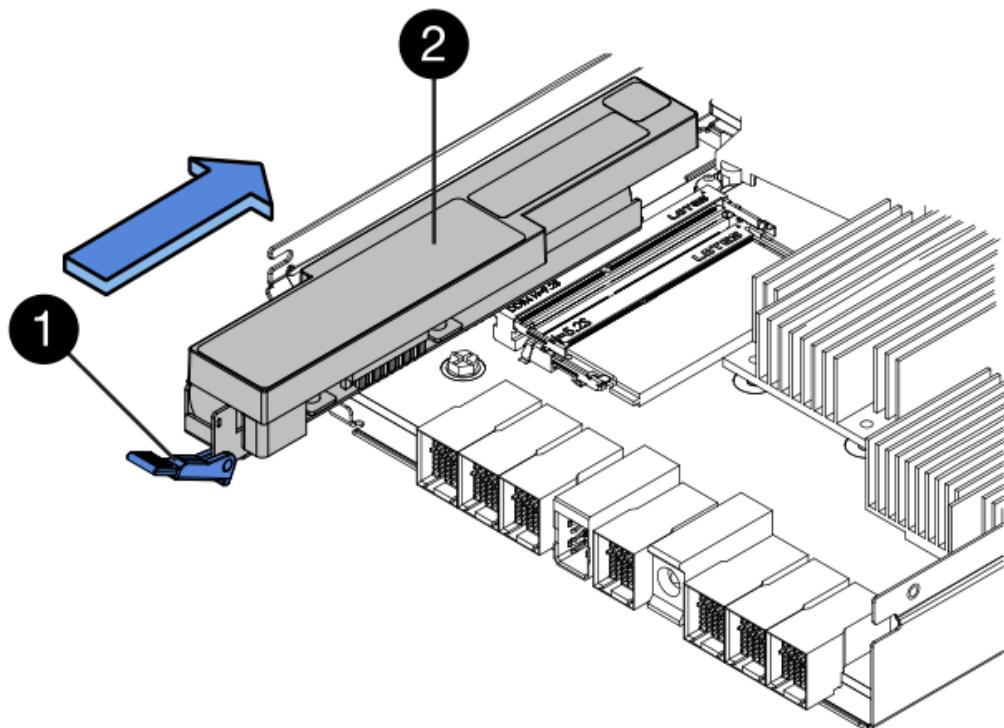
Steps

1. Turn the replacement controller canister over, 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 controller canister at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller canister and slide the top of the battery beneath the small alignment pin on the left side of the canister.

5. Move the battery latch up to secure the battery.

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



(1) Battery release latch

(2) Battery

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



Possible hardware damage — The metal flange at the front of the battery must be completely inserted into the slot on the controller canister (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage to the controller when you apply power.

- **Correct** — The battery's metal flange is completely inserted in the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



Step 3b: Install host interface card (duplex)

If you removed a HIC from the original controller canister, you must install that HIC in the new controller canister.

Steps

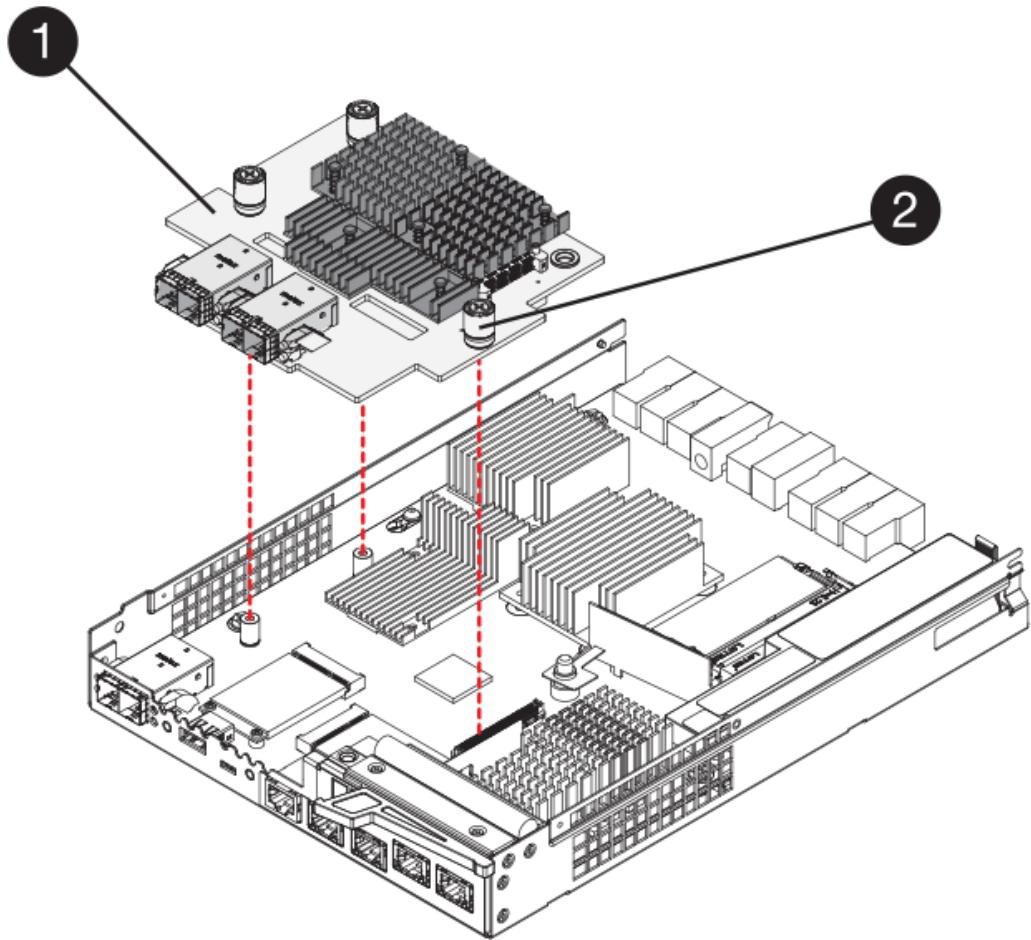
1. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller canister, and remove the faceplate.
2. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



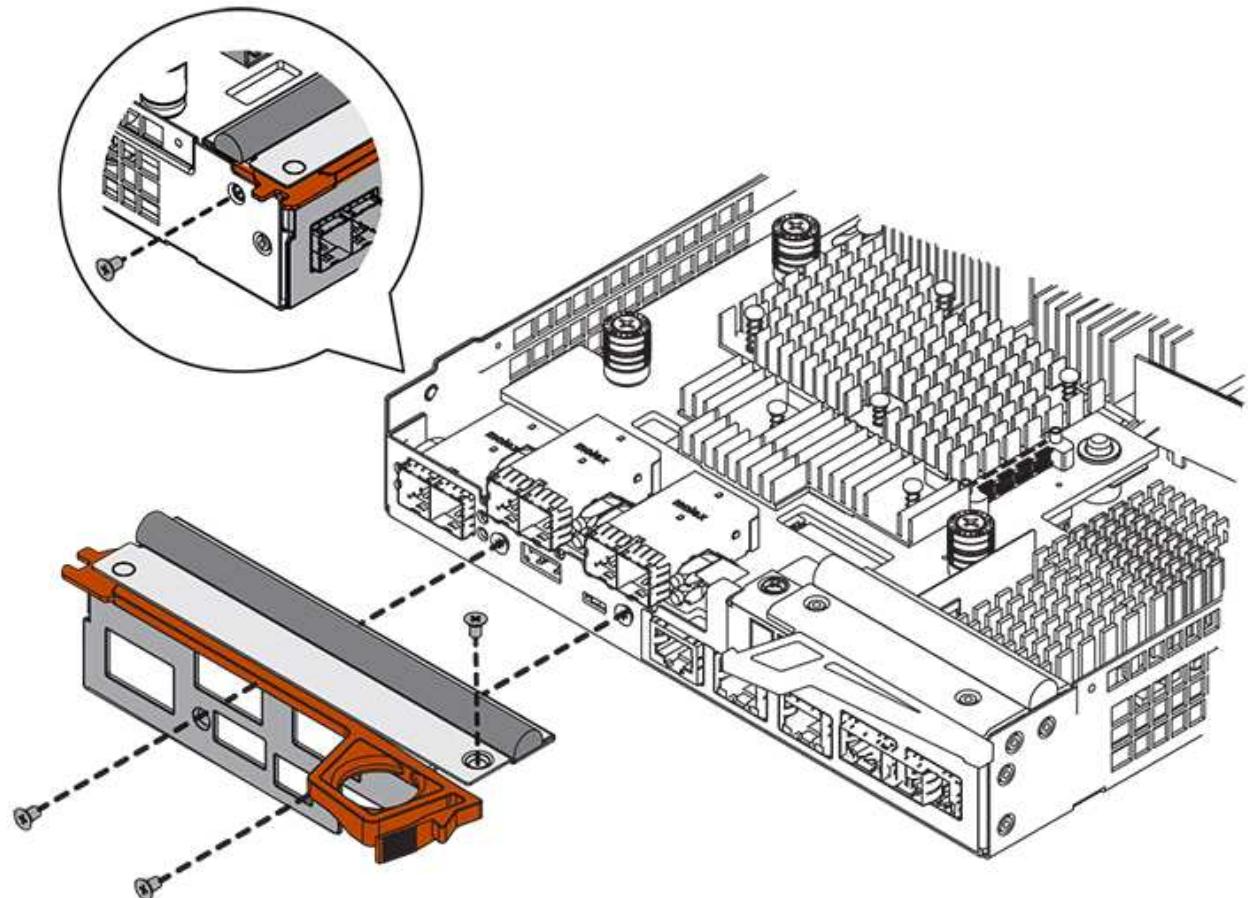
(1) *Host interface card (HIC)*

(2) *Thumbscrews*

4. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

5. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller canister to the new controller canister with four screws.

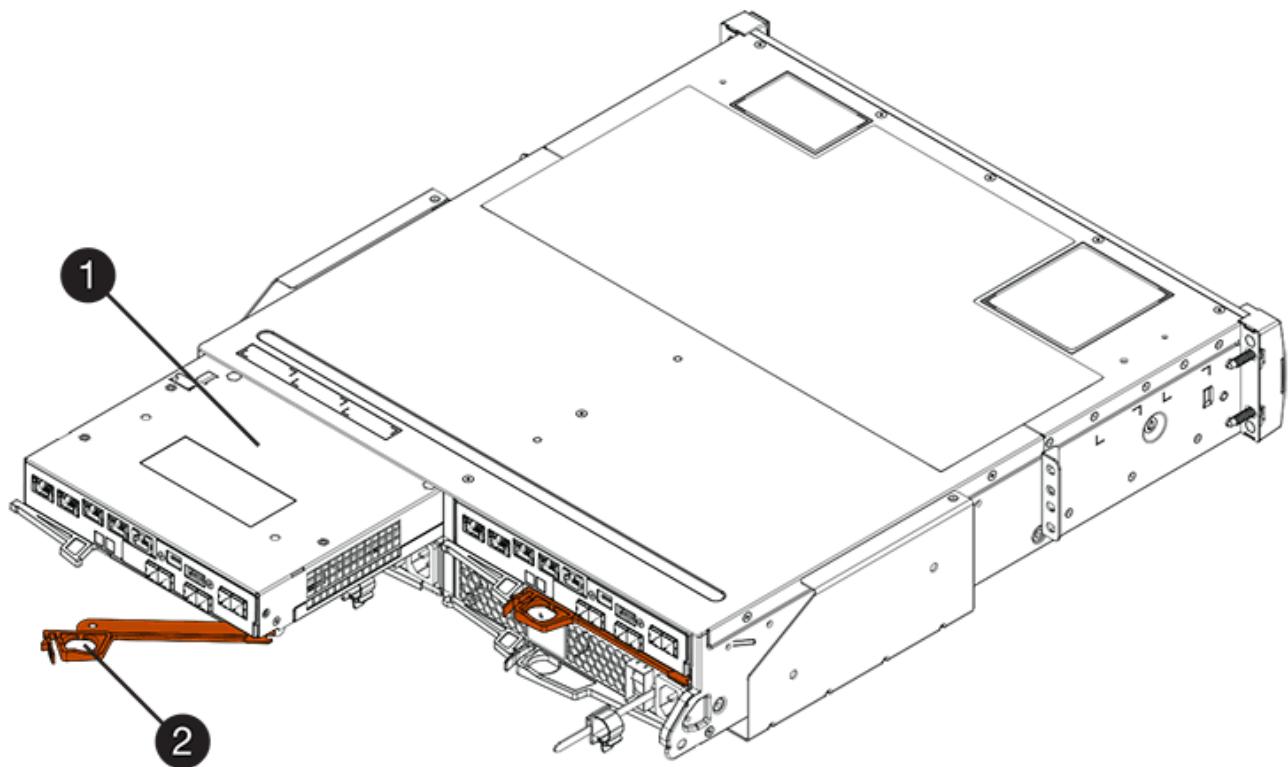


Step 3c: Install new controller canister (duplex)

After installing the battery and the host interface card (HIC), if one was initially installed, you can install the new controller canister into the controller shelf.

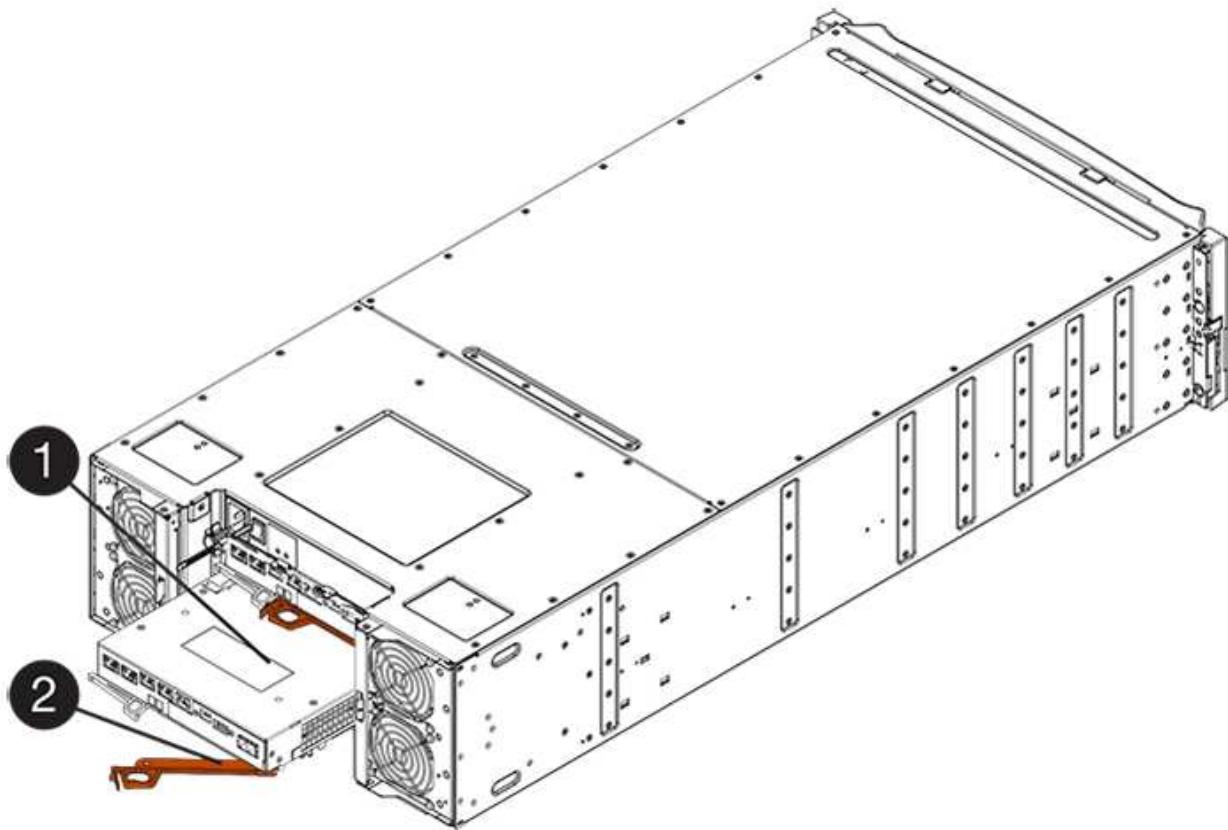
Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle



(1) Controller canister

(2) Cam handle

4. Move the cam handle to the left to lock the controller canister in place.
5. Install the SFPs from the original controller in the host ports on the new controller, and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

6. If the original controller used DHCP for the IP address, locate the MAC address on the label on the back of the replacement controller. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



If the original controller did not use DHCP for the IP address, the new controller will adopt the IP address of the controller you removed.

Step 4: Complete controller replacement (duplex)

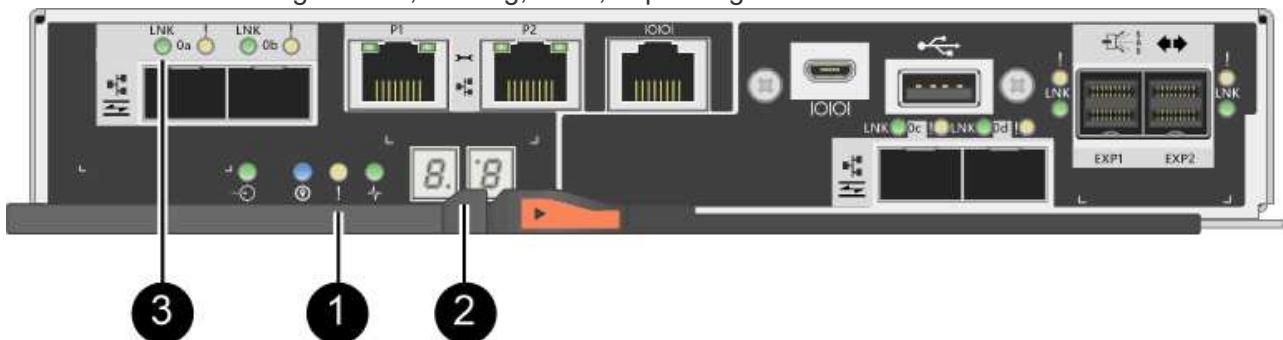
Place the controller online, collect support data, and resume operations.

Steps

1. As the controller boots, check the controller LEDs and the seven-segment display.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS, OL, blank** to indicate that the controller is offline.
- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) Attention LED (amber)

(2) Seven-segment display

(3) Host Link LEDs

2. Check the codes on the controller's seven-segment display as it comes back online. If the display shows one of the following repeating sequences, immediately remove the controller.
 - **OE, L0, blank** (mismatched controllers)
 - **OE, L6, blank** (unsupported HIC)



Possible loss of data access — If the controller you just installed shows one of these codes, and the other controller is reset for any reason, the second controller could also lock down.

- When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

- If required, redistribute all volumes back to their preferred owner using SANtricity System Manager.
 - Select **Storage > Volumes**.
 - Select **More > Redistribute volumes**.
- Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS software (controller firmware) is installed.

As needed, install the latest version.

- Collect support data for your storage array using SANtricity System Manager.
 - Select **Support > Support Center > Diagnostics**.
 - Select **Collect Support Data**.
 - Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your controller replacement is complete. You can resume normal operations.

Replace controller in E2800 simplex configuration

You can replace a failed controller canister in a simplex (single-controller) configuration, for the following controller shelves:

- E2812 controller shelf
- E2824 controller shelf
- EF280 flash array

About this task

The controller canister contains a controller card, a battery, and an optional host interface card (HIC). When you replace a failed controller canister, you must remove the battery and HIC, if one is installed, from the original controller canister, and install them in the replacement controller canister.

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.)

What you'll need

- A replacement controller canister with the same part number as the controller canister you are replacing.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace controller (simplex)

Prepare to replace a controller canister by saving the drive security key, backing up the configuration, and collecting support data. Then, you can stop host I/O operations and power down the controller shelf.

Steps

1. If possible, make a note of which version of SANtricity OS software is currently installed on the controller. Open SANtricity System Manager and select **Support > Upgrade Center > View Software and Firmware Inventory**.
2. If the Drive Security feature is enabled, be sure a saved key exists and that you know the pass phrase required to install it.



Possible loss of data access — If all drives in the storage array are security enabled, the new controller will not be able to access the storage array until you unlock the secured drives using the Enterprise Management Window in SANtricity Storage Manager.

To save the key (might not be possible, depending on the state of the controller):

- a. From SANtricity System Manager, select **Settings > System**.
 - b. Under **Drive security key management**, select **Back Up Key**.
 - c. In the **Define a pass phrase/Re-enter pass phrase** fields, enter and confirm a pass phrase for this backup copy.
 - d. Click **Backup**.
 - e. Record your key information in a secure location, and then click **Close**.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

4. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

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.



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. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

7. From the home page of SANtricity System Manager, select **View Operations in Progress**.
8. Confirm that all operations have completed before continuing with the next step.
9. Turn off both power switches on the controller shelf.
10. Wait for all LEDs on the controller shelf to turn off.
11. Select **Recheck** from the Recovery Guru, and confirm that the **OK to remove** field in the Details area displays **Yes**, indicating that it is safe to remove this component.

Data on the storage array will not be accessible until you replace the controller canister.

Step 2: Remove failed controller (simplex)

Replace the failed canister with a new one.

Step 2a: Remove controller canister (simplex)

Remove a controller canister.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



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

4. If the HIC ports on the controller canister use SFP+ transceivers, remove the SFPs.

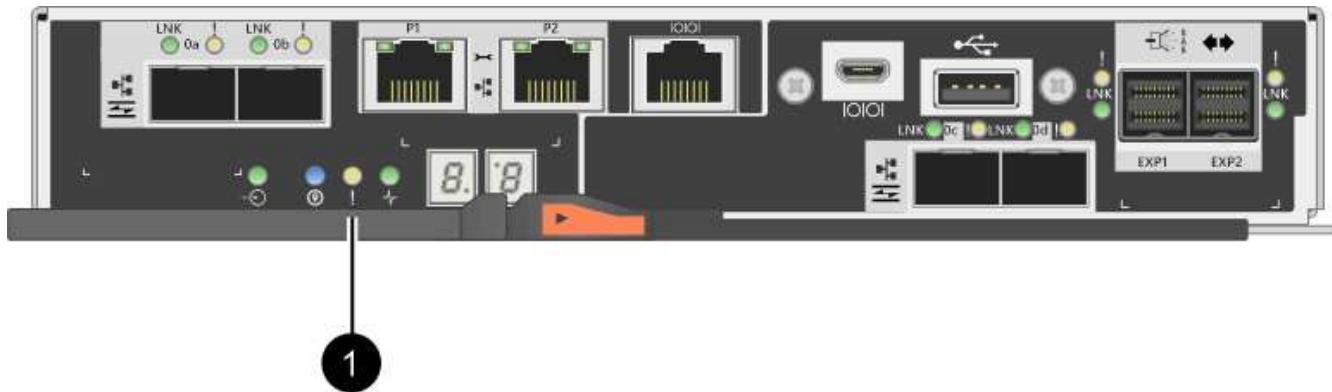
Because you must remove the HIC from the failed controller canister, you must remove any SFPs from the HIC ports. However, you can leave any SFPs installed in the baseboard host ports. When you are ready to cable the new controller, you can simply move those SFPs to the new controller canister. This approach is especially helpful if you have more than one type of SFP.

5. Confirm that the Cache Active LED on the back of the controller is off.

The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.

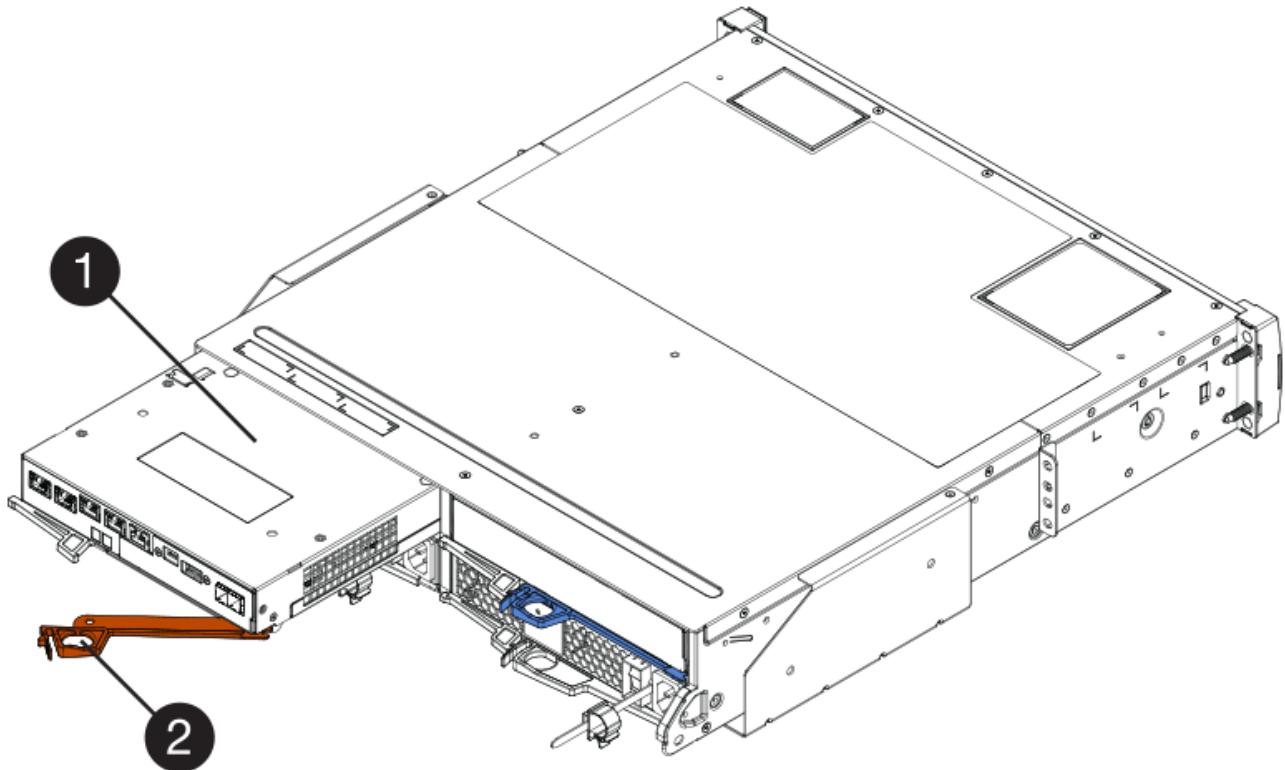


The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Cache Active LED

6. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the midplane.



(1) Controller canister

(2) Cam handle

7. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

When you remove the controller canister, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

8. Turn the controller canister over, so that the removable cover faces up.
9. Place the controller canister on a flat, static-free surface.

Step 2b: Remove battery (simplex)

After removing the controller canister from the controller shelf, remove the battery.

Steps

1. Remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

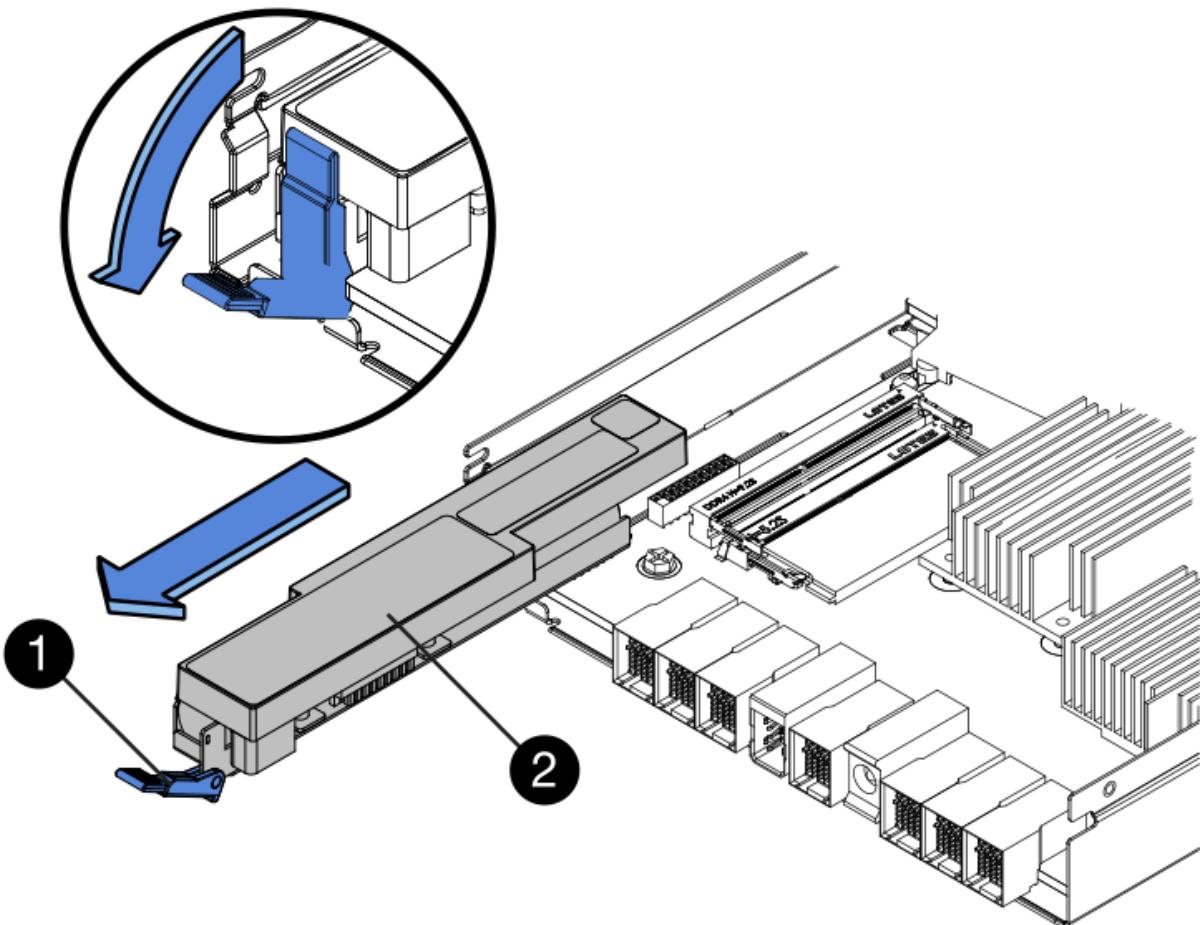
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active

(2) Battery

3. Locate the blue release latch for the battery.
4. Unlatch the battery by pushing the release latch down and away from the controller canister.



(1) *Battery release latch*

(2) *Battery*

5. Lift up on the battery, and slide it out of the controller canister.

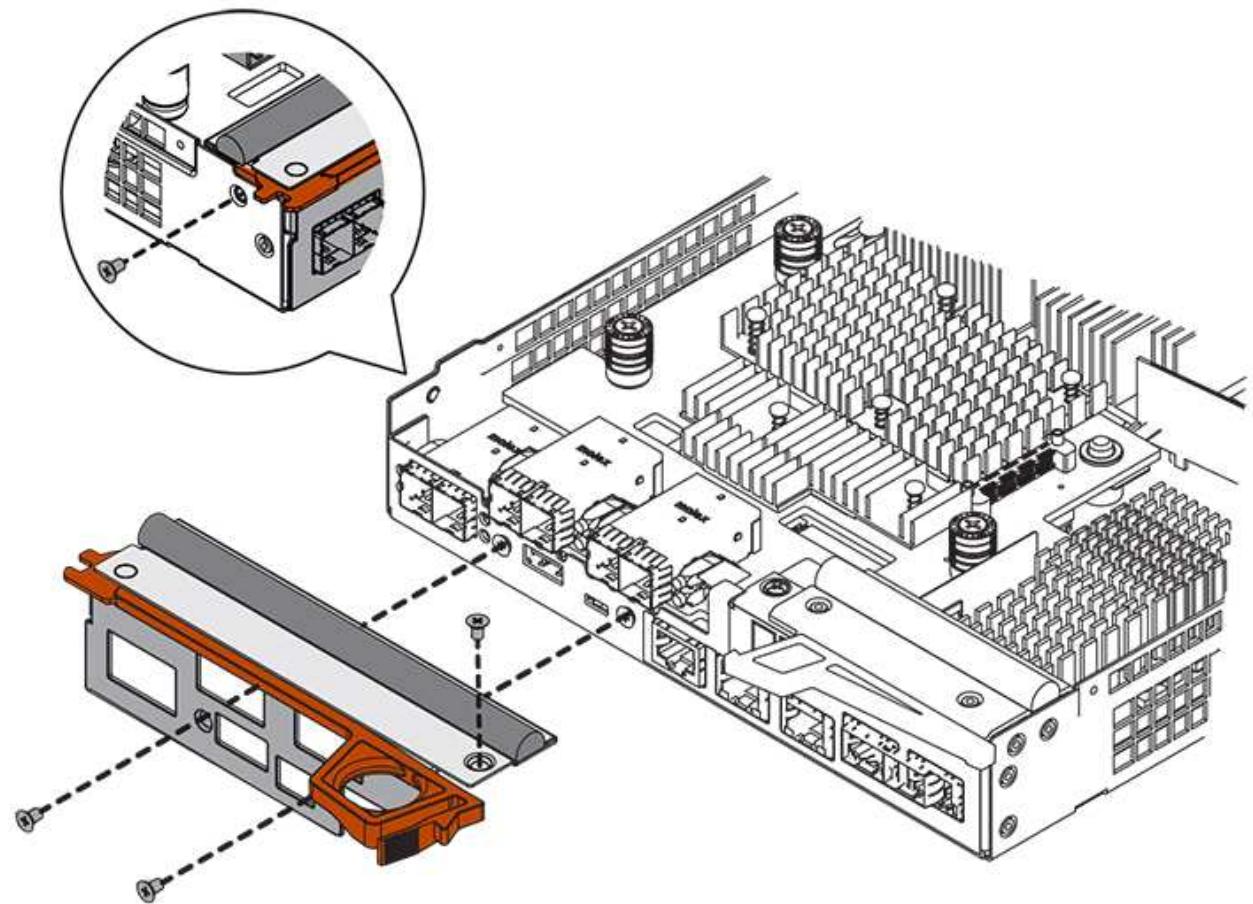
Step 2c: Remove host interface card (simplex)

If the controller canister includes a host interface card (HIC), remove the HIC from the original controller canister so you can reuse it in the new controller canister.

Steps

1. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller canister.

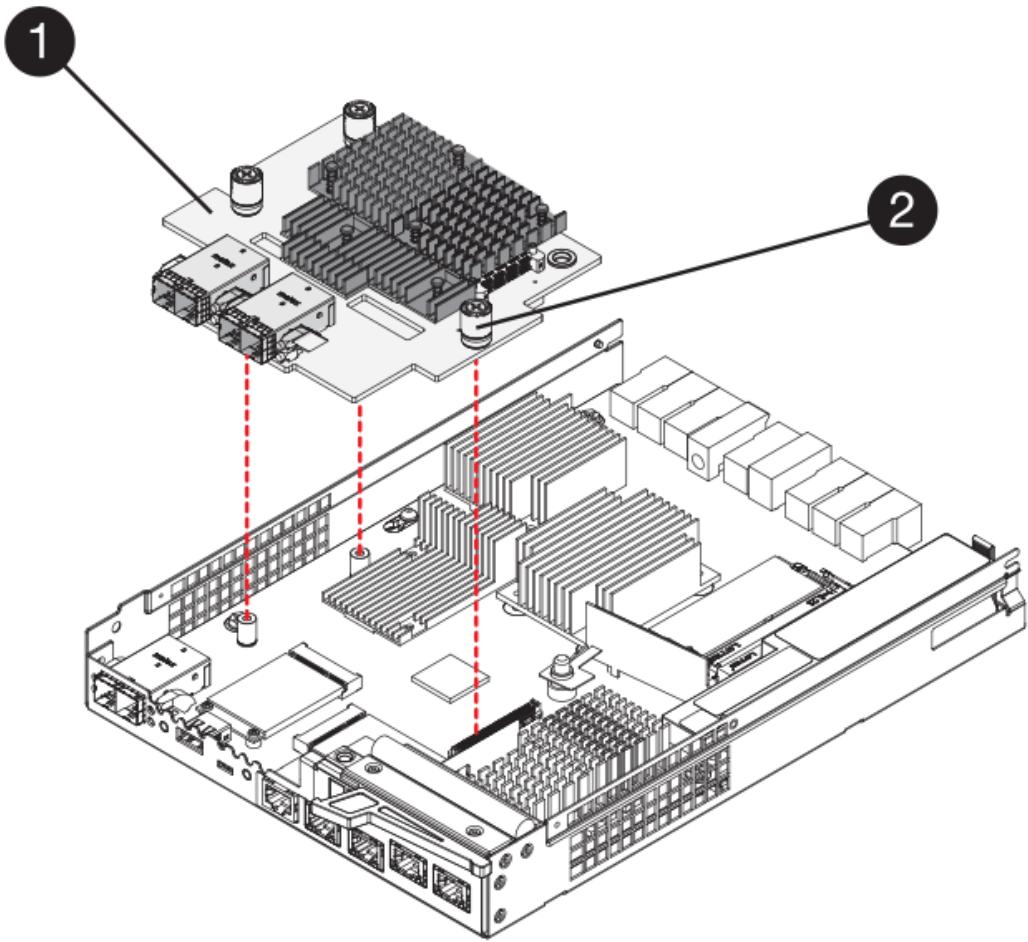
There are four screws: one on the top, one on the side, and two on the front.



2. Remove the HIC faceplate.
3. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
4. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



(1) Host interface card

(2) Thumbscrews

5. Place the HIC on a static-free surface.

Step 3: Install new controller (simplex)

Install a new controller canister to replace the failed one.

Step 3a: Install battery (simplex)

Install the battery into the replacement controller canister. You can install the battery that you removed from the original controller canister or install a new battery that you ordered.

Steps

1. Unpack the replacement controller canister, and set it on a flat, static-free surface so that the removable cover faces up.

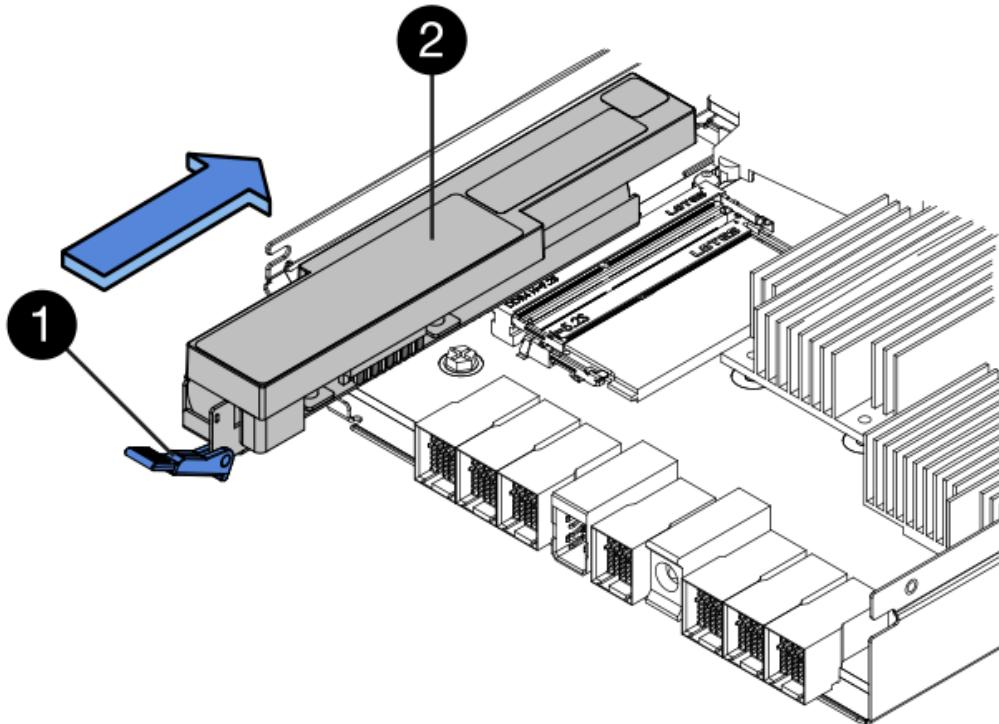
Save the packing materials to use when shipping the failed controller canister.

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 controller canister at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller canister, and slide the top of the battery beneath the small alignment pin on the left side of the canister.

5. Move the battery latch up to secure the battery.

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



(1) Battery release latch

(2) Battery

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



Possible hardware damage — The metal flange at the front of the battery must be completely inserted into the slot on the controller canister (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage to the controller when you apply power.

- **Correct** — The battery's metal flange is completely inserted in the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



Step 3b: Install host interface card (simplex)

If you removed a host interface card (HIC) from the original controller canister, install that HIC in the new controller canister.

Steps

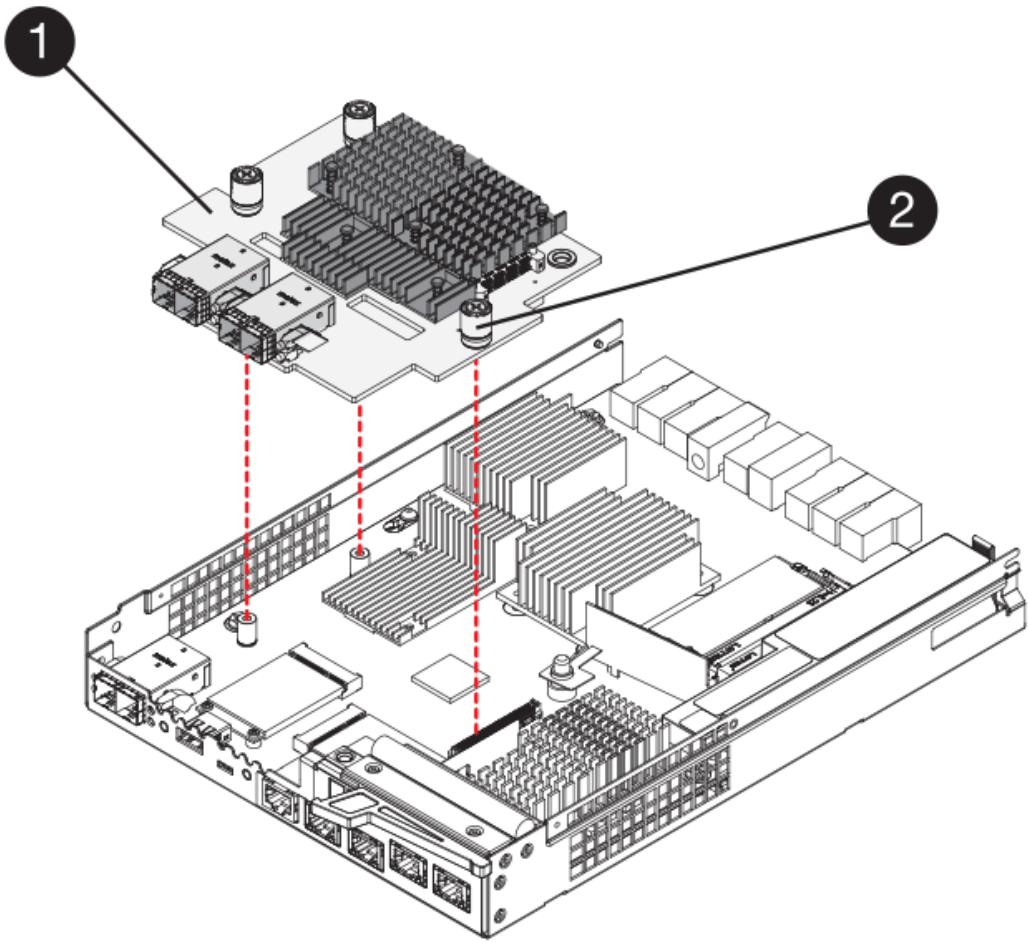
1. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller canister, and remove the faceplate.
2. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



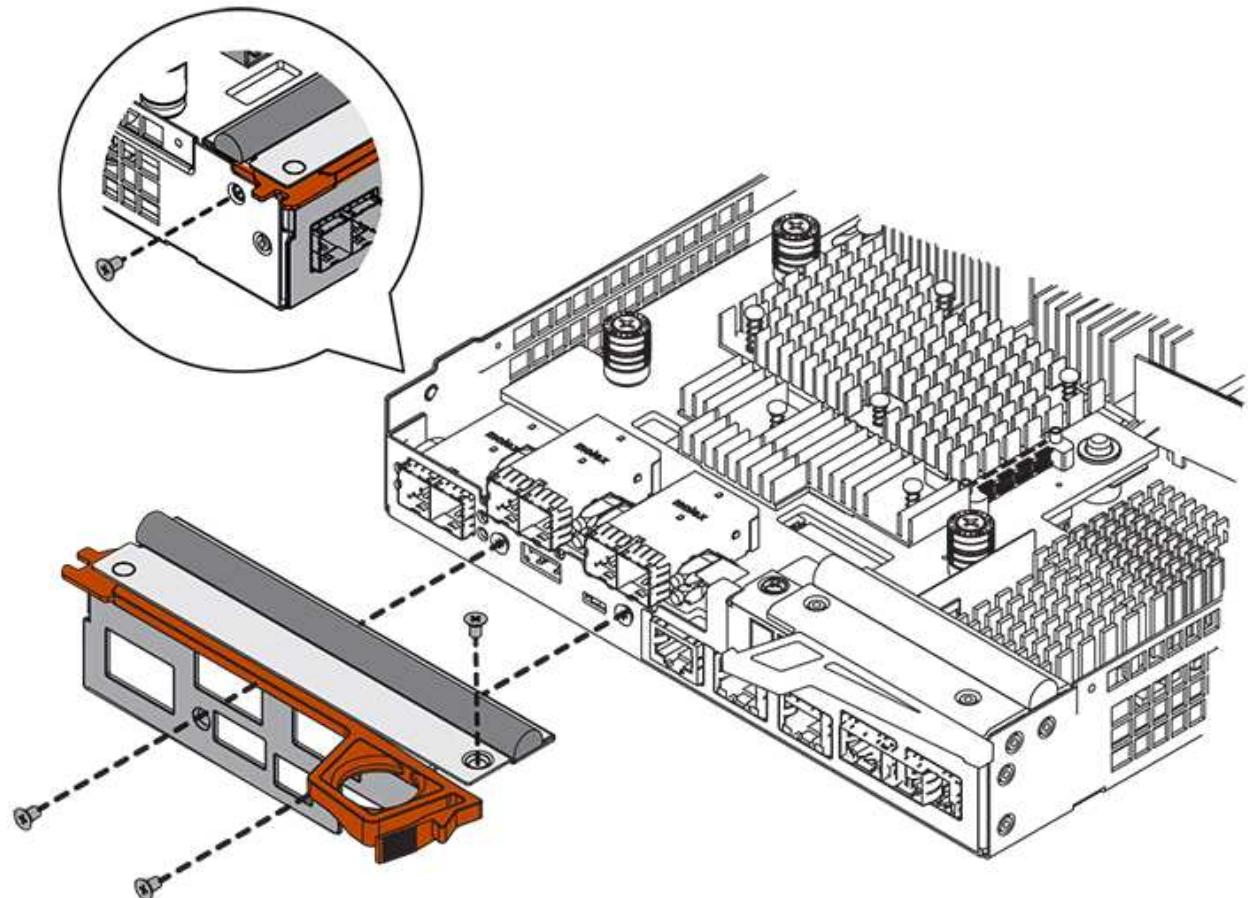
(1) *Host interface card*

(2) *Thumbscrews*

4. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

5. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller canister to the new controller canister with four screws.

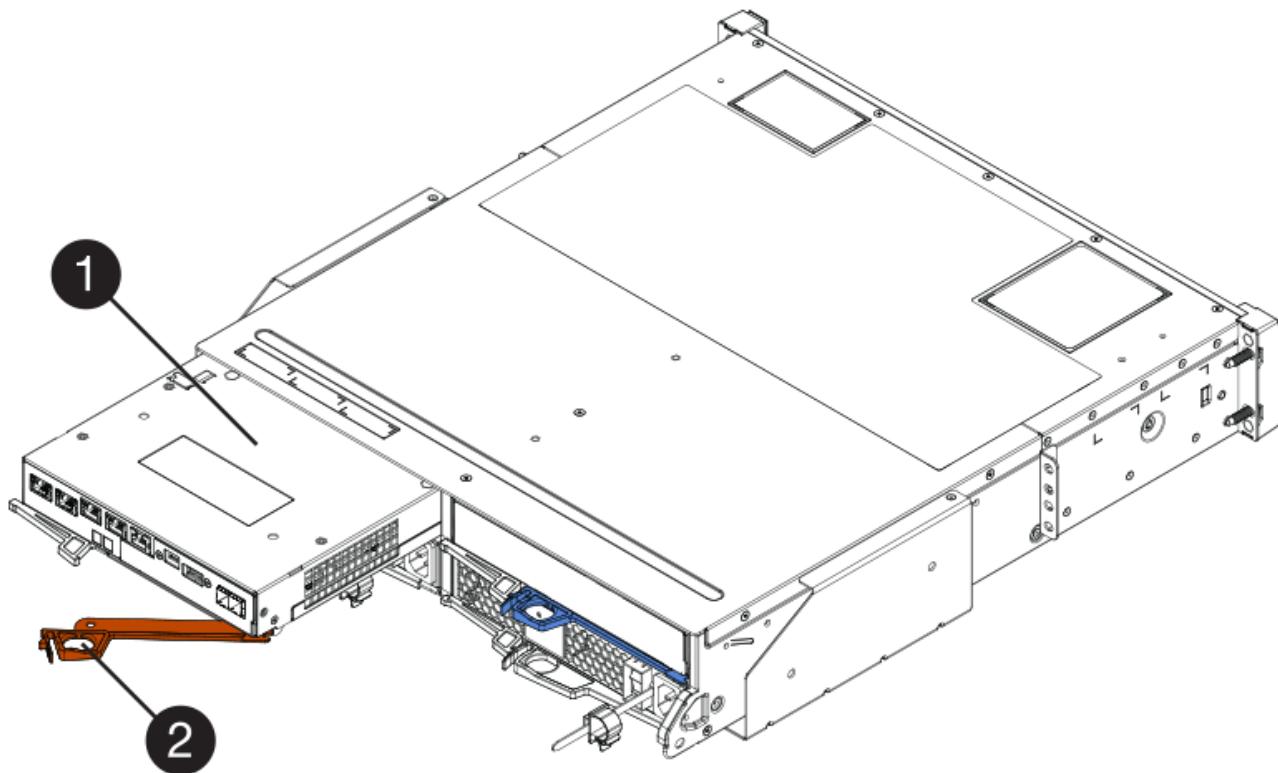


Step 3c: Install new controller canister (simplex)

After installing the battery and the HIC, if one was initially installed, you can install the new controller canister into the controller shelf.

Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle

4. Move the cam handle to the left to lock the controller canister in place.
5. Install the SFPs from the original controller in the host ports on the new controller, and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

6. Determine how you will assign an IP address to the replacement controller, based on whether you connected its Ethernet port 1 (labeled P1) to a network with a DHCP server and on whether all drives are secured.

| Using DHCP server? | All drives secured? | Steps |
|--------------------|---------------------|---|
| Yes | No | The new controller obtains its IP address from the DHCP server. This value might be different than the original controller's IP address. Locate the MAC address on the label on the back of the replacement controller, and contact your network administrator with this information to obtain the IP address that was assigned by the DHCP server. |

| Using DHCP server? | All drives secured? | Steps |
|--------------------|---------------------|--|
| Yes | Yes | The new controller obtains its IP address from the DHCP server. This value might be different than the original controller's IP address. Locate the MAC address on the label on the back of the replacement controller, and contact your network administrator with this information to obtain the IP address that was assigned by the DHCP server. You can then unlock the drives using the command line interface. |
| No | No | The new controller adopts the IP address of the controller you removed. |
| No | Yes | You must set the IP address of the new controller manually. (You can reuse the IP address of the old controller or use a new IP address.) When the controller has an IP address, you can unlock the drives using the command line interface. After the drives are unlocked, the new controller will re-use the original controller's IP address automatically. |

Step 4: Complete controller replacement (simplex)

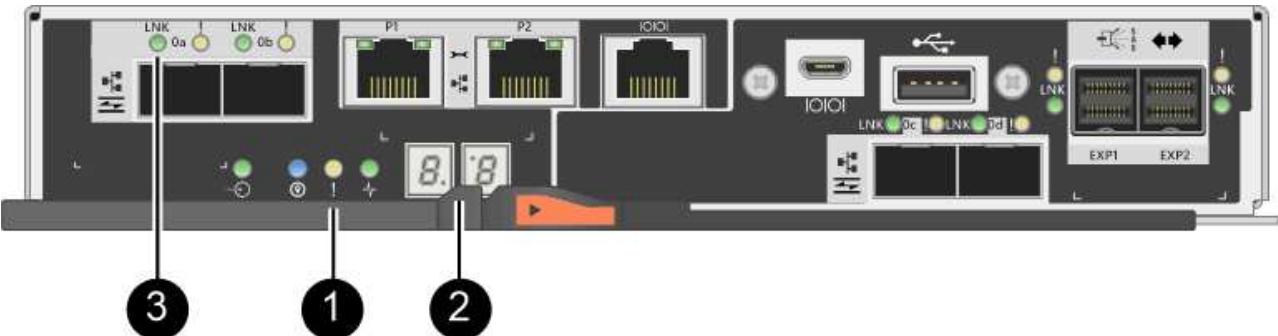
Power on the controller shelf, collect support data, and resume operations.

Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS**, **Sd**, **blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
 - The amber Attention LED on the controller turns on and then turns off, unless there is an error.
 - The green Host Link LEDs turn on.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) *Attention LED (amber)*

(2) *Seven-segment display*

(3) *Host Link LEDs*

3. If any of the controller shelf's Attention LEDs remain on, check that the controller canister has been installed correctly and that all cables are correctly seated. Reinstall the controller canister, if necessary.



If you cannot resolve the problem, contact technical support.

4. If the storage array has secure drives, import the drive security key; otherwise, go to the next step. Follow the appropriate procedure below for a storage array with all secure drives or a mix of secure and unsecure drives.



Unsecure drives are unassigned drives, global hot spare drives, or drives that are part of a volume group or a pool that is not secured by the Drive Security feature. *Secure drives* are assigned drives that are a part of a secured volume group or disk pool using Drive Security.

- **Only secured drives (no unsecure drives):**

- a. Access the storage array's command line interface (CLI).
- b. Enter the following command to import the security key:

```
import storageArray securityKey file="C:/file.slk"
passPhrase="passPhrase";
```

where:

- C:/file.slk represents the directory location and name of your drive security key
- passPhrase is the pass phrase needed to unlock the file
After the security key has been imported, the controller reboots, and the new controller adopts the saved settings for the storage array.

- c. Go to the next step to confirm that the new controller is Optimal.

- **Mix of secure and unsecure drives:**

- a. Collect the support bundle and open the storage array profile.
 - b. Find and record all the unsecure drives' locations, which are found in the support bundle.
 - c. Power off the system.
 - d. Remove the unsecure drives.
 - e. Replace the controller.
 - f. Power on the system and wait for the seven-segment display to show the tray number.
 - g. From SANtricity System Manager, select **Settings > System**.
 - h. In the Security Key Management section, select **Create/Change Key** to create a new security key.
 - i. Select **Unlock Secure Drives** to import the security key you saved.
 - j. Run the `set allDrives nativeState` CLI command.
- The controller will reboot automatically.
- k. Wait for the controller to boot up and for the seven-segment display to show the tray number or a flashing L5.
 - l. Power off the system.
 - m. Reinstall the unsecure drives.
 - n. Reset the controller using SANtricity System Manager.
 - o. Power on the system and wait for the seven-segment display to show the tray number.
 - p. Go to the next step to confirm that the new controller is Optimal.
5. From SANtricity System Manager, confirm that the new controller is Optimal.
 - a. Select **Hardware**.
 - b. For the controller shelf, select **Show back of shelf**.
 - c. Select the controller canister you replaced.
 - d. Select **View settings**.
 - e. Confirm that the controller's **Status** is Optimal.
 - f. If the status is not Optimal, highlight the controller, and select **Place Online**.
 6. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > *Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your controller replacement is complete. You can resume normal operations.

Canisters

Requirements for E2800 canister replacement

Before you replace a canister in an E2800 array, review the canister types and requirements.

Canister types include power supplies, power canisters, and fan canisters.

Power supply



The power supply replacement procedure is applicable for IOM replacements. To replace your IOM perform the power supply replacement procedure.

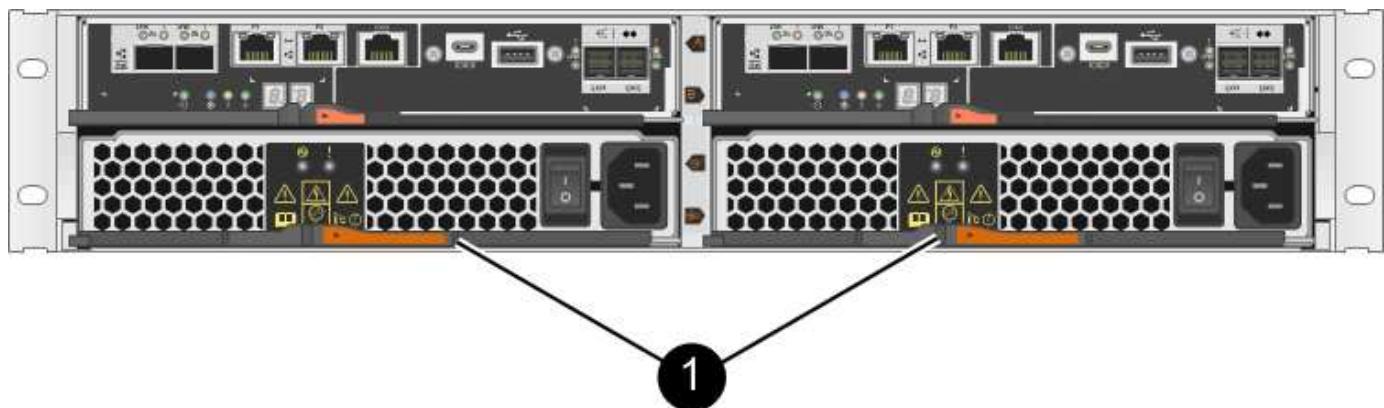
Each 12-drive or 24-drive controller shelf or drive shelf includes two power supplies with integrated fans. These are referred to as *power-fan canisters* in SANtricity System Manager. If a power-fan canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source and adequate cooling.

Shelf types for a power supply

You can replace a power supply in the following shelves:

- E2812 controller shelf
- E2824 controller shelf
- EF280 flash array
- DE212C drive shelf
- DE224C drive shelf

The following figure shows an example E2812 controller shelf, E2824 controller shelf, and EF280 flash array with two power supplies (power-fan canisters). The DE212C and DE224C drive shelves are identical, but they include I/O modules (IOMs) instead of controller canisters.



(1) Controller shelf with two power supplies (power-fan canisters) below the controller canisters

The procedure for replacing a power supply does not describe how to replace a failed power-fan canister in a DE1600 or DE5600 drive tray, which might be connected to the E5700 or E2800 controller shelves. For instructions for those drive tray models, refer to [Replacing a Power-Fan Canister in the DE1600 Drive Tray or the DE5600 Drive Tray](#).

Requirements for replacing a power supply

If you plan to replace a power supply, keep the following requirements in mind.

- You must have a replacement power supply (power-fan canister) that is supported for your controller shelf or drive shelf model.
- You have an ESD wristband, or you have taken other antistatic precautions.
- You can replace a power supply (power-fan canister) while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:
 - The second power supply (power-fan canister) in the shelf has an Optimal status.
 - The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second power supply (power-fan canister) in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the power-fan canister, contact technical support.

Power canister

Each 60-drive controller shelf or drive shelf includes two power canisters for power redundancy.

Shelf types for a power canister

You can replace a power canister in the following shelves:

- E2860 controller shelves
- DE460C drive shelf

The procedure for replacing a power canister does not describe how to replace a failed power canister in a DE6600 drive tray, which might be connected to the controller shelf.

The following figure shows the back of a DE460C drive shelf with the two power canisters:



The following figure shows a power canister:



Requirements for replacing a power canister

If you plan to replace a power canister, keep the following requirements in mind.

- You have a replacement power canister that is supported for your controller shelf or drive shelf model.
- You have one power canister that is installed and running.
- You have an ESD wristband, or you have taken other antistatic precautions.
- You can replace a power canister while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:
 - The other power canister in the shelf has Optimal status.



While you perform the procedure, the other power canister supplies power to both fans to ensure that the equipment does not overheat.

- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second power canister in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the power canister, contact technical support.

Fan canister

Each 60-drive controller shelf or drive shelf includes two fan canisters.

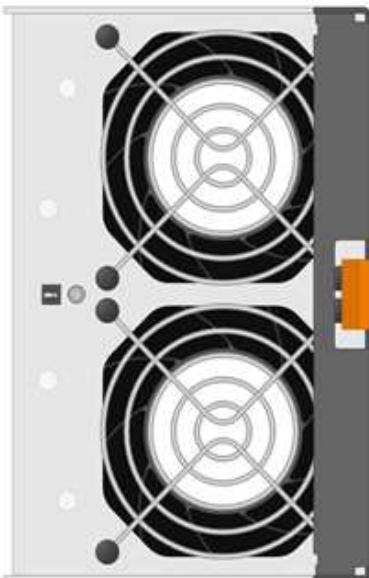
Shelf types for a fan canister

You can replace a fan canister in the following shelves:

- E2860 controller shelves
- DE460C drive shelf

The procedure for replacing a fan canister does not describe how to replace a failed fan canister in a DE6600 drive tray, which might be connected to the controller shelf.

The following figure shows a fan canister:



The following figure shows the back of a DE460C shelf with two fan canisters:



Possible equipment damage — If you replace a fan canister with the power turned on, you must complete the replacement procedure within 30 minutes to prevent the possibility of overheating the equipment.

Requirements for replacing a fan canister

If you plan to replace a fan canister, keep the following requirements in mind.

- You have a replacement fan canister (fan) that is supported for your controller shelf or drive shelf model.
- You have one fan canister that is installed and running.
- You have an ESD wristband, or you have taken other antistatic precautions.
- If you perform this procedure with the power turned on, you must complete it within 30 minutes to prevent the possibility of overheating the equipment.
- You can replace a fan canister while your storage array is powered on and performing host I/O operations,

as long as the following conditions are true:

- The second fan canister in the shelf has an Optimal status.
- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second fan canister in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the fan canister, contact technical support.

Replace E2800 power supply (12-drive or 24-drive)

You can replace a power supply in an E2800 array with a 12-drive or 24-drive shelf, including the following shelf types:

- E2812 controller shelf
- E2824 controller shelf
- EF280 flash array
- DE212C drive shelf
- DE224C drive shelf

About this task

Each 12-drive or 24-drive controller shelf or drive shelf includes two power supplies with integrated fans. These are referred to as *power-fan canisters* in SANtricity System Manager. If a power-fan canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source and adequate cooling.

You can replace a power supply while your storage array is powered on and performing host I/O operations, as long as the second power supply in the shelf has an Optimal status and the **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**.

Before you begin

- Review the power supply requirements in [Requirements for canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with the power supply. Select **Recheck** from the Recovery Guru to ensure no other items must be addressed first.
- Check that the amber Attention LED on the power supply is on, indicating that the power supply or its integrated fan has a fault. Contact technical support for assistance if both power supplies in the shelf have their amber Attention LEDs on.

What you'll need

- A replacement power supply that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.

Step 1: Prepare to replace power supply

Prepare to replace a power supply in a 12-drive or 24-drive controller shelf or drive shelf.

Steps

1. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.

b. Select **Collect Support Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which power supply has failed.

You can find this information in the Details area of the Recovery Guru, or you can review the information displayed for the shelf.

a. Select **Hardware**.

b. Look at the power  and fan  icons to the right of the **Shelf** drop-down lists to determine which shelf has the failed power supply.

If a component has failed, either or both of these icons are red.

c. When you find the shelf with a red icon, select **Show back of shelf**.

d. Select either power supply.

e. On the **Power Supplies** and **Fans** tabs, look at the statuses of the power-fan canisters, the power supplies, and the fans to determine which power supply must be replaced.

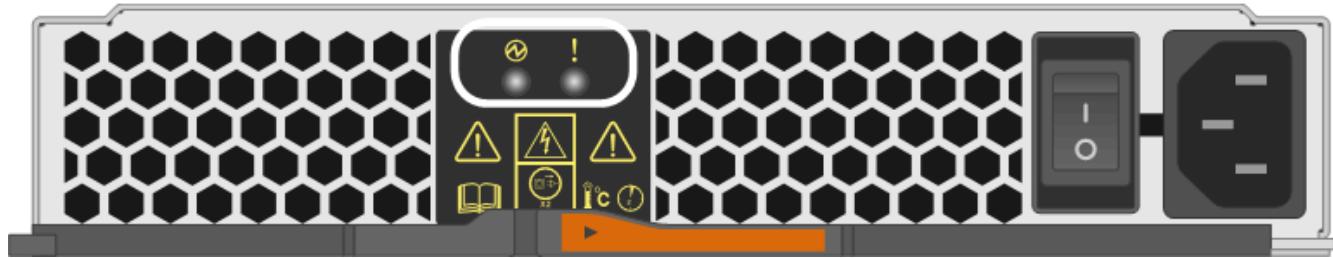
A component with a **Failed** status must be replaced.



If the second power supply canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed power supply. Instead, contact technical support for assistance.

3. From the back of the storage array, look at the Attention LEDs to locate the power supply you need to remove.

You must replace the power supply that has its Attention LED on.



- Power LED: If it is **solid green**, the power supply is functioning correctly. If it is **Off**, the power supply failed, the AC switch is turned off, the AC power cord is not properly installed, or the AC power cord input voltage is not within margin (there is a problem at the source end of the AC power cord).

- Attention LED: If it is **solid amber**, the power supply or its integrated fan has a fault.

Step 2: Remove failed power supply

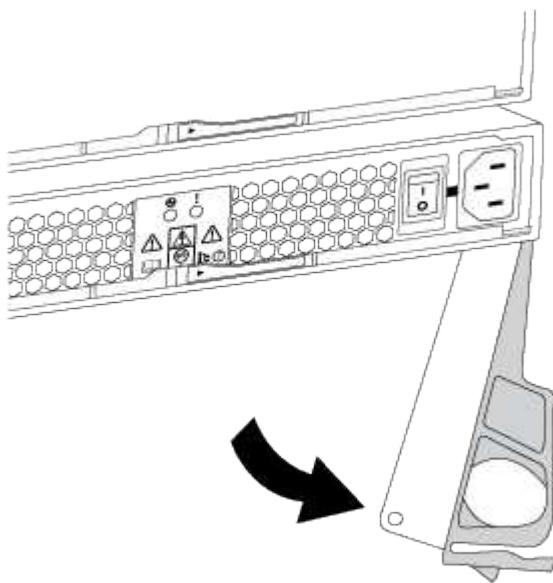
Remove a failed power supply so you can replace it with a new one.

Steps

1. Unpack the new power supply, and set it on a level surface near the drive shelf.

Save all packing materials for use when returning the failed power supply.

2. Turn off the power supply and disconnect the power cables:
 - a. Turn off the power switch on the power supply.
 - b. Open the power cord retainer, and then unplug the power cord from the power supply.
 - c. Unplug the power cord from the power source.
3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.



4. Use the cam handle to slide the power supply out of the system.



When removing a power supply, always use two hands to support its weight.

As you remove the power supply, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

Step 3: Install new power supply

Install a new power supply to replace the failed one.

Steps

1. Make sure that the on/off switch of the new power supply is in the **Off** position.
2. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system; you can damage the connector.

3. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
4. Reconnect the power supply cabling:
 - a. Reconnect the power cord to the power supply and the power source.
 - b. Secure the power cord to the power supply using the power cord retainer.
5. Turn on the power to the new power supply canister.

Step 4: Complete power supply replacement

Confirm that the new power supply is working correctly, gather support data, and resume normal operations.

Steps

1. On the new power supply, check that the green Power LED is on and the amber Attention LED is OFF.
2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed power supply is still being reported, repeat the steps in [Step 2: Remove failed power supply](#), and in [Step 3: Install new power supply](#). If the problem continues to persist, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your power supply replacement is complete. You can resume normal operations.

Replace E2800 power canister (60-drive)

You can replace a power canister in an E2800 array with a 60-drive shelf, which include the following shelf types:

- E2860 controller shelf
- DE460C drive shelf

About this task

Each 60-drive controller shelf or drive shelf includes two power canisters for power redundancy. If a power canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source.

You can replace a power canister while your storage array is powered on and performing host I/O operations, as long as the second power canister in the shelf has an Optimal status and the **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**.

While you perform this task, the other power canister supplies power to both fans to ensure that the equipment does not overheat.

Before you begin

- Review the power canister requirements in [Requirements for canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with the power canister and select **Recheck** from the Recovery Guru to ensure no other items must be addressed first.
- Check that the amber Attention LED on the power canister is on, indicating that the canister has a fault. Contact technical support for assistance if both power canisters in the shelf have their amber Attention LEDs on.

What you'll need

- A replacement power canister that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.

Step 1: Prepare to replace power canister

Prepare to replace a power canister in a 60-drive controller shelf or drive shelf.

Steps

1. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which power canister has failed.
 - a. Select **Hardware**.
 - b. Look at the power  icon to the right of the **Shelf** drop-down lists to determine which shelf has the failed power canister.
If a component has failed, this icon is red.
 - c. When you find the shelf with a red icon, select **Show back of shelf**.
 - d. Select either power canister or the red power icon.
 - e. On the **Power Supplies** tab, look at the statuses of the power canisters to determine which power canister must be replaced.

A component with a **Failed** status must be replaced.



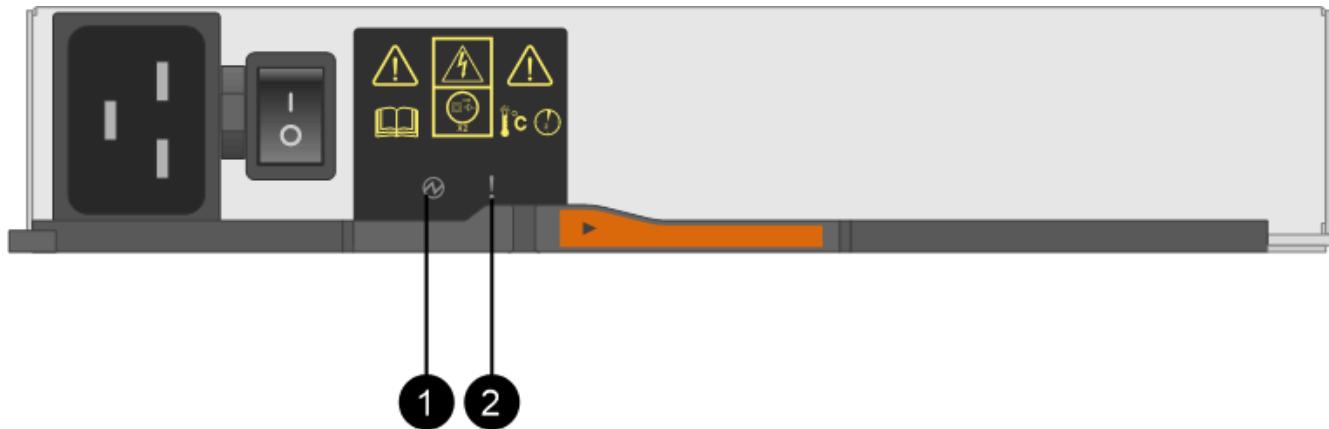
If the second power canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed power canister. Instead, contact technical support for assistance.



You can also find information about the failed power canister in the Details area of the Recovery Guru, or you can review the information displayed for the shelf, or you can review the Event Log under Support and filter by Component Type.

3. From the back of the storage array, look at the Attention LEDs to locate the power canister you need to remove.

You must replace the power canister that has its Attention LED on.



(1) Power LEDs. If it is **Solid green**, the power canister is functioning correctly. If it is **Off**, the power canister failed, the AC switch is turned off, the AC power cord is not properly installed, or the AC power cord input voltage is not within margin (there is a problem at the source end of the AC power cord).

(2) Attention LED. If it is **Solid amber**, the power canister has a fault, or there is no input power to this power canister, but the other power canister is operating.

Step 2: Remove failed power canister

Remove a failed power canister so you can replace it with a new one.

Steps

1. Put on antistatic protection.
 2. Unpack the new power canister, and set it on a level surface near the shelf.
- Save all packing materials for use when returning the failed power canister.
3. Turn off the power switch on the power canister that you need to remove.
 4. Open the power cord retainer of the power canister that you need to remove, and then unplug the power cord from the power canister.
 5. Press the orange latch on the power canister cam handle, and then open the cam handle to fully release the power canister from the mid plane.
 6. Use the cam handle to slide the power canister out of the shelf.



When removing a power canister, always use two hands to support its weight.

Step 3: Install new power canister

Install a new power canister to replace the failed one.

Steps

1. Make sure the on/off switch of the new power canister is in the Off position.
2. Using both hands, support and align the edges of the power canister with the opening in the system chassis, and then gently push the power canister into the chassis using the cam handle until it locks into place.



Do not use excessive force when sliding the power canister into the system; you can damage the connector.

3. Close the cam handle so that the latch clicks into the locked position and the power canister is fully seated.
4. Reconnect the power cord to the power canister, and secure the power cord to the power canister using the power cord retainer.
5. Turn on the power to the new power canister.

Step 4: Complete power canister replacement

Confirm that the new power canister is working correctly, gather support data, and resume normal operations.

Steps

1. On the new power canister, check that the green Power LED is on and the amber Attention LED is OFF.
2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed power canister is still being reported, repeat the steps in [Step 2: Remove failed power canister](#) and in [Step 3: Install new power canister](#). If the problem continues to persist, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your power canister replacement is complete. You can resume normal operations.

Replace E2800 fan canister (60-drive)

You can replace a fan canister in an E2800 array with a 60-drive shelf, which include the following shelf types:

- E2860 controller shelf
- DE460C drive shelf

About this task

Each 60-drive controller shelf or drive shelf includes two fan canisters. If a fan canister fails, you must replace it as soon as possible to ensure that the shelf has adequate cooling.



Possible equipment damage—If you perform this procedure with the power turned on, you must complete it within 30 minutes to prevent the possibility of overheating the equipment.

Before you begin

- Review the fan canister requirements in [Requirements for canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with the fan canister and select **Recheck** from the Recovery Guru to ensure no other items must be addressed first.
- Check that the amber Attention LED on the fan canister is on, indicating that the fan has a fault. Contact technical support for assistance if both fan canisters in the shelf have their amber Attention LEDs on.

What you'll need

- A replacement fan canister (fan) that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.

Step 1: Prepare to replace fan canister

Prepare to replace a fan canister in a 60-drive controller shelf or drive shelf by collecting support data about your storage array and locating the failed component.

Steps

1. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support** > **Support Center** > **Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which fan canister has failed.
 - a. Select **Hardware**.
 - b. Look at the fan  icon to the right of the **Shelf** drop-down lists to determine which shelf has the failed fan canister.

If a component has failed, this icon is red.

 - c. When you find the shelf with a red icon, select **Show back of shelf**.
 - d. Select either fan canister or the red fan icon.
 - e. On the **Fans** tab, look at the statuses of the fan canisters to determine which fan canister must be replaced.

A component with a **Failed** status must be replaced.

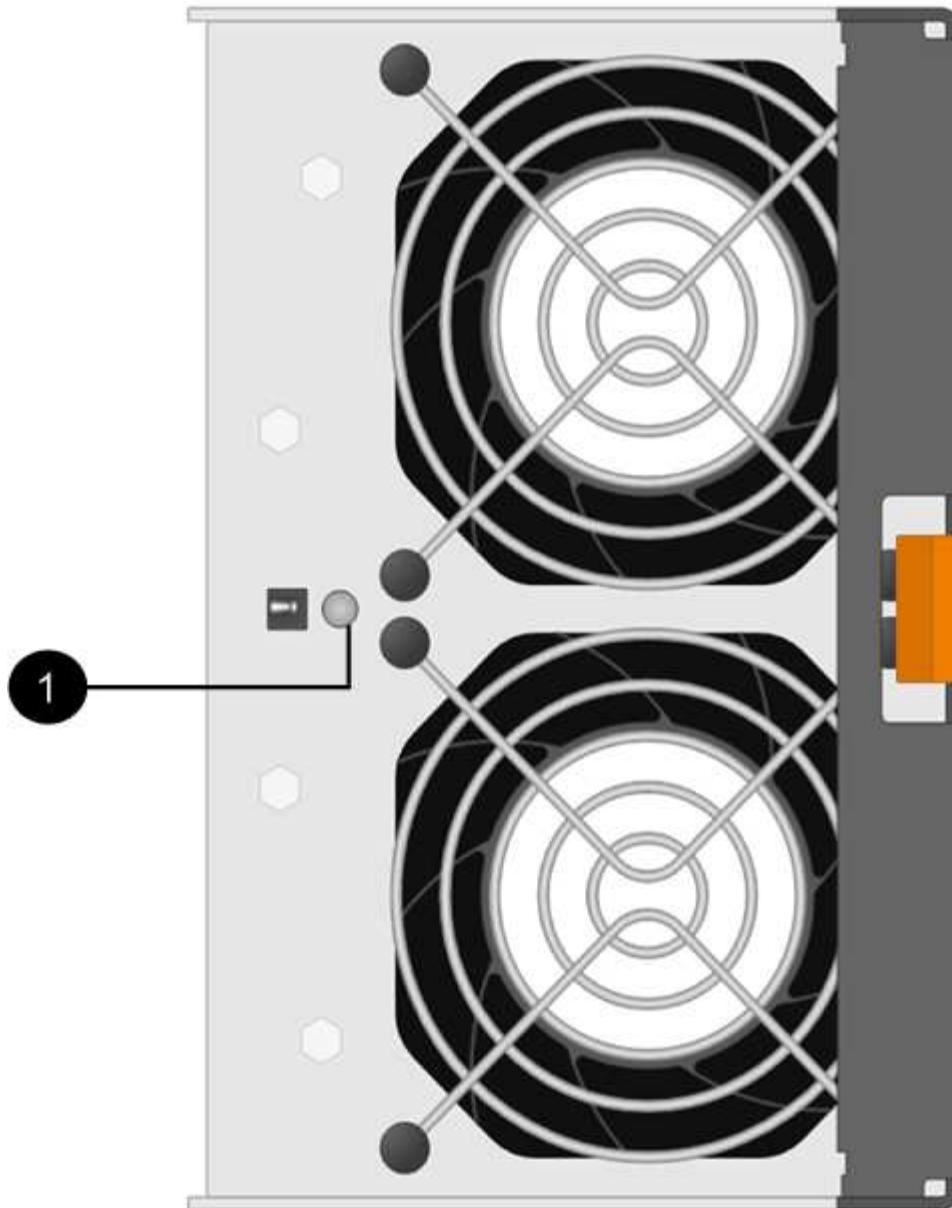


If the second fan canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed fan canister. Instead, contact technical support for assistance.

You can also find information about the failed fan canister in the Details area of the Recovery Guru, or you can review the Event Log under Support and filter by Component Type.

3. From the back of the storage array, look at the Attention LEDs to locate the fan canister you need to remove.

You must replace the fan canister that has its Attention LED on.



(1) **Attention LED.** If this LED displays as **Solid amber**, then the fan has a fault.

Step 2: Remove failed fan canister and install new one

Remove a failed fan canister so you can replace it with a new one.



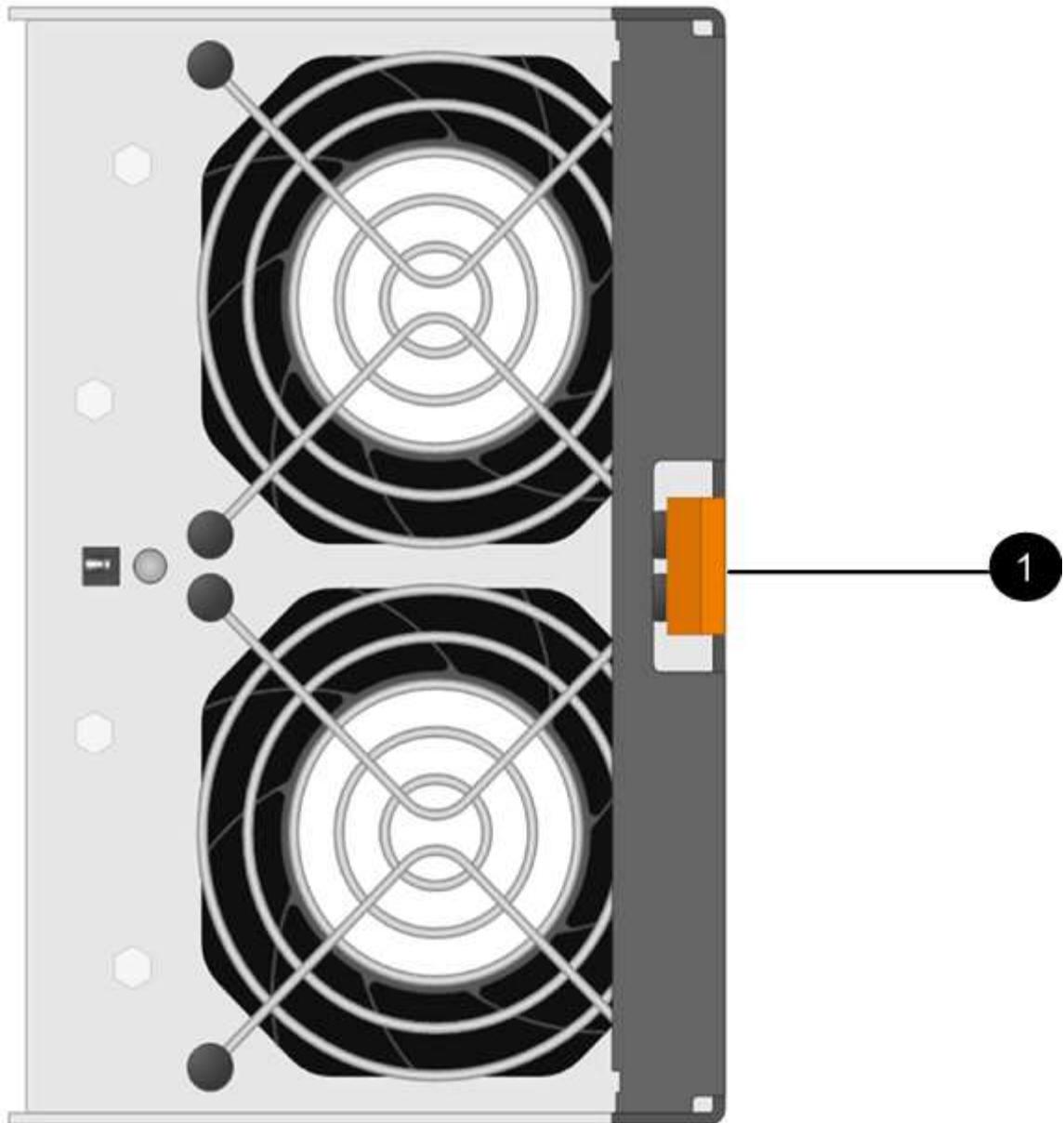
If you do not turn off the power to your storage array, ensure that you remove and replace the fan canister within 30 minutes to prevent the system from overheating.

Steps

1. Unpack the new fan canister, and place it on a level surface near the shelf.

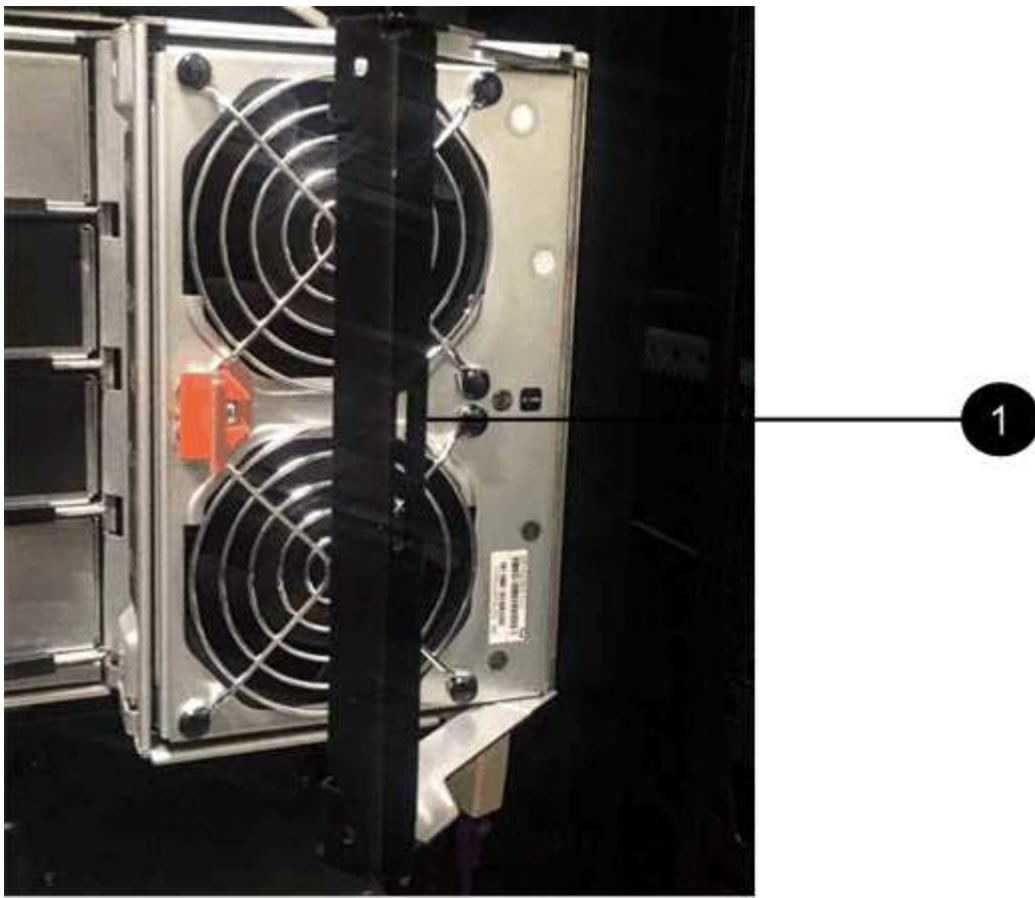
Save all packing material for use when returning the failed fan.

2. Press the orange tab to release the fan canister handle.



(1) Tab that you press to release the fan canister handle

3. Use the fan canister handle to pull the fan canister out of the shelf.



(1) Handle to pull the fan canister out

4. Slide the replacement fan canister all the way into the shelf, and then move the fan canister handle until it latches with the orange tab.

Step 3: Complete fan canister replacement

Confirm that the new fan canister is working correctly, gather support data, and resume normal operations.

Steps

1. Check the amber Attention LED on the new fan canister.



After you replace the fan canister, the Attention LED stays on (solid amber) while the firmware checks that the fan canister was installed correctly. The LED goes off after this process is complete.

2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed fan canister is still being reported, repeat the steps in [Step 2: Remove failed fan canister and install new one](#). If the problem persists, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your fan canister replacement is complete. You can resume normal operations.

Drives

Requirements for E2800 drive replacement

Before you replace an E2800 drive, review the requirements and considerations.

Shelf types

You can replace a drive in either a 12-drive, 24-drive, or 60-drive controller shelf or drive shelf.

This procedure applies to IOM12 and IOM12B drive shelves, and DCM and DCM2 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.)

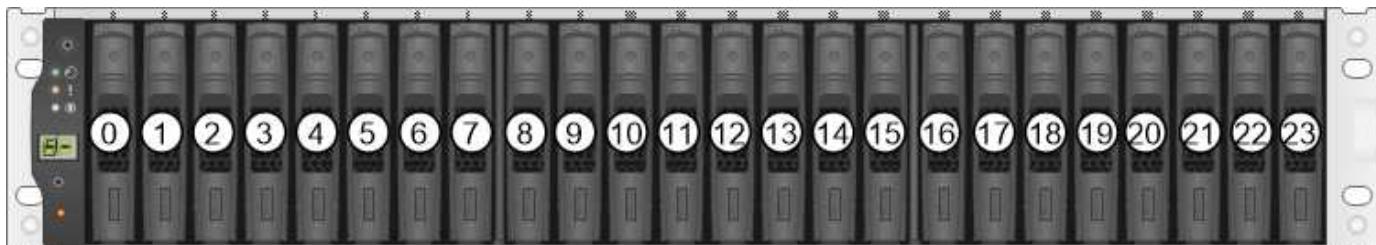
12-drive or 24-drive shelves

The figures show how the drives are numbered in each type of shelf (the shelf's front bezel or end caps have been removed).

Drive numbering in an E2812 controller shelf or DE212C drive shelf:



Drive numbering in an E2824 controller shelf, EF280 flash array, or DE224C drive shelf:

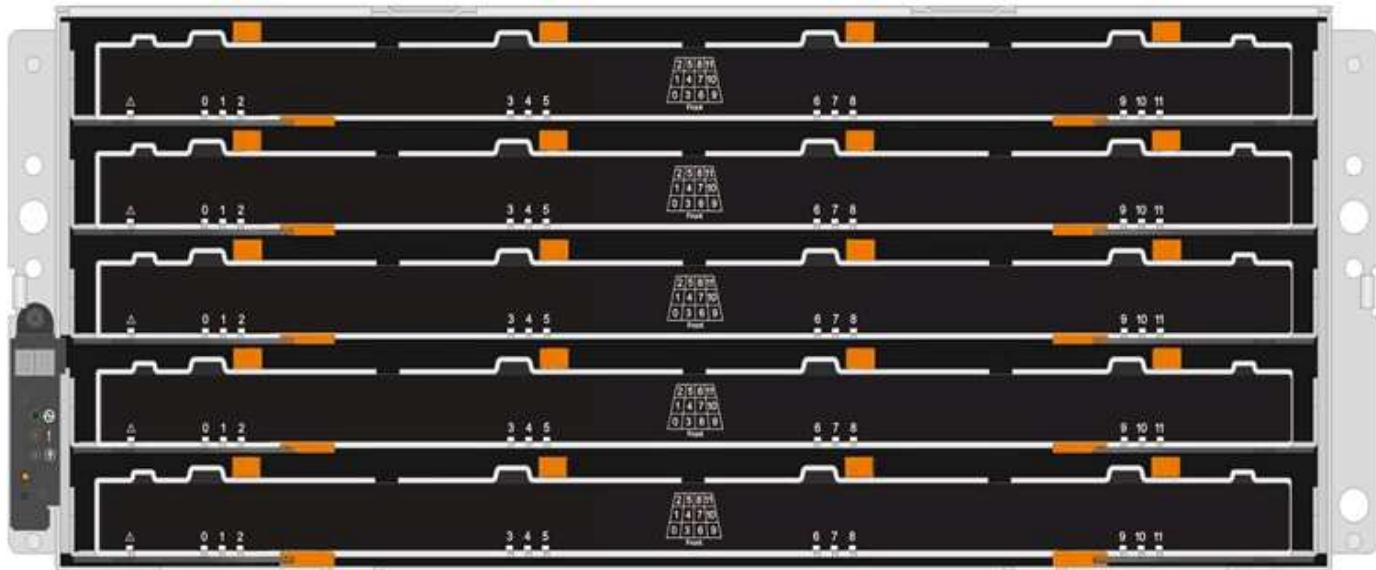




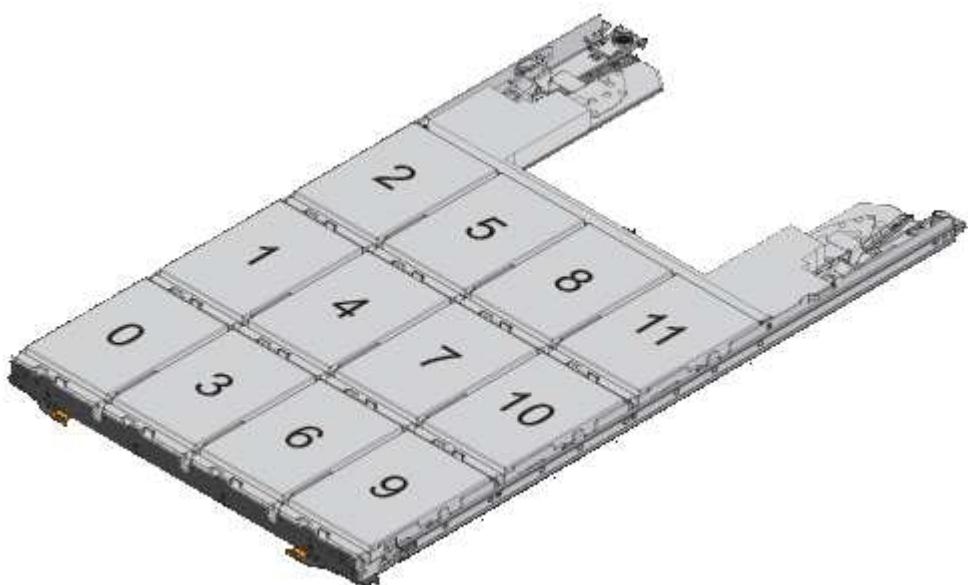
Your E2812, E2824, EF280 storage array might include one or more SAS-2 legacy expansion drive trays, including the DE1600 12-drive tray, the DE5600 24-drive tray, or the DE6600 60-drive tray. For instructions for replacing a drive in one of these drive trays, see [Replacing a Drive in E2660, E2760, E5460, E5560, or E5660 Trays](#) and [Replacing a Drive in E2600, E2700, E5400, E5500, and E5600 12-Drive or 24-Drive Trays](#).

60-drive shelves

Both the E2860 controller shelf and the DE460C drive shelf consist of five drive drawers that each contain 12 drive slots. Drive drawer 1 is at the top, and drive drawer 5 is at the bottom.



For both an E2860 controller shelf drawer and a DE460C drive shelf drawer, drives are numbered from 0 to 11 in each drive drawer within the shelf.

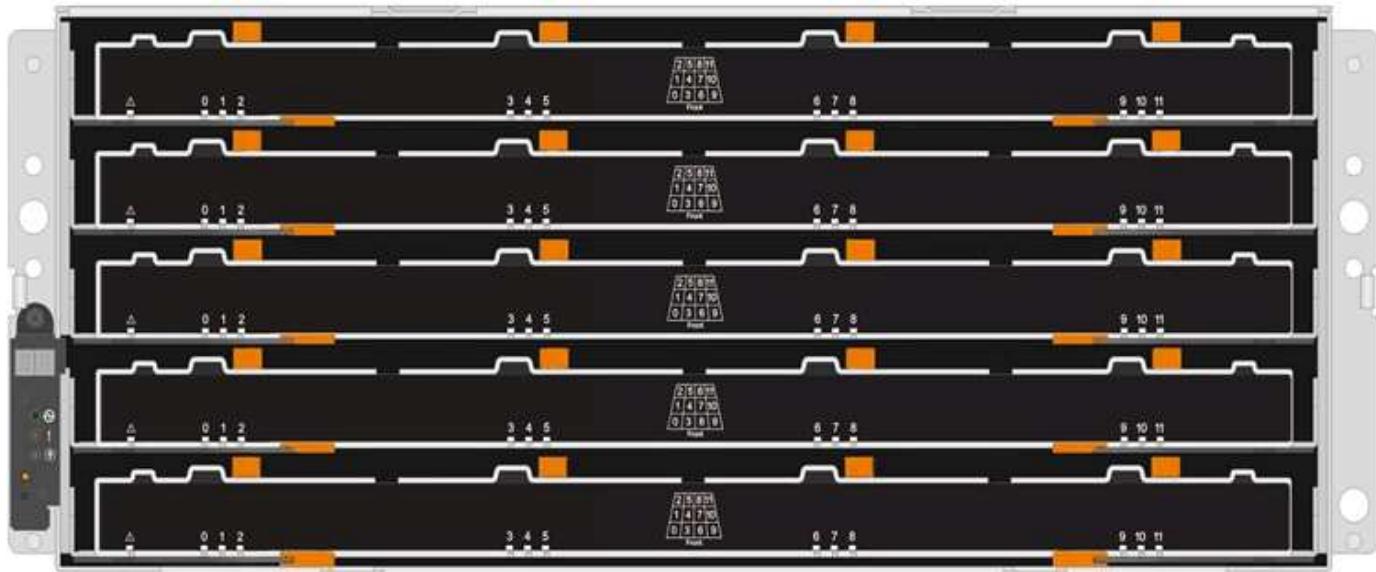




Your E2860 storage array might include one or more SAS-2 legacy expansion drive trays, including the DE1600 12-drive tray, the DE5600 24-drive tray, or the DE6600 60-drive tray. For instructions for replacing a drive in one of these drive trays, see [Replacing a Drive in E2660, E2760, E5460, E5560, or E5660 Trays](#) and [Replacing a Drive in E2600, E2700, E5400, E5500, and E5600 12-Drive or 24-Drive Trays](#).

Drive drawer

You can replace a drive drawer in a E2860 controller shelf and a DE460C drive shelf. Each of these 60-drive shelves has five drive drawers.



Each of the five drawers can hold up to 12 drives.



Drive handling

The drives in your storage array are fragile. Improper drive handling is a leading cause of drive failure.

Follow these rules to avoid damaging the drives in your storage array:

- Prevent electrostatic discharge (ESD):
 - Keep the drive in the ESD bag until you are ready to install it.
 - Do not insert a metal tool or knife into the ESD bag.
- Open the ESD bag by hand or cut the top off with a pair of scissors.
- Keep the ESD bag and any packing materials in case you must return a drive later.
- Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis.
- If a wrist strap is unavailable, touch an unpainted surface on your storage enclosure chassis before handling the drive.
- Handle drives carefully:
 - Always use two hands when removing, installing, or carrying a drive.
 - Never force a drive into a shelf, and use gentle, firm pressure to completely engage the drive latch.
 - Place drives on cushioned surfaces, and never stack drives on top of each other.
 - Do not bump drives against other surfaces.
 - Before removing a drive from a shelf, unlatch the handle and wait 30 seconds for the drive to spin down.
 - Always use approved packaging when shipping drives.
- Avoid magnetic fields:
 - Keep drives away from magnetic devices.

Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry.

Replace drive in E2800 (12-drive or 24-drive shelf)

You can replace a drive in an E2800 with a 12-drive or 24-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O.

Before you begin

- Review the drive handling requirements in [Requirements for E2800 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive

Prepare to replace a drive by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.
 - d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state disk (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within your storage array. From the drive's context menu on the Hardware page, select **Turn on locator light**.

The drive's Attention LED (amber) blinks so you can identify which drive to replace.



If you are replacing a drive in a shelf that has a bezel, you must remove the bezel to see the drive LEDs.

Step 2: Remove failed drive

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials.

2. Press the release button on the failed drive.



- For drives in E2812 controller shelves or DE212C drive shelves, the release button is located at the left of the drive.
- For drives in E2824 controller shelves, EF280 flash array, for DE224C drive shelves, the release button is located at the top of the drive.

The cam handle on the drive springs open partially, and the drive releases from the midplane.

3. Open the cam handle, and slide out the drive slightly.
4. Wait 30 seconds.
5. Using both hands, remove the drive from the shelf.

6. Place the drive on an antistatic, cushioned surface away from magnetic fields.
7. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive

Install a new drive to replace the failed one.



Install the replacement drive as soon as possible after removing the failed drive. Otherwise, there is a risk that the equipment might overheat.

Steps

1. Open the cam handle.
2. Using two hands, insert the replacement drive into the open bay, firmly pushing until the drive stops.
3. Slowly close the cam handle until the drive is fully seated in the midplane and the handle clicks into place.

The green LED on the drive comes on when the drive is inserted correctly.



Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement

Complete the drive replacement to confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced. (When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.)
 - Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
 - Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
 - Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.
2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.

c. From the drive's context menu, select **Reconstruct**.

d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.

5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace drive in E2800 (60-drive shelf)

You can replace a drive in an E2800 with a 60-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O operations.

This procedure applies to DCM and DCM2 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

- Review the drive handling requirements in [Requirements for E2800 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive

Prepare to replace a drive by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.

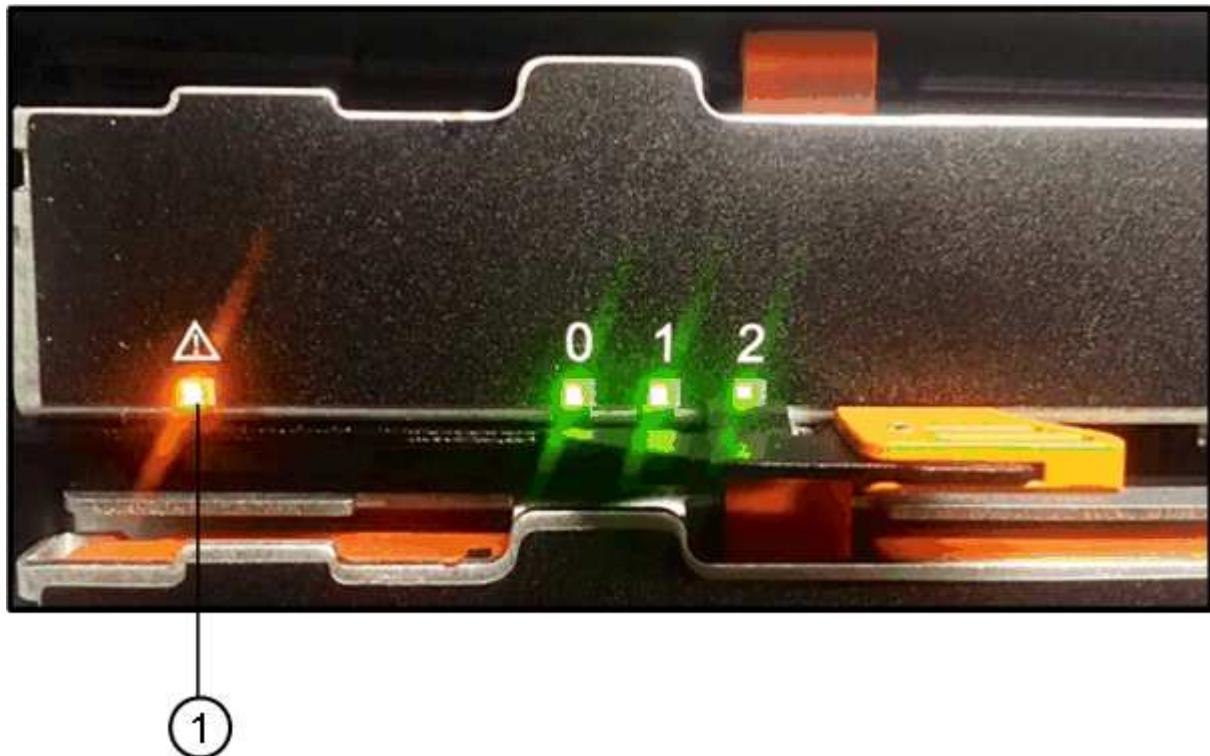
- d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state disk (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within the storage array.

- If the shelf has a bezel, remove it so you can see the LEDs.
- From the drive's context menu, select **Turn on locator light**.

The drive drawer's Attention LED (amber) blinks so you can open the correct drive drawer to identify which drive to replace.



(1) Attention LED

- Unlatch the drive drawer by pulling on both levers.
- Using the extended levers, carefully pull the drive drawer out until it stops.
- Look at the top of the drive drawer to find the Attention LED in front of each drive.



(1) Attention LED light on for the drive on the top right side

The drive drawer Attention LEDs are on the left side in front of each drive, with an attention icon on the drive handle just behind the LED.



(1) Attention icon

(2) Attention LED

Step 2: Remove failed drive

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials for the next time you need to send a drive back.

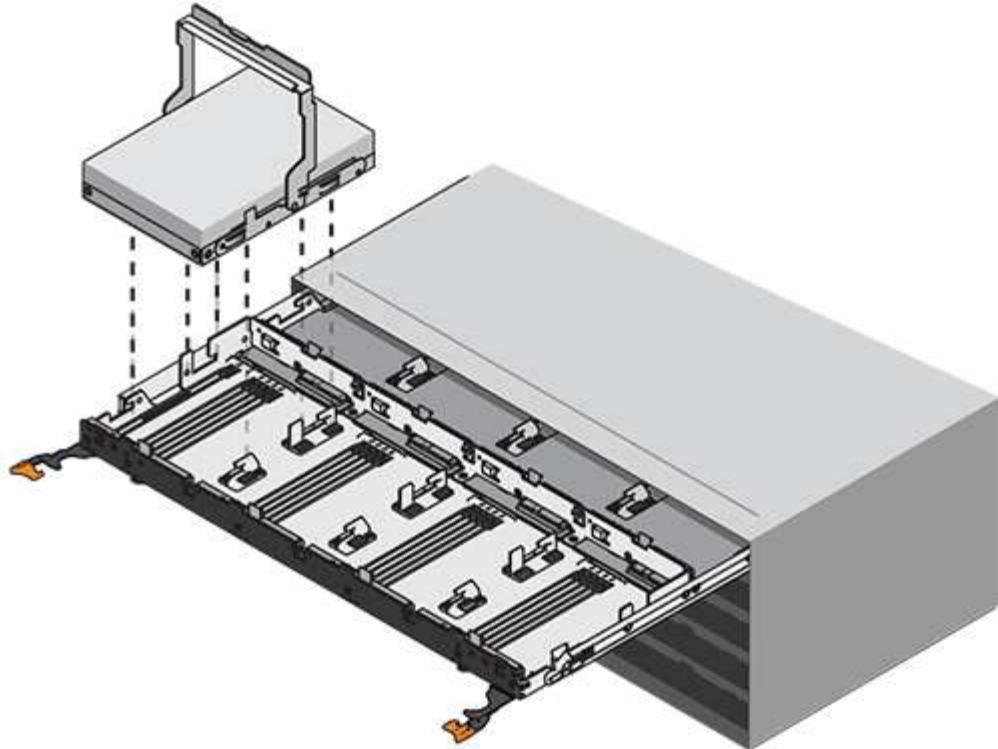
2. Release the drive drawer levers from the center of the appropriate drive drawer by pulling both towards the sides of the drawer.
3. Carefully pull on the extended drive drawer levers to pull out the drive drawer to its full extension without removing it from the enclosure.
4. Gently pull back the orange release latch that is in front of the drive you want to remove.

The cam handle on the drive springs open partially, and the drive is released from the drawer.



(1) Orange release latch

5. Open the cam handle, and lift out the drive slightly.
6. Wait 30 seconds.
7. Use the cam handle to lift the drive from the shelf.



8. Place the drive on an antistatic, cushioned surface away from magnetic fields.
9. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive

Install a new drive to replace the failed one.



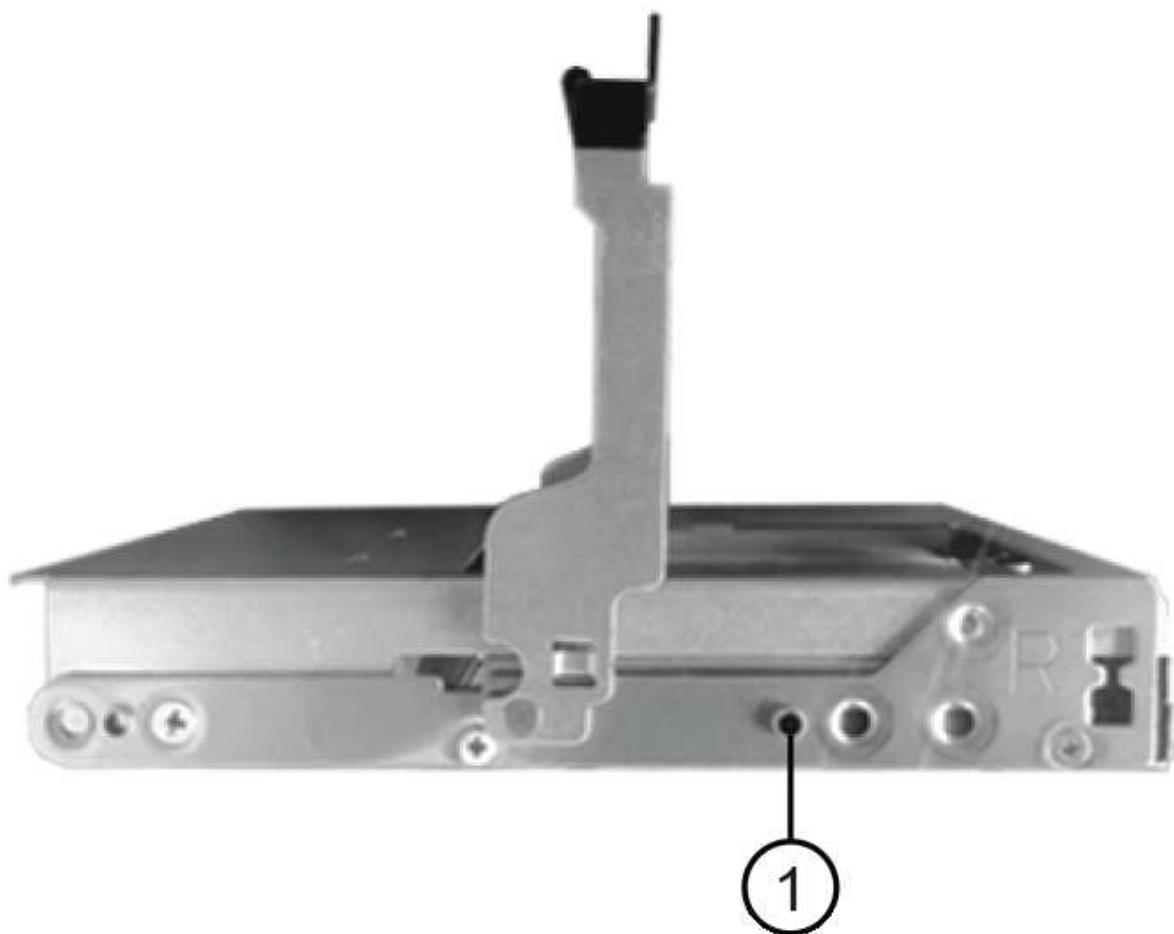
Install the replacement drive as soon as possible after removing the failed drive. Otherwise, there is a risk that the equipment might overheat.



Possible loss of data access — When pushing the drive drawer back into the enclosure, never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

Steps

1. Raise the cam handle on the new drive to vertical.
2. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.



(1) Raised button on the right side of the drive carrier

3. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.
4. Carefully push the drive drawer back into the enclosure. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.
5. Close the drive drawer by pushing both levers towards the center.

The green Activity LED for the replaced drive on the front of the drive drawer comes on when the drive is inserted correctly.

Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement

Confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced. (When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.)
 - Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
 - Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
 - Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.
2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.
5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace drive drawer in E2800 (60-drive shelf)

You can replace a drive drawer in an E2860 controller shelf or a DE460C drive shelf.

About this task

The steps to replace a failed drive drawer in an E2860 controller shelf or a DE460C drive shelf depend on whether the volumes in the drawer are protected by Drawer Loss Protection. If all volumes in the drive drawer are in disk pools or volume groups that have Drawer Loss Protection, you can perform this procedure online. Otherwise, you must stop all host I/O activity and power off the shelf before replacing the drive drawer.

Before you begin

- Review the drive drawer requirements in [Requirements for E2800 drive replacement](#).
- Make sure the drive shelf meets all of these conditions:
 - The drive shelf cannot be over temperature.
 - Both fans must be installed and have a status of Optimal.
 - All drive shelf components must be in place.
 - The volumes in the drive drawer cannot be in a Degraded state.



Possible loss of data access — If a volume is already in a Degraded state, and you remove drives from the drive drawer, the volume can fail.

What you'll need

- A replacement drive drawer.
- An ESD wristband, or you have taken other antistatic precautions.
- A flashlight.
- A permanent marker to note the exact location of each drive as you remove the drive from the drawer.
- Access to the storage array's command line interface (CLI). If you do not have access to the CLI, you can do one of the following:
 - **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
 - **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Step 1: Prepare to replace drive drawer

Determine if you can perform the replacement procedure while the drive shelf is online or if you need to stop host I/O activity and power off any of the shelves that are powered on.

If you are replacing a drawer in a shelf with Drawer Loss Protection, there is no need to stop host I/O activity and power off any of the shelves.

Steps

1. Determine if the drive shelf is powered on.
 - If the power is off, you do not need to issue the CLI command. Go to [Step 2: Remove cable chains](#).
 - If the power is on, go to the next step.
2. Access the CLI, and then enter the following command:

```
SMcli <ctrlr_IP1> -p "array_password" -c "set tray [trayID] drawer  
[drawerID]  
serviceAllowedIndicator=on;"
```

where:

- `<ctrlr_IP1>` is the identifier of the controller.
- `array_password` is the password for the storage array. You must enclose the value for `array_password` in double quotation marks ("").
- `[trayID]` is the identifier of the drive shelf that contains the drive drawer that you want to replace. Drive shelf ID values are 0 to 99. You must enclose the value for `trayID` in square brackets.
- `[drawerID]` is the identifier of the drive drawer that you want to replace. Drawer ID values are 1 (top drawer) to 5 (bottom drawer). You must enclose the value for `drawerID` in square brackets.

This command ensures you can remove the top-most drawer in drive shelf 10:

```
SMcli <ctrlr_IP1\> -p "safety-1" -c "set tray [10] drawer [1]  
serviceAllowedIndicator=forceOnWarning;"
```

3. Determine if you need to stop host I/O activity, as follows:

- If the command succeeds, you do not need to stop host I/O activity. All drives in the drawer are in pools or volume groups with Drawer Loss Protection. Go to [Step 2: Remove cable chains](#).



Possible damage to drives — Wait 30 seconds after the command completes before you open the drive drawer. Waiting 30 seconds allows the drives to spin down, which prevents possible damage to the hardware.

- If a warning is displayed indicating that this command could not be completed, you must stop host I/O activity before removing the drawer. The warning is displayed because one or more drives in the affected drawer are in pools or volume groups without Drawer Loss Protection. To avoid losing data, you must complete the next steps to stop host I/O activity and to power off the drive shelf and the controller shelf.

4. 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.



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.

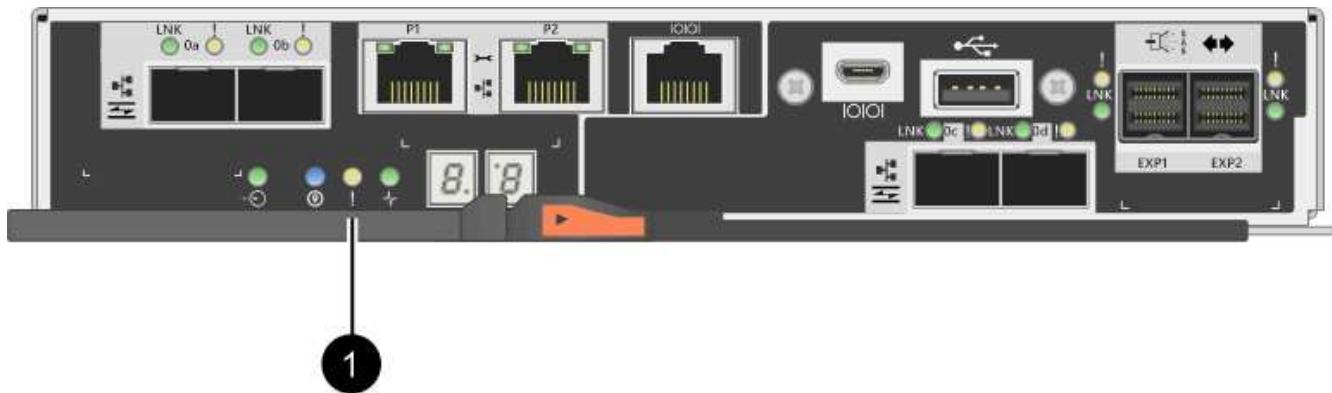
5. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose data because the storage array will not be accessible.

6. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**.

8. Wait for all operations to complete before continuing with the next step.

9. Power off the shelves, using one of the following procedures:

- *If you are replacing a drawer in a shelf with Drawer Loss Protection:* There is NO need to power off any of the shelves. You can perform the replace procedure while the drive drawer is online, because the Set Drawer Service Action Allowed Indicator CLI command completed successfully.
- *If you are replacing a drawer in a controller shelf without Drawer Loss Protection:*
 - a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to go dark.
- *If you are replacing a drawer in an expansion drive shelf without Drawer Loss Protection:*
 - a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to go dark.
 - c. Turn off both power switches on the drive shelf.
 - d. Wait two minutes for drive activity to stop.

Step 2: Remove cable chains

Remove both cable chains so you can remove and replace a failed drive drawer.

About this task

Each drive drawer has left and right cable chains. The left and right cable chains allow the drawers to slide in and out.

The metal ends on the cable chains slide into corresponding vertical and horizontal guide rails inside the enclosure, as follows:

- The left and right vertical guide rails connect the cable chain to the enclosure's midplane.
- The left and right horizontal guide rails connect the cable chain to the individual drawer.

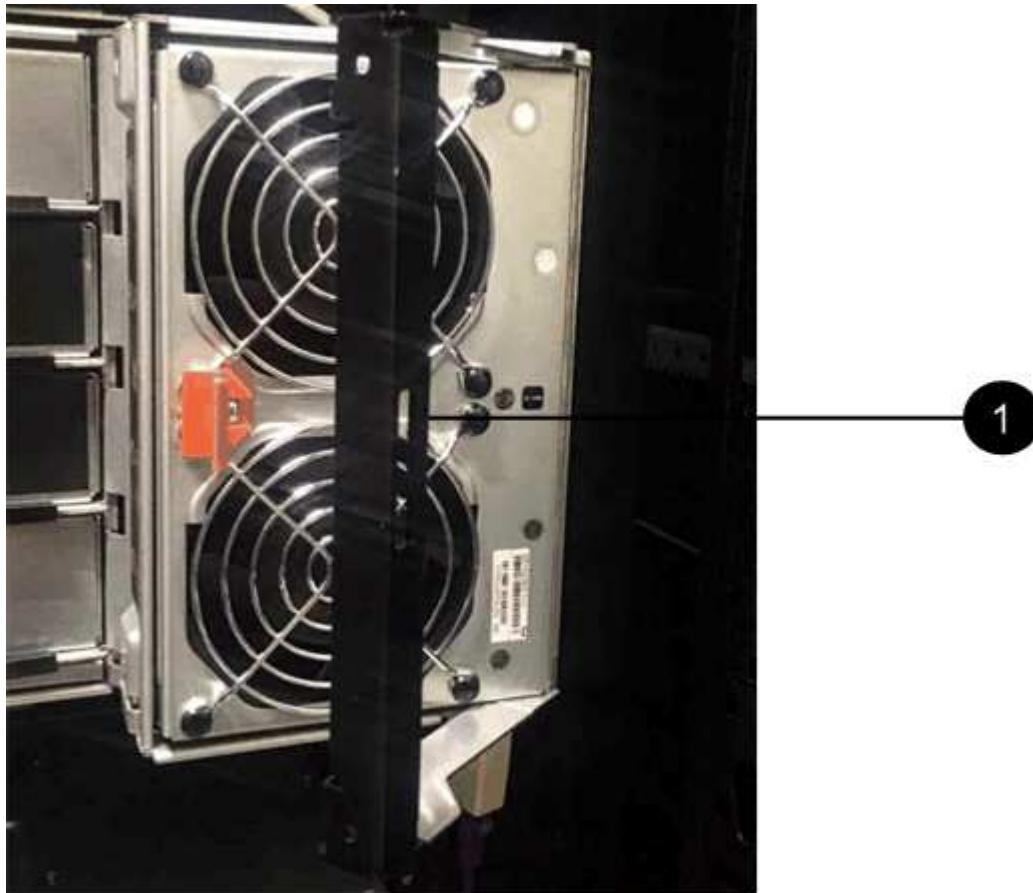


Possible hardware damage — If the drive tray is powered on, the cable chain is energized until both ends are unplugged. To avoid shorting out the equipment, do not allow the unplugged cable chain connector to touch the metal chassis if the other end of the cable chain is still plugged in.

Steps

1. Make sure that the drive shelf and controller shelf no longer has I/O activity and is powered off, or you have issued the Set Drawer Attention Indicator CLI command.
2. From the rear of the drive shelf, remove the right fan canister:
 - a. Press the orange tab to release the fan canister handle.

The figure shows the handle for the fan canister extended and released from the orange tab on the left.



(1) Fan canister handle

- b. Using the handle, pull the fan canister out of the drive tray, and set it aside.
- c. If the tray is powered on, ensure that the left fan goes to its maximum speed.



Possible equipment damage due to overheating — If the tray is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

3. Determine which cable chain to disconnect:

- If the power is on, the amber Attention LED on the front of the drawer indicates the cable chain you need to disconnect.
- If the power is off, you must manually determine which of the five cable chains to disconnect.
The figure shows the right side of the drive shelf with the fan canister removed. With the fan canister removed, you can see the five cable chains and the vertical and horizontal connectors for each drawer.

The top cable chain is attached to drive drawer 1. The bottom cable chain is attached to drive drawer 5. The callouts for drive drawer 1 are provided.



(1) Cable chain

(2) Vertical connector (connected to midplane)

(3) Horizontal connector (connected to drawer)

4. For easy access, use your finger to move the cable chain on the right side to the left.
5. Disconnect any of the right cable chains from their corresponding vertical guide rail.
 - a. Using a flashlight, locate the orange ring on the end of the cable chain that is connected to the vertical guide rail in the enclosure.



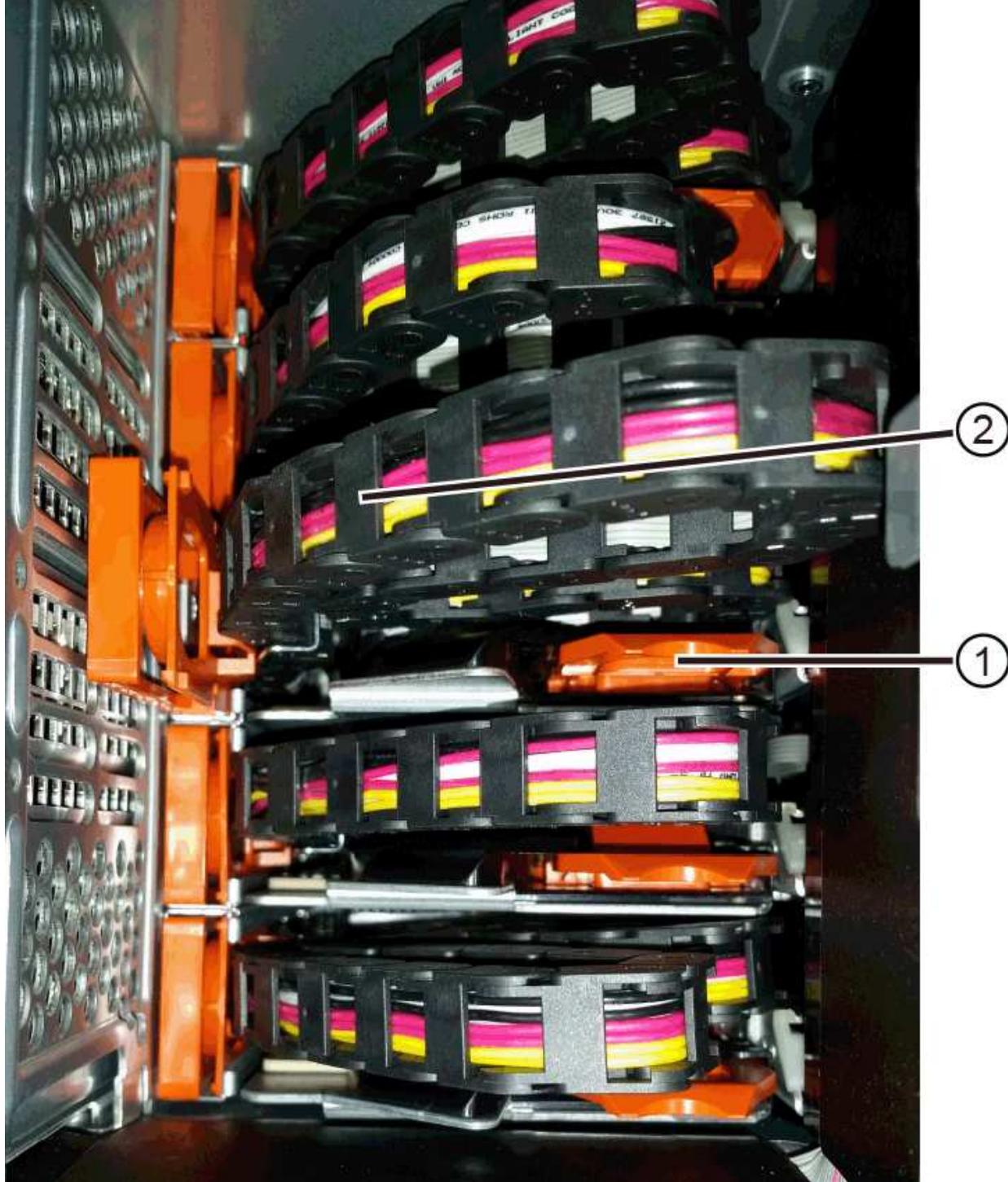
(1) Orange ring on vertical guide rail

(2) Cable chain, partially removed

- b. To unlatch the cable chain, insert your finger into the orange ring and press towards the middle of the system.

- c. To unplug the cable chain, carefully pull your finger toward you approximately 1 inch (2.5 cm). Leave the cable chain connector within the vertical guide rail. (If the drive tray is powered on, do not allow the cable chain connector to touch the metal chassis.)
6. Disconnect the other end of the cable chain:
 - a. Using a flashlight, locate the orange ring on the end of the cable chain that is attached to the horizontal guide rail in the enclosure.

The figure shows the horizontal connector on the right and the cable chain disconnected and partially pulled out on the left side.



(1) Orange ring on horizontal guide rail

(2) Cable chain, partially removed

- b. To unlatch the cable chain, gently insert your finger into the orange ring and push down.

The figure shows the orange ring on the horizontal guide rail (see item 1 in the figure above), as it is pushed down so that the rest of the cable chain can be pulled out of the enclosure.

- c. Pull your finger toward you to unplug the cable chain.

7. Carefully pull the entire cable chain out of the drive shelf.

8. Replace the right fan canister:

- a. Slide the fan canister all the way into the shelf.

- b. Move the fan canister handle until it latches with the orange tab.

- c. If the drive shelf is receiving power, confirm that the amber Attention LED on the back of the fan is not illuminated and that air is coming out the back of the fan.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the correct speed.

If the power is off, the fans do not run and the LED is not on.

9. From the back of the drive shelf, remove the left fan canister.

10. If the drive shelf is receiving power, ensure that the right fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

11. Disconnect the left cable chain from its vertical guide rail:

- a. Using a flashlight, locate the orange ring on the end of the cable chain attached to the vertical guide rail.
- b. To unlatch the cable chain, insert your finger into the orange ring.
- c. To unplug the cable chain, pull toward you approximately 1 inch (2.5 cm). Leave the cable chain connector within the vertical guide rail.



Possible hardware damage — If the drive tray is powered on, the cable chain is energized until both ends are unplugged. To avoid shorting out the equipment, do not allow the unplugged cable chain connector to touch the metal chassis if the other end of the cable chain is still plugged in.

12. Disconnect the left cable chain from the horizontal guide rail, and pull the entire cable chain out of the drive shelf.

If you are performing this procedure with the power on, all LEDs turn off when you disconnect the last cable chain connector, including the amber Attention LED.

13. Replace the left fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is not illuminated and that air is coming out the back of the fan.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the

correct speed.

Step 3: Remove failed drive drawer

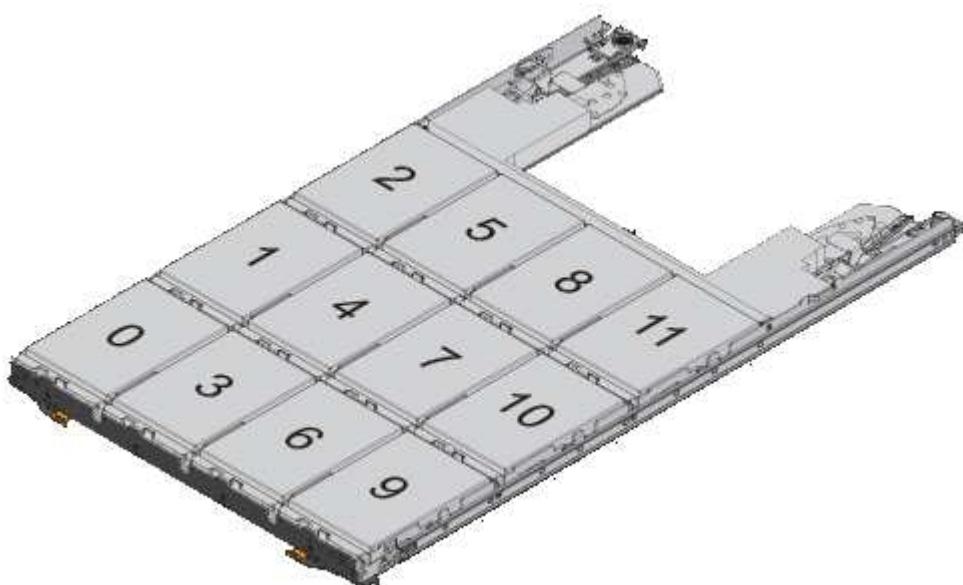
Remove a failed drive drawer to replace it with a new one.



Possible loss of data access — Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry. To avoid loss of data access and damage to the drives, always keep drives away from magnetic devices.

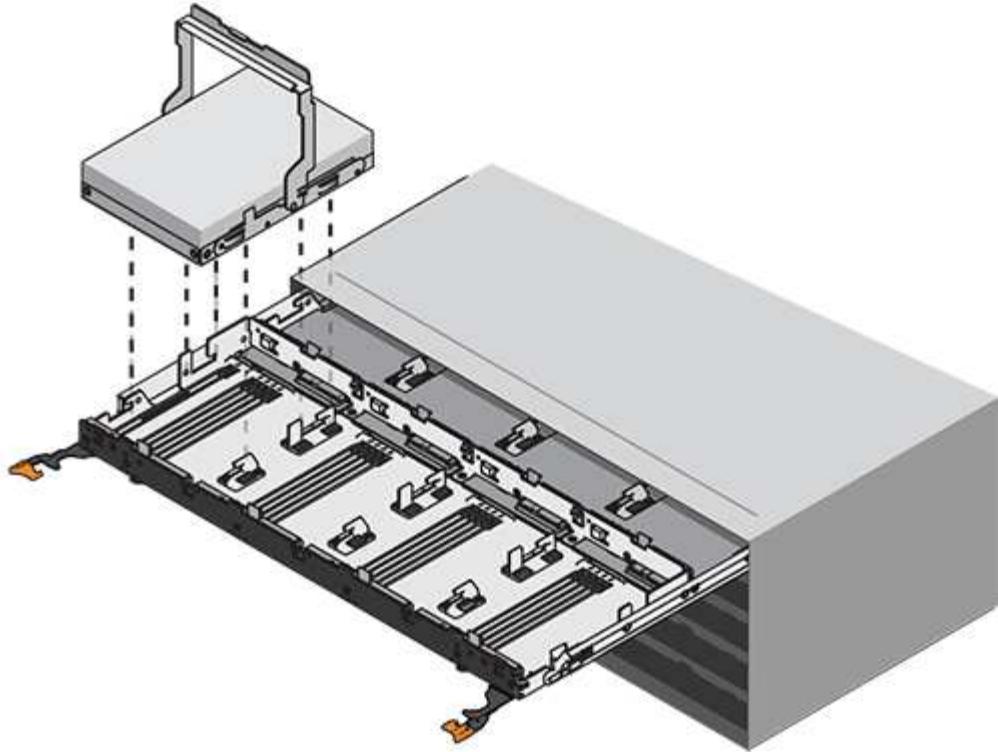
Steps

1. Make sure that:
 - The right and left cable chains are disconnected.
 - The right and left fan canisters are replaced.
2. Remove the bezel from the front of the drive shelf.
3. Unlatch the drive drawer by pulling out on both levers.
4. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
5. If volumes have already been created and assigned, use a permanent marker to note the exact location of each drive. For example, using the following drawing as a reference, write the appropriate slot number on the top of each drive.

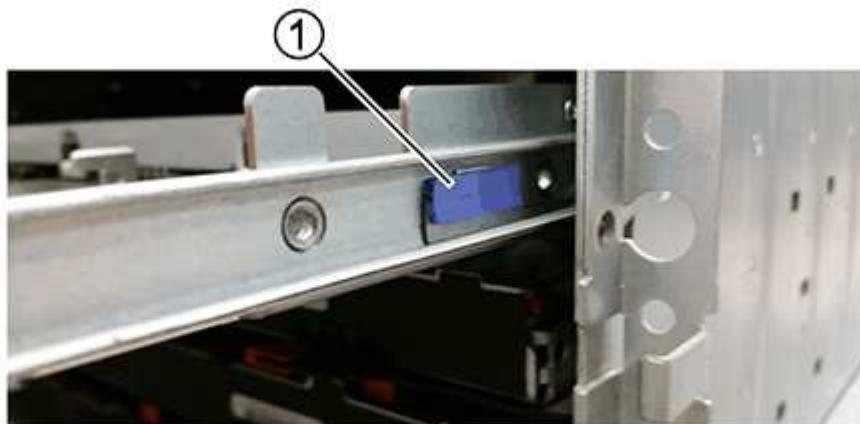


Possible loss of data access — Make sure to record the exact location of each drive before removing it.

6. Remove the drives from the drive drawer:
 - a. Gently pull back the orange release latch that is visible on the center front of each drive.
 - b. Raise the drive handle to vertical.
 - c. Use the handle to lift the drive from the drive drawer.



- d. Place the drive on a flat, static-free surface and away from magnetic devices.
- 7. Remove the drive drawer:
 - a. Locate the plastic release lever on each side of the drive drawer.



(1) Drive drawer release lever

- b. Disengage both release levers by pulling the latches toward you.
- c. While holding both release levers, pull the drive drawer toward you.
- d. Remove the drive drawer from the drive shelf.

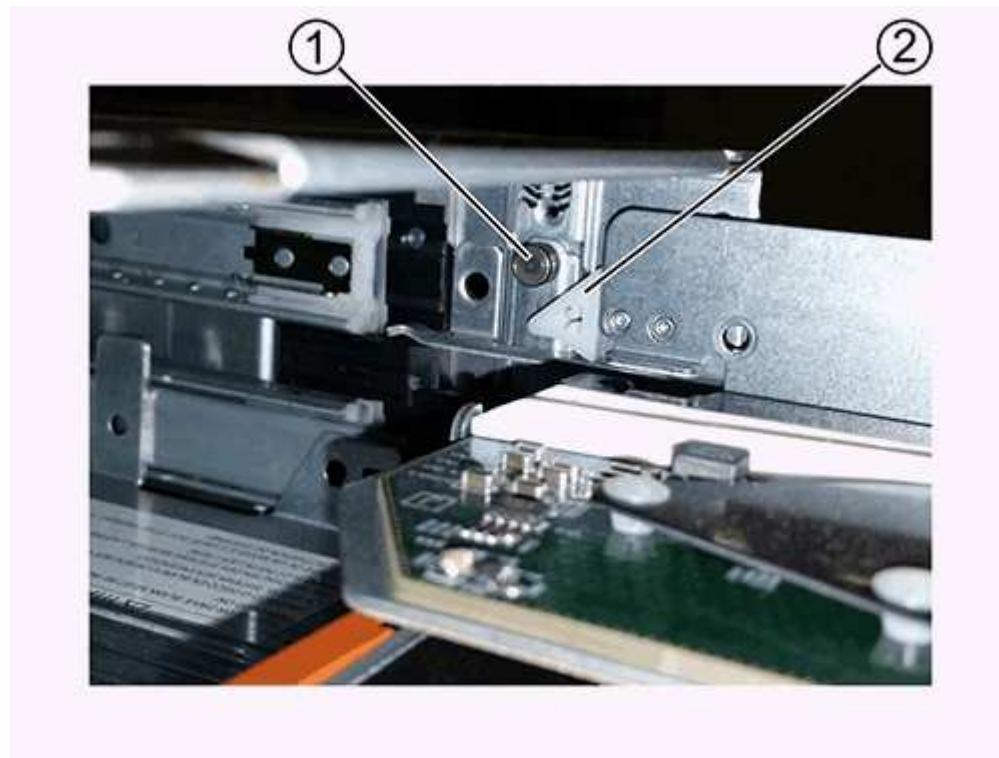
Step 4: Install new drive drawer

Install a new drive drawer to replace the failed one.

Steps

1. From the front of the drive shelf, shine a flashlight into the empty drawer slot, and locate the lock-out tumbler for that slot.

The lock-out tumbler assembly is a safety feature that prevents you from being able to open more than one drive drawer at one time.



(1) Lock-out tumbler

(2) Drawer guide

2. Position the replacement drive drawer in front of the empty slot and slightly to the right of center.

Positioning the drawer slightly to the right of center helps to ensure that the lock-out tumbler and the drawer guide are correctly engaged.

3. Slide the drive drawer into the slot, and ensure that the drawer guide slides under the lock-out tumbler.



Risk of equipment damage — Damage occurs if the drawer guide does not slide under the lock-out tumbler.

4. Carefully push the drive drawer all the way in until the latch fully engages.

Experiencing a higher level of resistance is normal when pushing the drawer closed for the first time.



Risk of equipment damage — Stop pushing the drive drawer if you feel binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, reinsert the drawer into the slot, ensure the tumbler is above the rail, and the rails are aligned correctly.

Step 5: Attach cable chains

Attach the cable chains so you can safely re-install the drives in the drive drawer.

About this task

When attaching a cable chain, reverse the order you used when disconnecting the cable chain. You must insert the chain's horizontal connector into the horizontal guide rail in the enclosure before inserting the chain's vertical connector into the vertical guide rail in the enclosure.

Steps

1. Make sure that:
 - A new drive drawer installed.
 - You have two replacement cable chains, marked as LEFT and RIGHT (on the horizontal connector next to the drive drawer).
2. From the back of the drive shelf, remove the fan canister on the right side, and set it aside.
3. If the shelf is powered on, ensure that the left fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

4. Attach the right cable chain:
 - a. Locate the horizontal and vertical connectors on the right cable chain and the corresponding horizontal guide rail and vertical guide rail inside the enclosure.
 - b. Align both cable chain connectors with their corresponding guide rails.
 - c. Slide the cable chain's horizontal connector onto the horizontal guide rail, and push it in as far as it can go.



Risk of equipment malfunction — Make sure to slide the connector into the guide rail. If the connector rests on the top of the guide rail, problems might occur when the system runs.

The figure shows the horizontal and vertical guide rails for the second drive drawer in the enclosure.



(1) Horizontal guide rail

(2) Vertical guide rail

- d. Slide the vertical connector on the right cable chain into the vertical guide rail.
- e. After you have reconnected both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.



Risk of equipment malfunction — If the connectors are not latched, the cable chain might come loose during drawer operation.

5. Reinstall the right fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is now off and that air is now coming out of the back.

The LED could remain on for as long as a minute after you reinstall the fan while the fan settles into the correct speed.

6. From the back of the drive shelf, remove the fan canister on the left side of the shelf.
7. If the shelf is powered on, ensure that the right fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

8. Reattach the left cable chain:

- a. Locate the horizontal and vertical connectors on the cable chain and their corresponding horizontal and vertical guide rails inside the enclosure.
- b. Align both cable chain connectors with their corresponding guide rails.
- c. Slide the cable chain's horizontal connector into the horizontal guide rail and push it in as far as it will go.



Risk of equipment malfunction — Make sure to slide the connector within the guide rail. If the connector rests on the top of the guide rail, problems might occur when the system runs.

- d. Slide the vertical connector on the left cable chain into the vertical guide rail.
- e. After you reconnect both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.



Risk of equipment malfunction — If the connectors are not latched, the cable chain might come loose during drawer operation.

9. Reinstall the left fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is now off and that air is now coming out of the back.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the correct speed.

Step 6: Complete drive drawer replacement

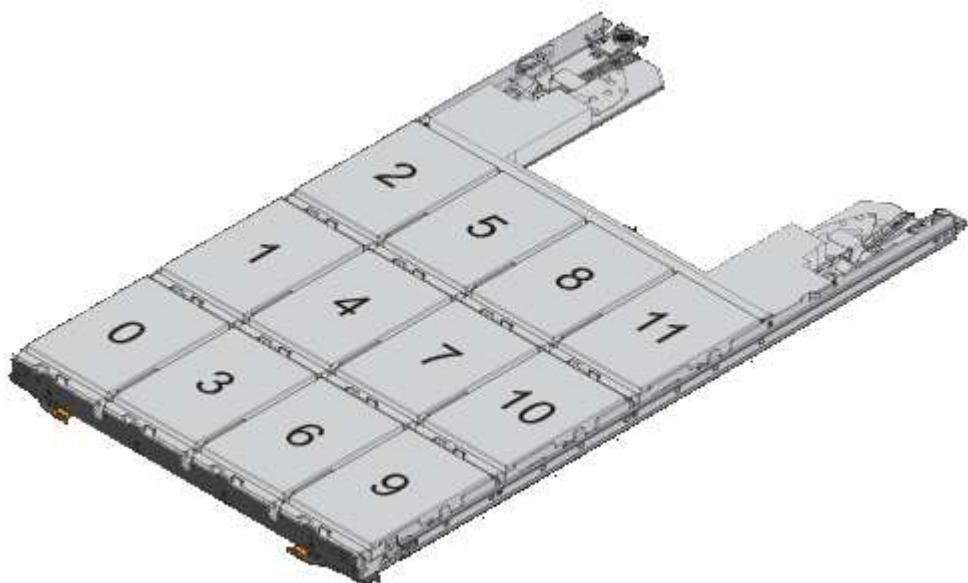
Reinsert the drives and replace the front bezel in the correct order.



Possible loss of data access — You must install each drive in its original location in the drive drawer.

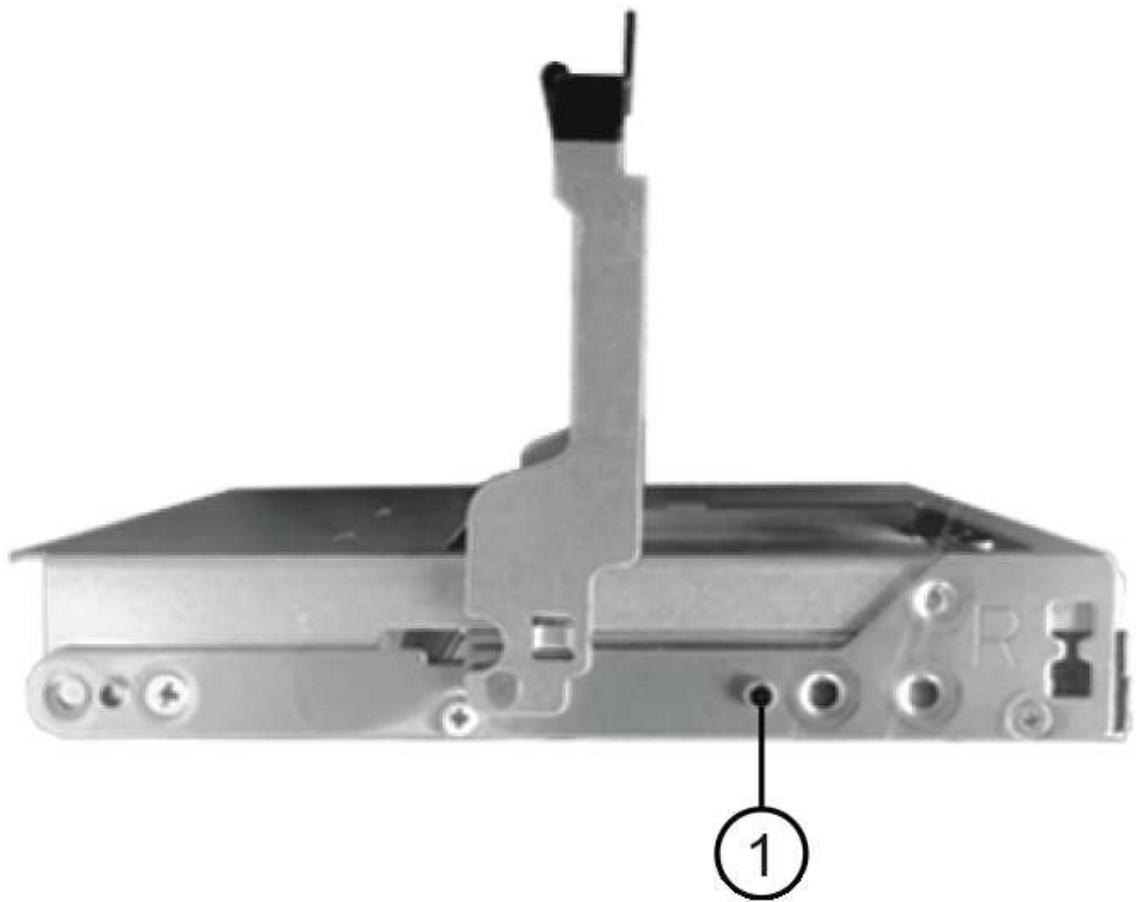
Steps

1. Make sure that:
 - You know where to install each drive.
 - You have replaced the drive drawer.
 - You have installed the new drawer cables.
2. Reinstall the drives in the drive drawer:
 - a. Unlatch the drive drawer by pulling out on both levers at the front of the drawer.
 - b. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
 - c. Determine which drive to install in each slot by using the notes you made when removing the drives.



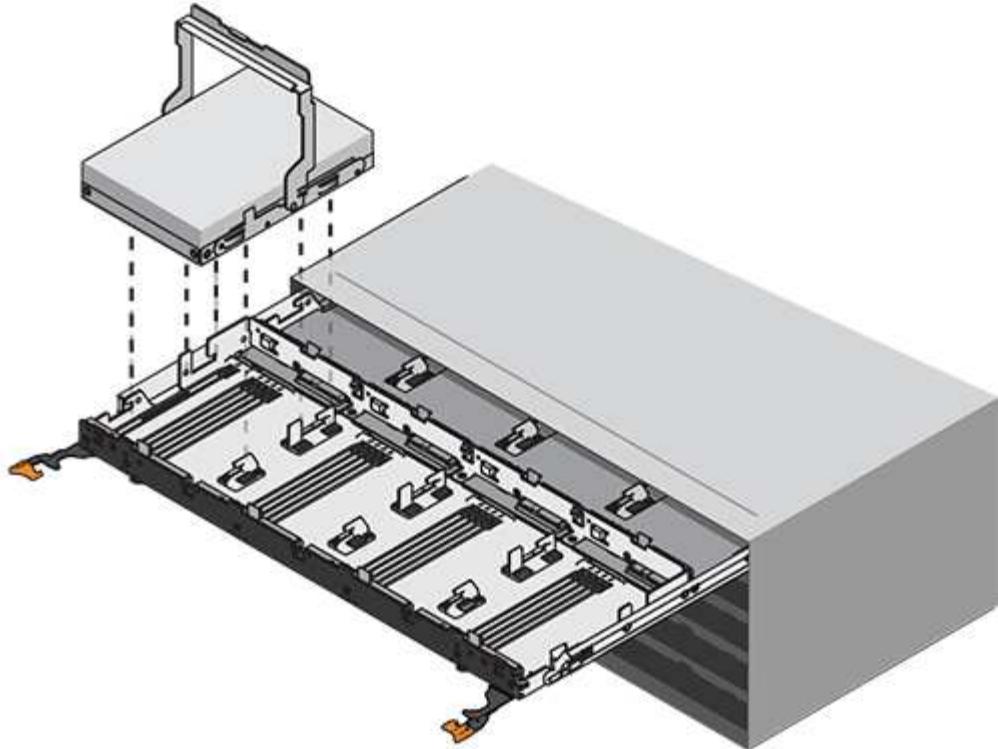
- d. Raise the handle on the drive to vertical.
- e. Align the two raised buttons on each side of the drive with the notches on the drawer.

The figure shows the right side view of a drive, showing the location of the raised buttons.



(1) Raised button on the right side of the drive

- f. Lower the drive straight down, making sure the drive is pressed all the way down into the bay, and then rotate the drive handle down until the drive snaps into place.



- g. Repeat these steps to install all the drives.
 3. Slide the drawer back into the drive shelf by pushing it from the center and closing both levers.
- Risk of equipment malfunction** — Make sure to completely close the drive drawer by pushing both levers. You must completely close the drive drawer to allow proper airflow and prevent overheating.
4. Attach the bezel to the front of the drive shelf.
 5. If you have powered down one or more shelves, reapply power using one of the following procedures:
 - *If you replaced a drive drawer in a controller shelf without Drawer Loss Protection:*
 - a. Turn on both power switches on the controller shelf.
 - b. Wait 10 minutes for the power-on process to complete.
Confirm that both fans come on and that the amber LED on the back of the fans is off.
 - *If you replaced a drive drawer in an expansion drive shelf without Drawer Loss Protection:*
 - a. Turn on both power switches on the drive shelf.
 - b. Confirm that both fans come on and that the amber LED on the back of the fans is off.
 - c. Wait two minutes before applying power to the controller shelf.
 - d. Turn on both power switches on the controller shelf.
 - e. Wait 10 minutes for the power-on process to complete.
Confirm that both fans come on and that the amber LED on the back of the fans is off.

What's next?

Your drive drawer replacement is complete. You can resume normal operations.

Host interface cards

Requirements for E2800 HIC replacement

Before you add, upgrade, or replace a host interface card (HIC) in an E2800, review the requirements and considerations.

Procedure overview

The steps to replace a HIC depend on whether you have one or two controllers, as follows:

| If your storage array has... | You must... |
|--|---|
| One controller (E2812 or E2824 simplex) | <ol style="list-style-type: none">1. Stop host I/O operations2. Power down the controller shelf3. Remove the controller canister4. Replace the battery5. Replace the controller canister6. Apply power to the controller shelf |
| Two controllers (E2860, E2812 or E2824 duplex) | <ol style="list-style-type: none">1. Take the controller offline2. Remove the controller canister3. Replace the battery4. Replace the controller canister5. Bring the controller online |

Requirements for adding, upgrading, or replacing a HIC

If you plan to add, upgrade, or replace a host interface card (HIC), keep the following requirements in mind.

- You have scheduled a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)
- You have one or two HICs, based on whether you have one or two controllers in your storage array. The HICs must be compatible with your controllers.

If you have a duplex configuration (two controllers), the HICs installed in the two controller canisters must be identical. The presence of mismatched HICs causes the controller with the replacement HIC to lock down when you bring it online.

- You have all cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- You have an ESD wristband, or you have taken other antistatic precautions.

- You have a #1 Phillips screwdriver.
- You have labels to identify each cable that is connected to the controller canister.
- You have a management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Add E2800 host interface card (HIC)

You can add a host interface card (HIC) to E2800 controller canisters with baseboard host ports. This addition increases the number of host ports in your E2800 storage array and provides additional host protocols.

About this task

During this procedure, you must power off the storage array, install the HIC, and reapply power.

Before you begin

- Review [Requirements for E2800 HIC replacement](#).
- Schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)

What you'll need

- One or two HICs, based on whether you have one or two controllers in your storage array. The HICs must be compatible with your controllers.
- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- Any required host hardware installed for the new host ports, such as switches or host bus adapters (HBAs).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) and the [NetApp Hardware Universe](#).

- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to add HIC

Prepare to add the HIC by backing up the storage array's configuration database, collecting support data, and stopping host I/O operations. Then, you can power down the controller shelf.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. 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.



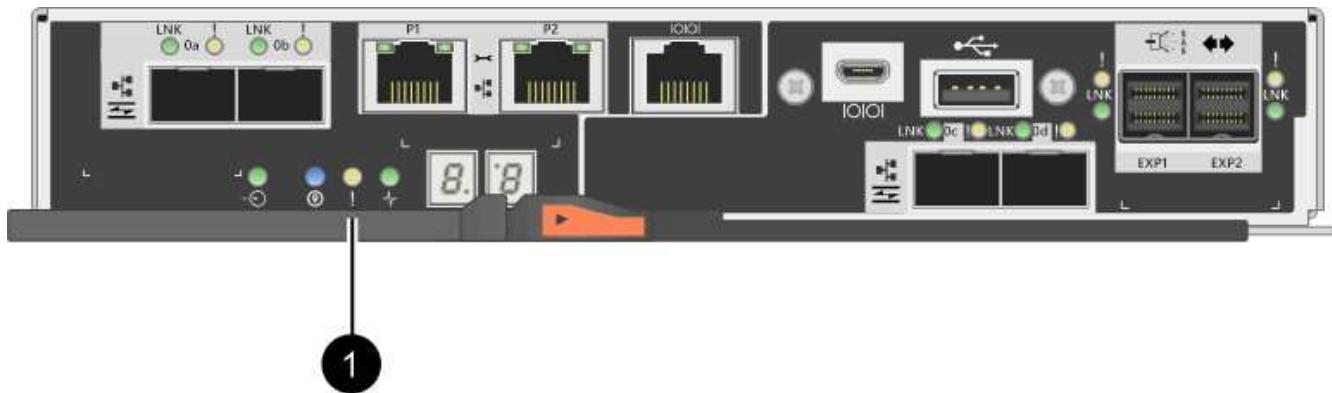
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose access to the data because the storage is not accessible.

5. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
6. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
8. Power down the controller shelf.
 - a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can add the new host interface card.

Steps

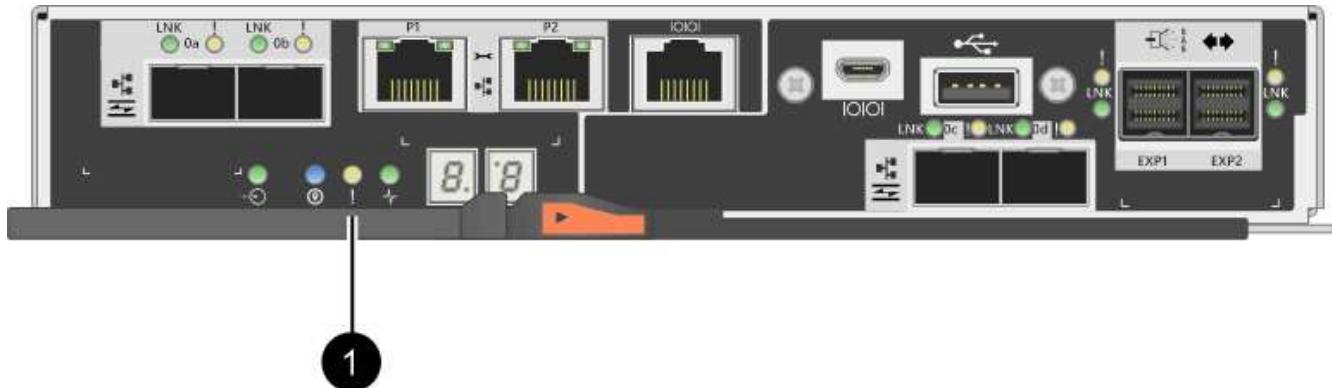
1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



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

3. Confirm that the Cache Active LED on the back of the controller is off.

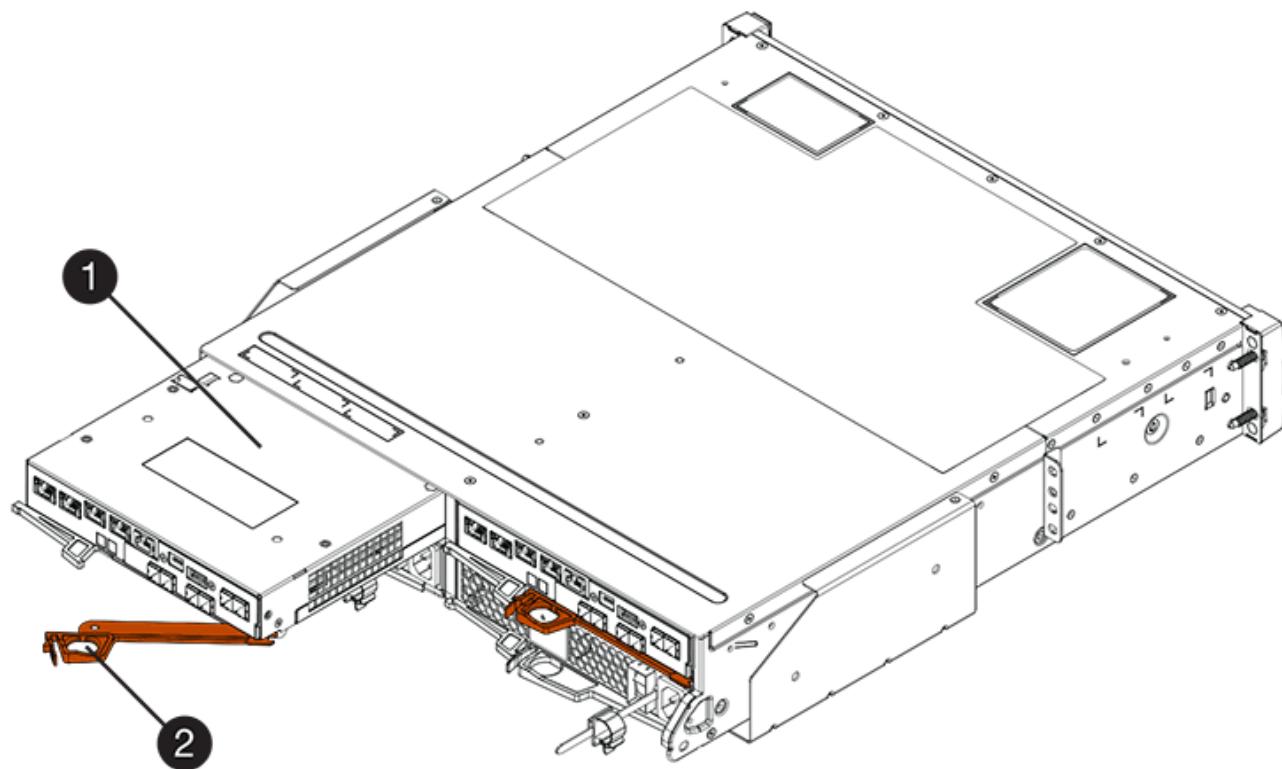
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

4. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

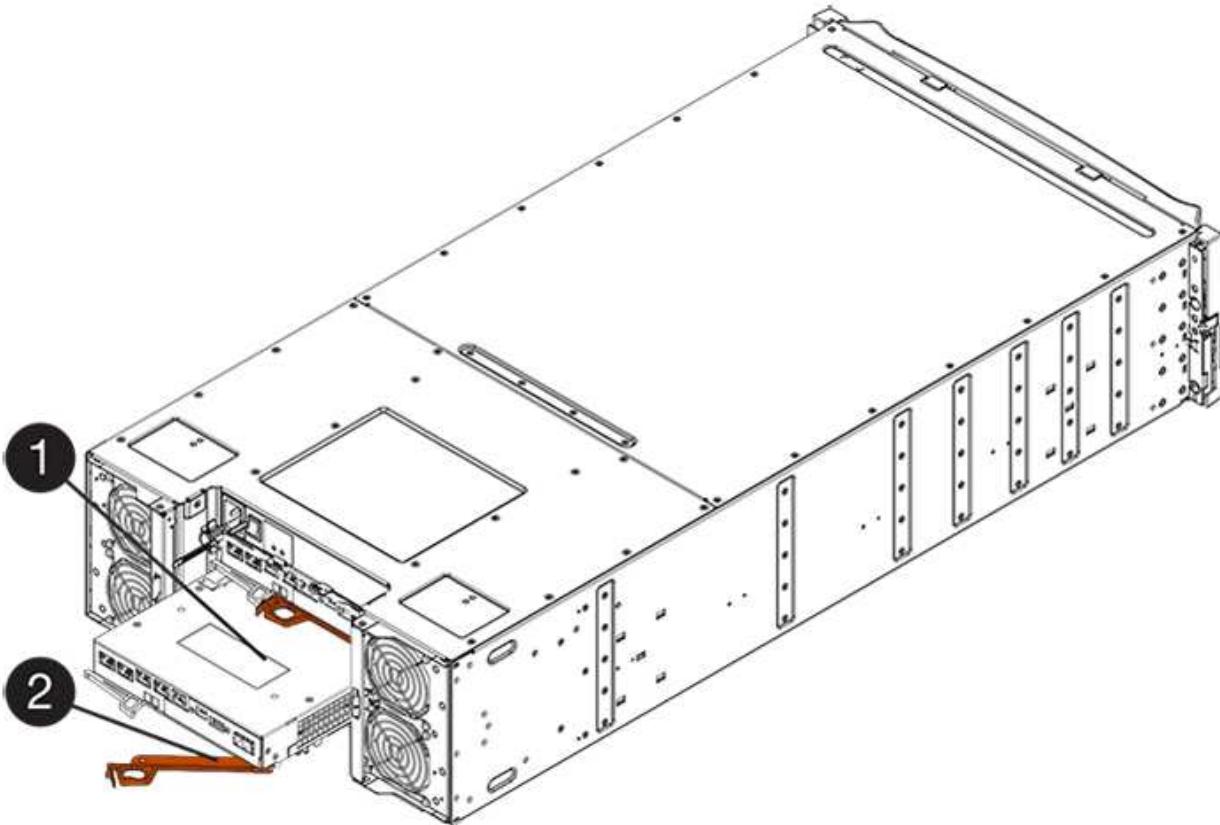
The following figure is an example of an E2812 controller shelf, E2824 controller shelf, or EF280 flash array:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

5. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E2812 controller shelf, E2824 controller shelf or EF280 flash array, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

6. Turn the controller canister over, so that the removable cover faces up.
7. Place the controller canister on a flat, static-free surface.

Step 3: Install the HIC

Install the HIC to increase the number of host ports in your storage array.



Possible loss of data access — Never install a HIC in an E2800 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs will cause the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Press the button on the cover of the controller canister, and slide the cover off.
3. Confirm that the green LED inside the controller (by the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active

(2) Battery

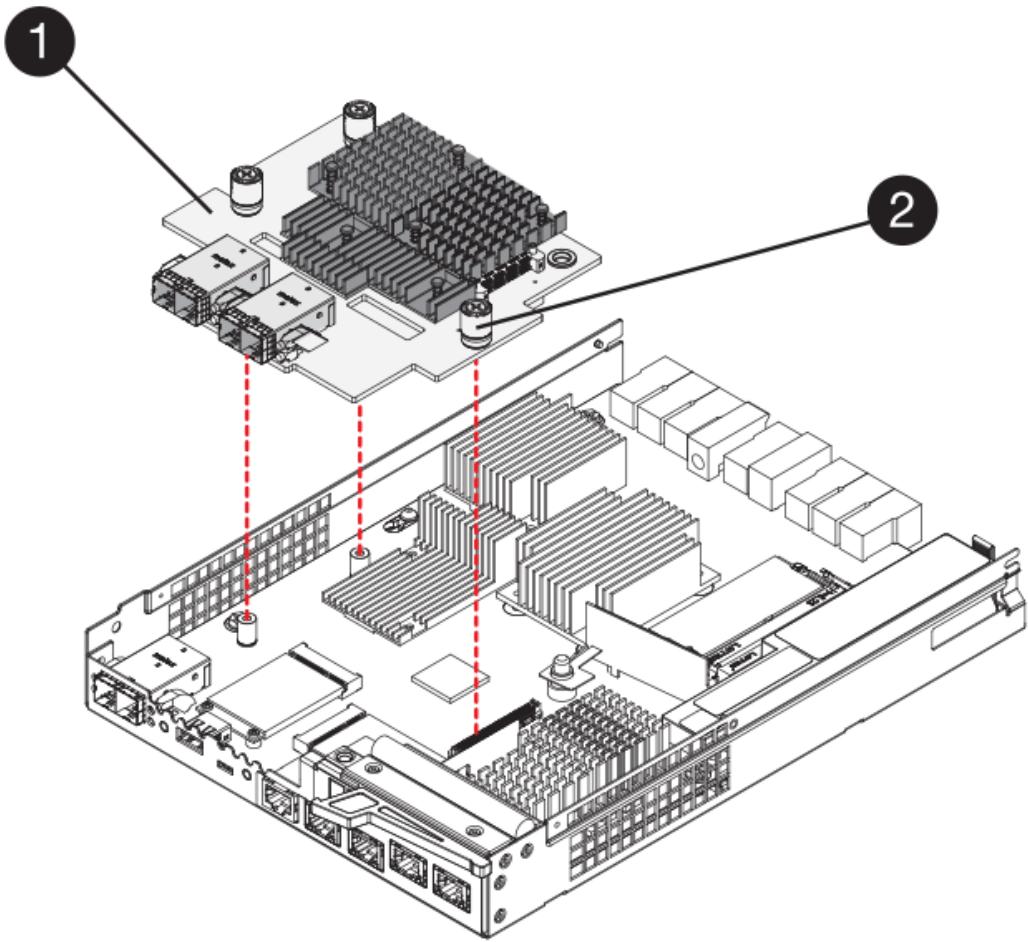
4. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the controller canister, and remove the faceplate.
5. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

6. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



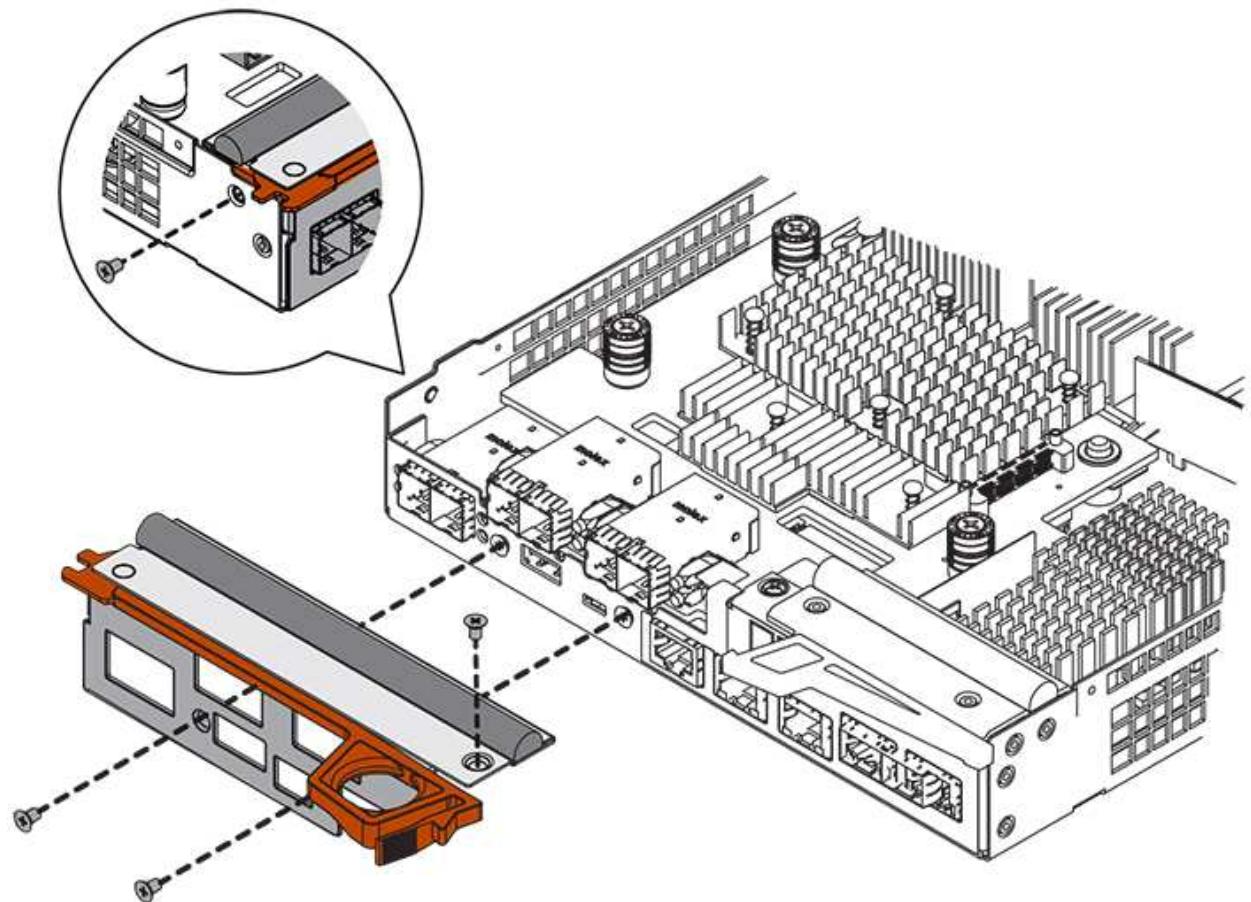
(1) Host interface card (HIC)

(2) Thumbscrews

7. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

8. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.



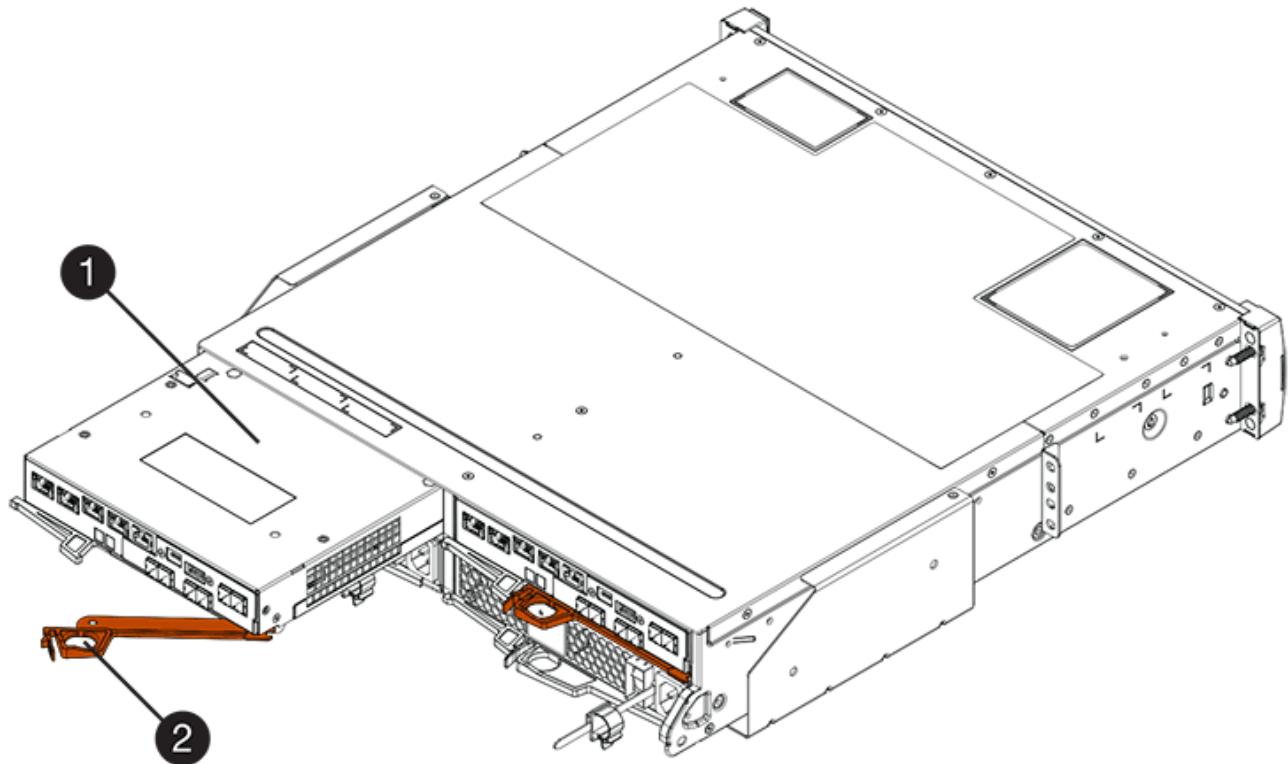
Step 4: Reinstall controller canister

Reinstall the controller canister into the controller shelf after installing the new HIC.

Steps

1. Turn the controller canister over, so that the removable cover faces down.
2. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

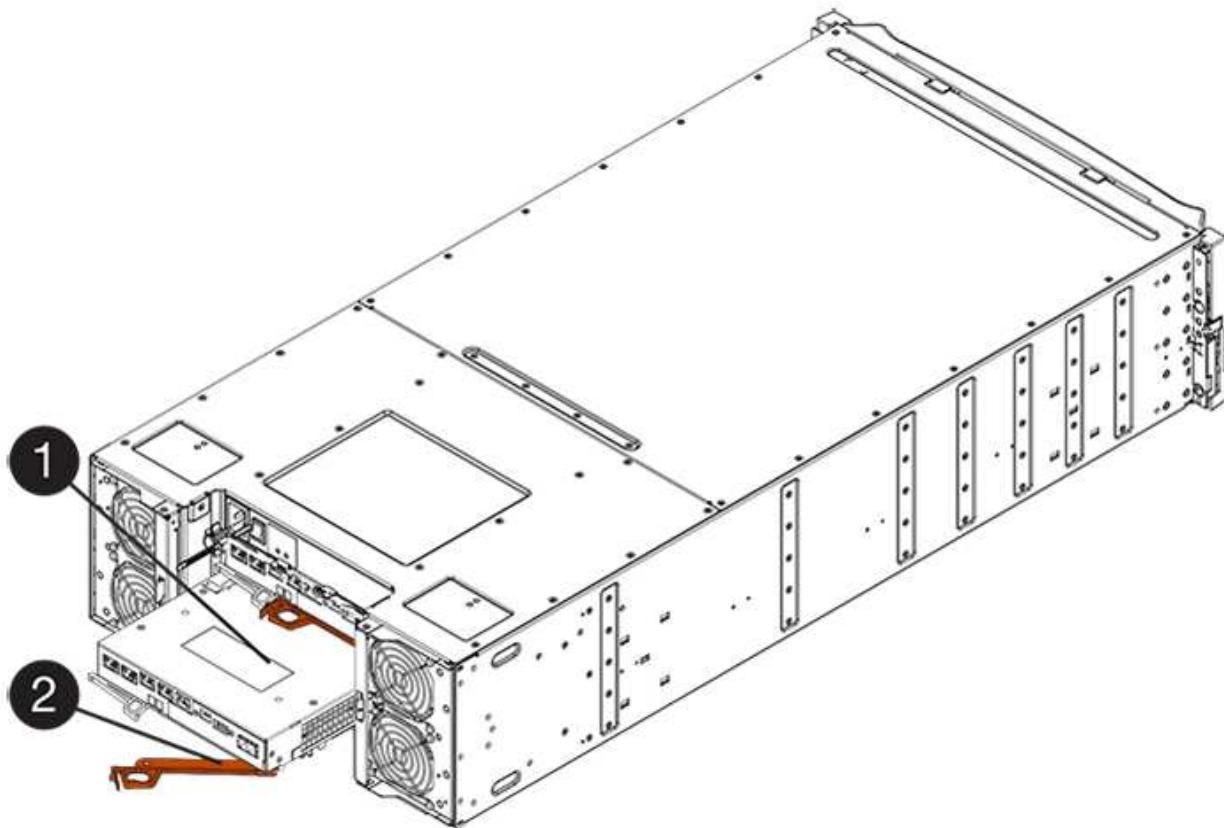
The following figure is an example of an E2824 controller shelf, or EF280 flash array:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

3. Move the cam handle to the left to lock the controller canister in place.
4. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

5. (Optional) If you are adding HICs to a duplex configuration, repeat all steps to remove the second controller canister, install the second HIC, and reinstall the second controller canister.

Step 5: Complete HIC addition

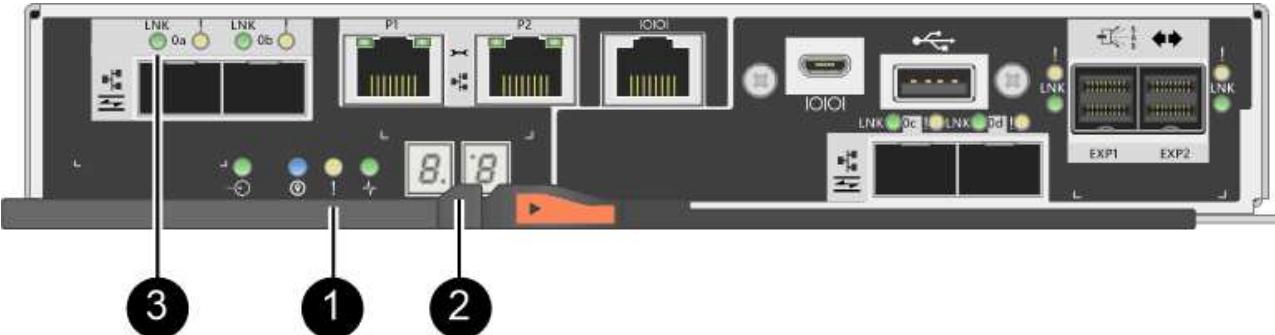
Check the controller LEDs and seven-segment display, and then confirm that the controller's status is Optimal.

Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS, Sd, blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
 - The amber Attention LED on the controller turns on and then turns off, unless there is an error.
 - The green Host Link LEDs remain off until you connect the host cables.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Attention LED (amber)

(2) Seven-segment display

(3) Host Link LEDs

3. From SANtricity System Manager, confirm that the controller's status is Optimal.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly

seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

4. If the new HIC ports require SFP+ transceivers, install these SFPs.
5. If you installed a HIC with SFP+ (optical) ports, confirm the new ports have the host protocol you expect.
 - a. From SANtricity System Manager, select **Hardware**.
 - b. If the graphic shows the drives, click **Show back of shelf**.
 - c. Select the graphic for either Controller A or Controller B.
 - d. Select **View settings** from the context menu.
 - e. Select the **Host Interfaces** tab.
 - f. Click **Show more settings**.
- g. Review the details shown for the HIC ports (the ports labelled **e0x** or **0x** in HIC Location **slot 1**) to determine if you are ready to connect the host ports to the data hosts:
 - *If the new HIC ports have the protocol you expect:* You are ready to connect the new HIC ports to the data hosts; go to the next step.
 - *If the new HIC ports do not have the protocol you expect:* You must apply a software feature pack before you can connect the new HIC ports to the data hosts. See [Change host protocol for E2800](#). Then, connect the host ports to the data hosts and resume operations.
6. Connect the cables from the controller's host ports to the data hosts.

If you need instructions for configuring and using a new host protocol, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

What's next?

The process of adding a host interface card to your storage array is complete. You can resume normal operations.

Upgrade E2800 host interface card (HIC)

You can upgrade a host interface card (HIC) in an E2800 array to increase the number of host ports or to change host protocols.

About this task

When you upgrade the HICs, you must power off the storage array, remove the existing HIC from each controller, install a new HIC, and reapply power.

Before you begin

- Review [Requirements for E2800 HIC replacement](#).
- Schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)

What you'll need

- One or two HICs, based on whether you have one or two controllers in your storage array. The HICs must

be compatible with your controllers.

- Labels to identify each cable that is connected to the controller canister.
- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- Any new host hardware installed for the new host ports, such as switches or host bus adapters (HBAs).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to upgrade host interface cards

Prepare to upgrade host interface cards (HICs) by backing up the storage array's configuration database, collecting support data, and stopping host I/O operations. Then, you can power down the controller shelf.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. 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.



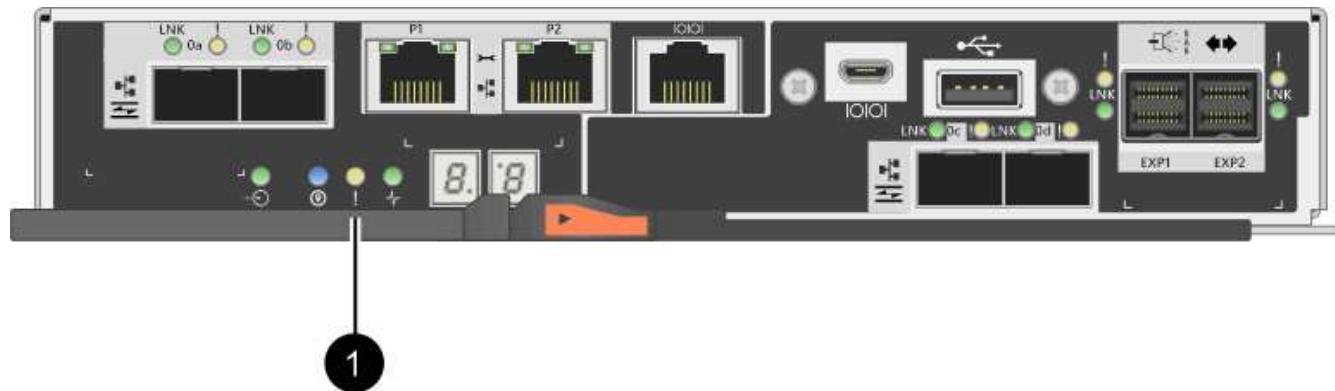
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose access to the data because the storage is not accessible.

5. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
6. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
8. Power down the controller shelf.
- a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

You remove the controller canister so you can upgrade the new host interface card (HIC). When you remove a controller canister, you must disconnect all cables. Then, you can slide the controller canister out of the controller shelf.

Steps

1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



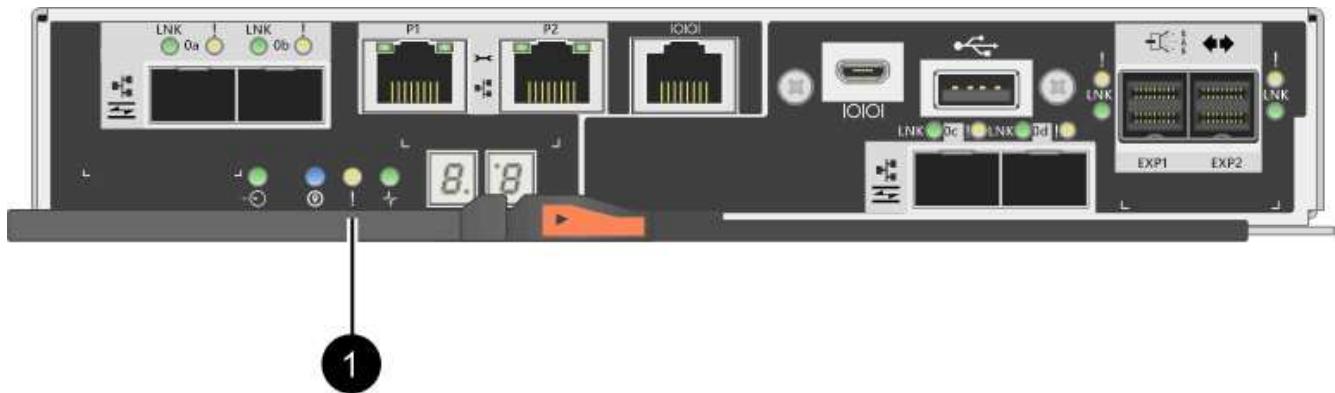
To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

3. If the HIC ports use SFP+ transceivers, remove them.

Depending on what type of HIC you are upgrading to, you might be able to reuse these SFPs.

4. Confirm that the Cache Active LED on the back of the controller is off.

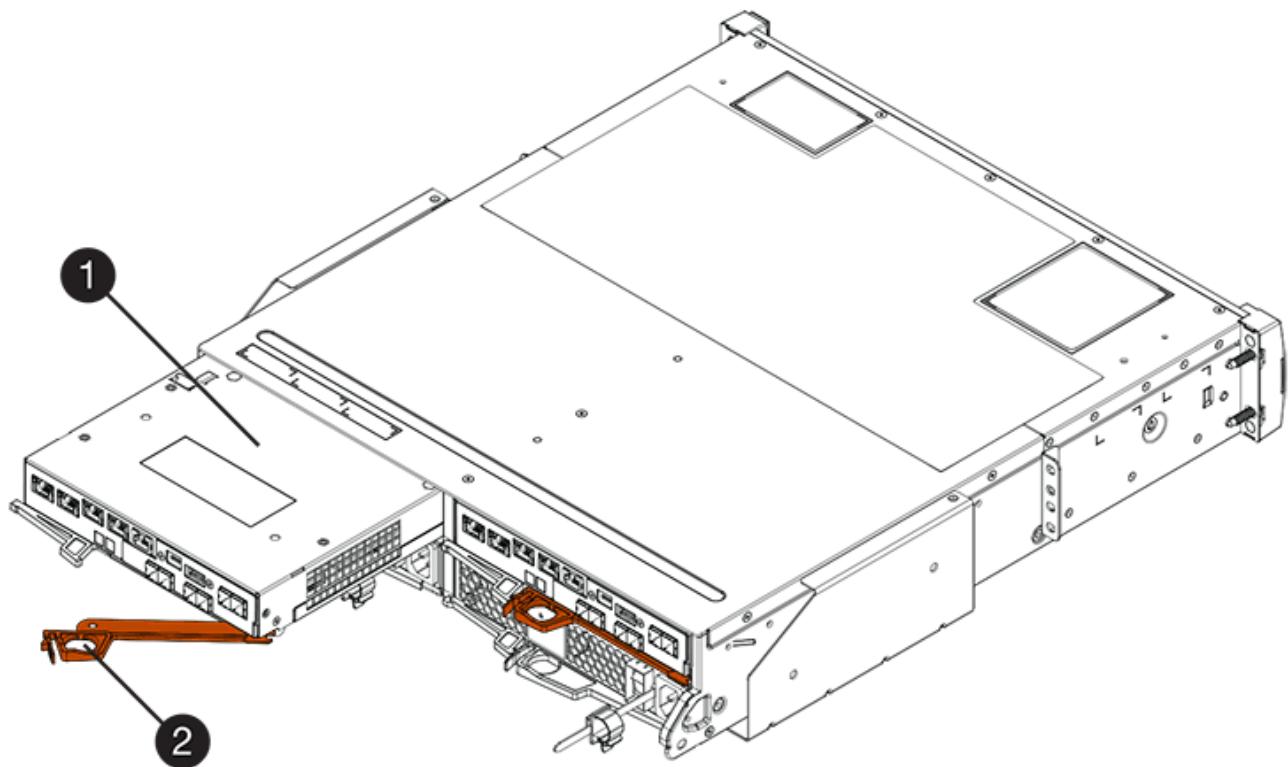
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

5. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

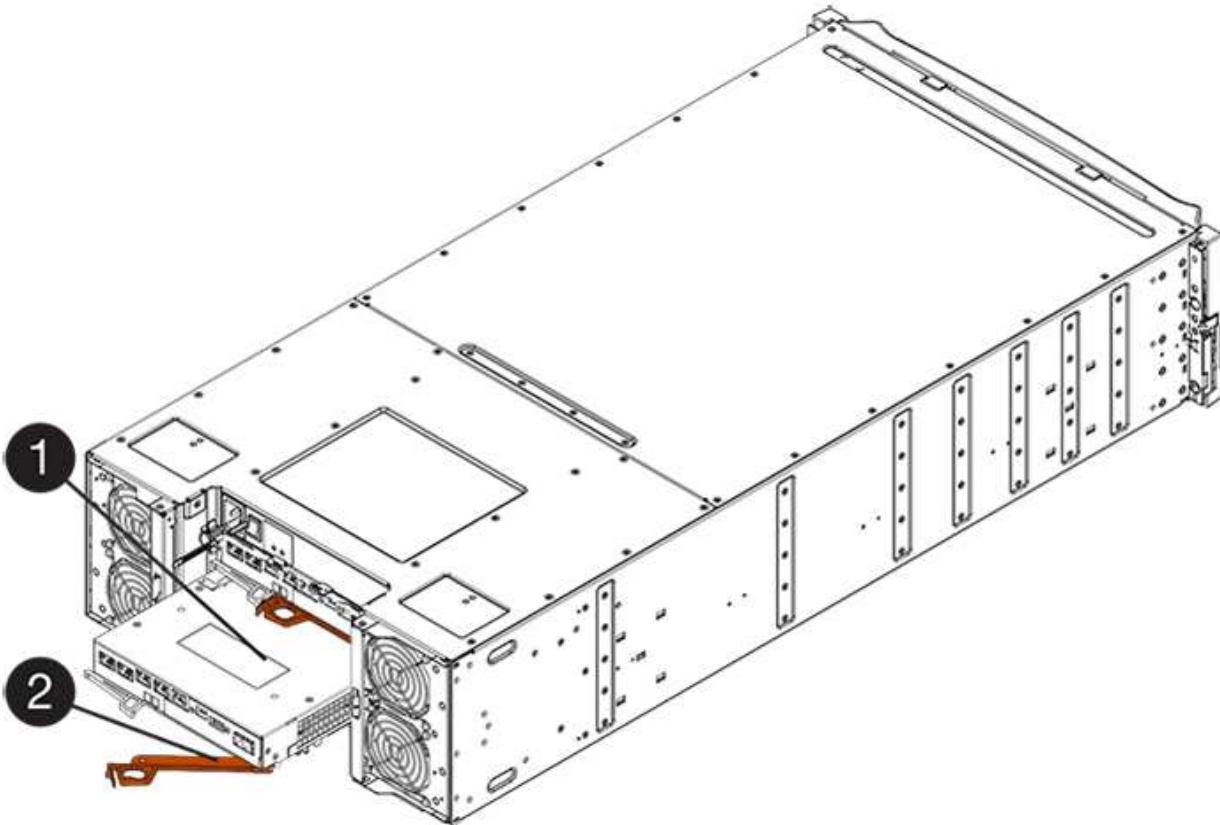
The following figure is an example of an E2812 controller shelf, E2824 controller shelf, or EF280 flash array:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

- Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E2812 controller shelf, E2824 controller shelf or EF280 flash array, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

- Turn the controller canister over, so that the removable cover faces up.
- Place the controller canister on a flat, static-free surface.

Step 3: Remove a host interface card

Remove the original host interface card (HIC) so you can replace it with an upgraded one.

Steps

- Remove the controller canister's cover by pressing down on the button and sliding the cover off.
- Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.

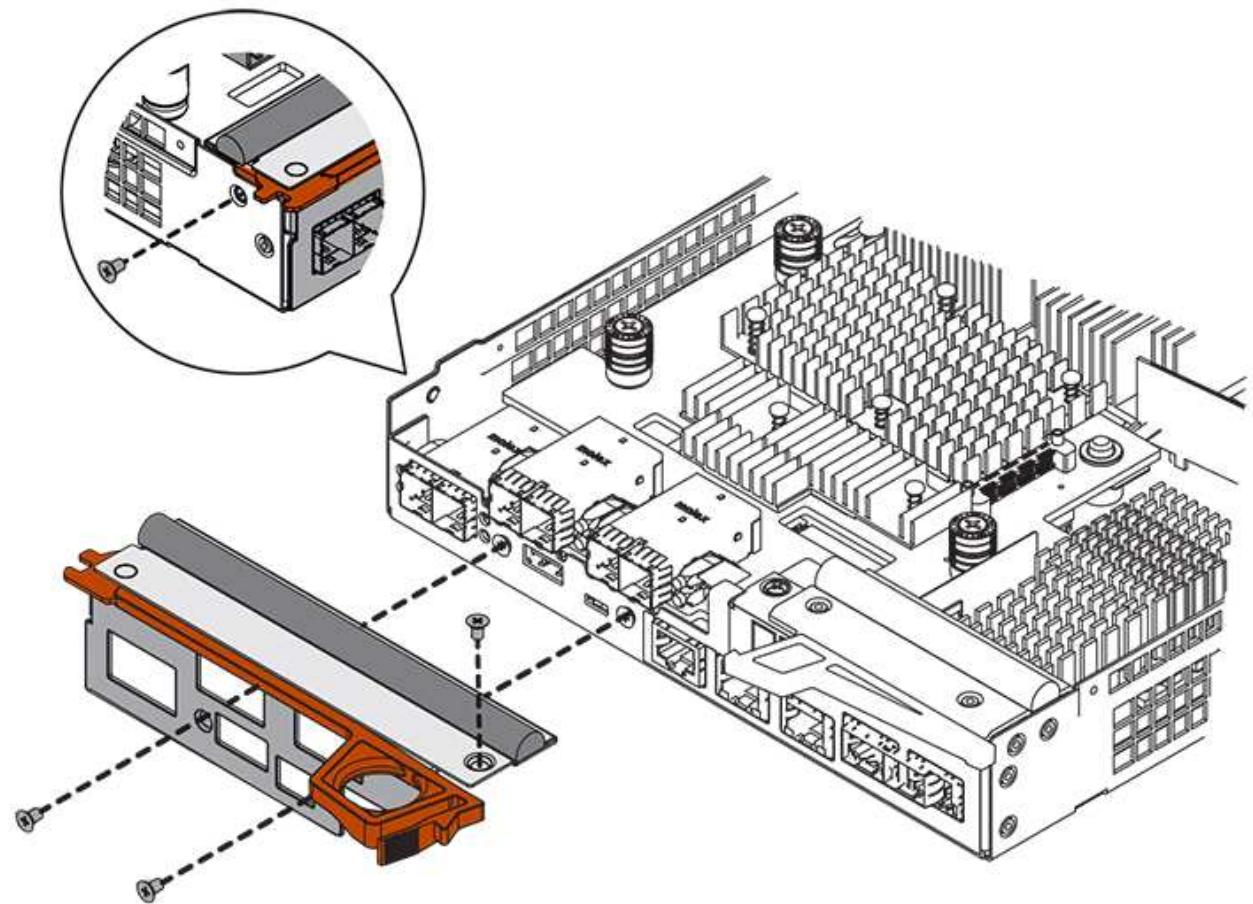


(1) Internal Cache Active

(2) Battery

- Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller canister.

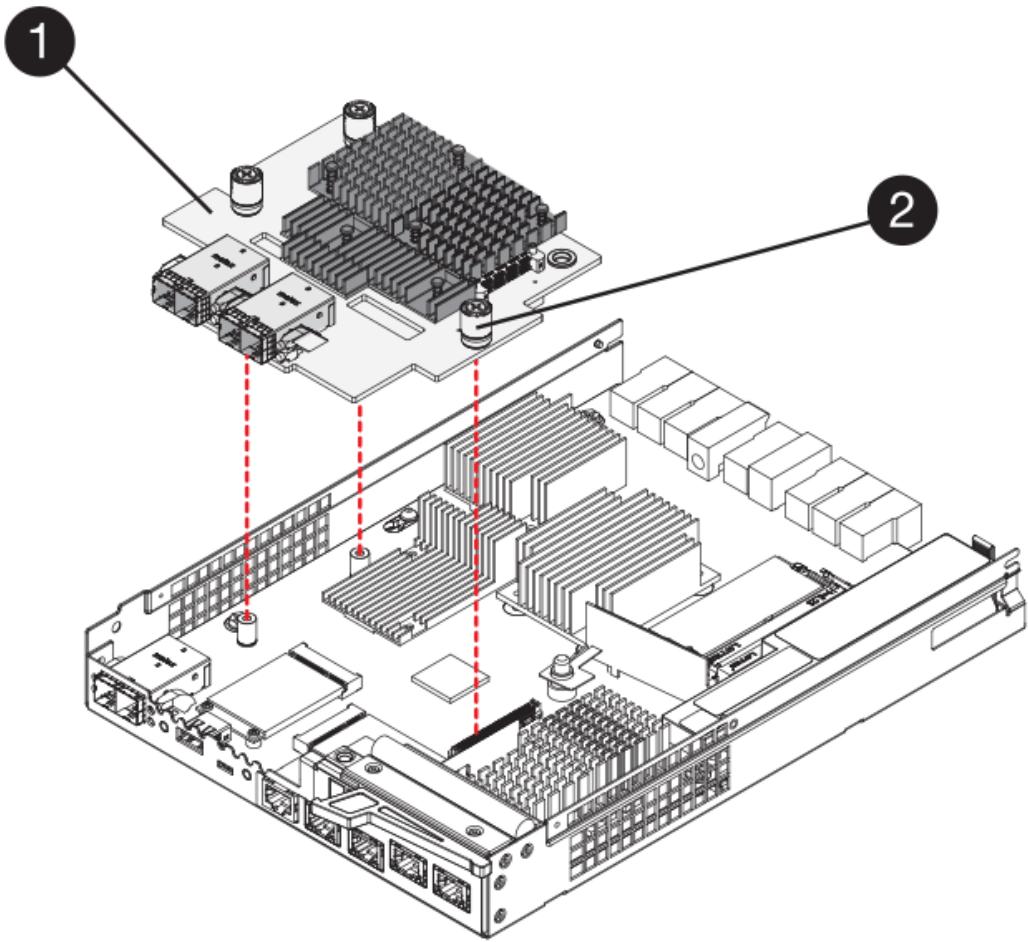
There are four screws: one on the top, one on the side, and two on the front.



4. Remove the HIC faceplate.
5. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
6. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



(1) Host interface card (HIC)

(2) Thumbscrews

7. Place the HIC on a static-free surface.

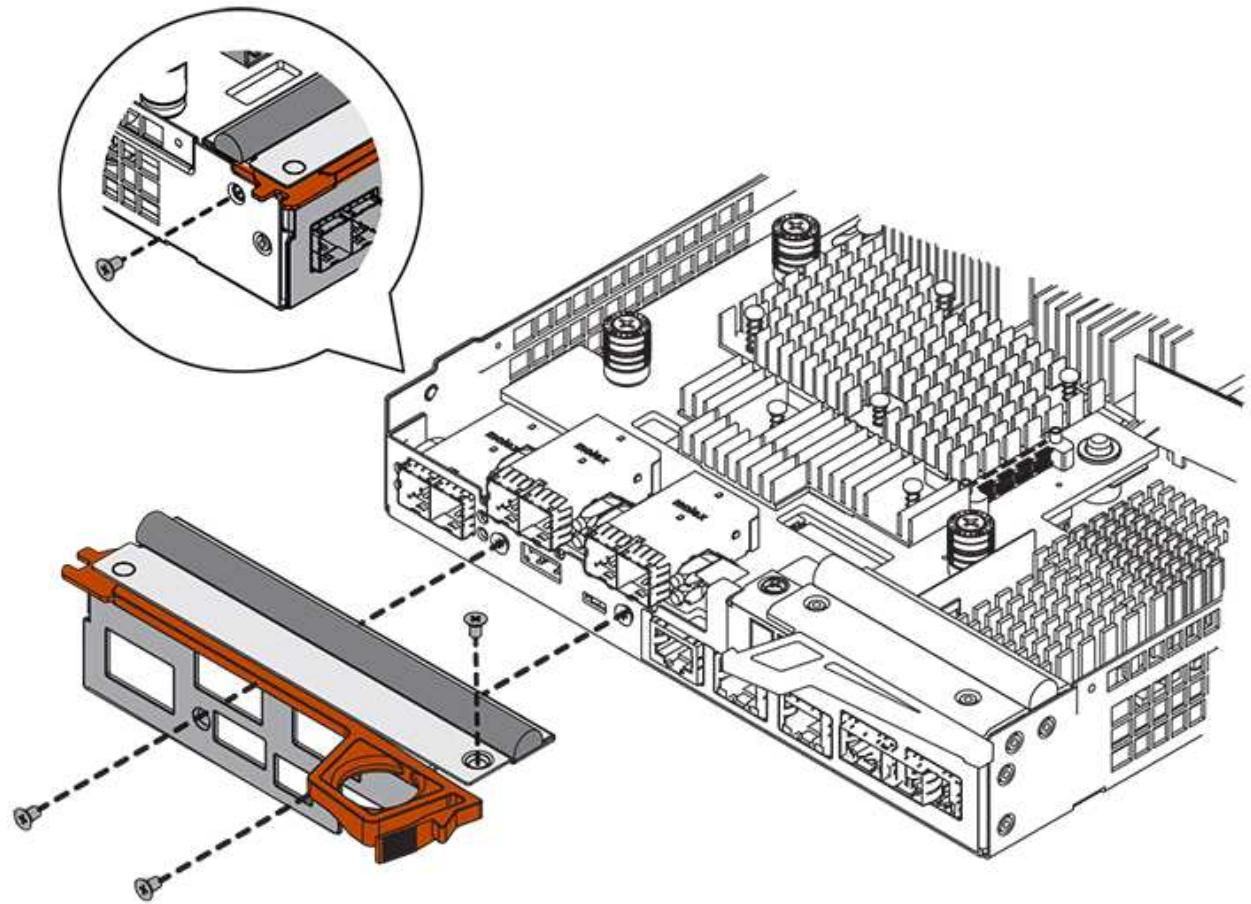
Step 4: Install host interface card

Install the new host interface card (HIC) to increase the number of host ports in your storage array.

Possible loss of data access — Never install a HIC in an E2800 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs will cause the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Using a #1 Phillips screwdriver, remove the four screws that attach the HIC faceplate to the controller canister, and remove the faceplate.



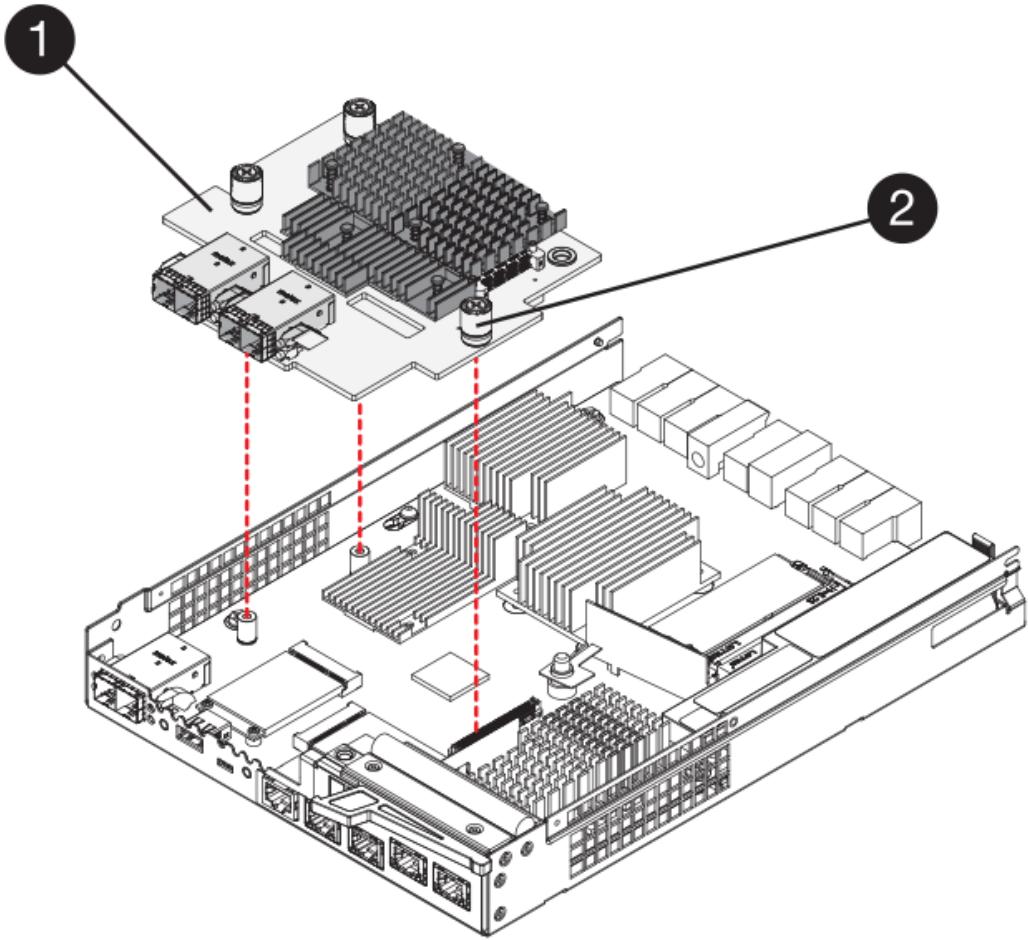
3. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

4. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



(1) Host interface card

(2) Thumbscrews

5. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over-tighten the screws.

6. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.

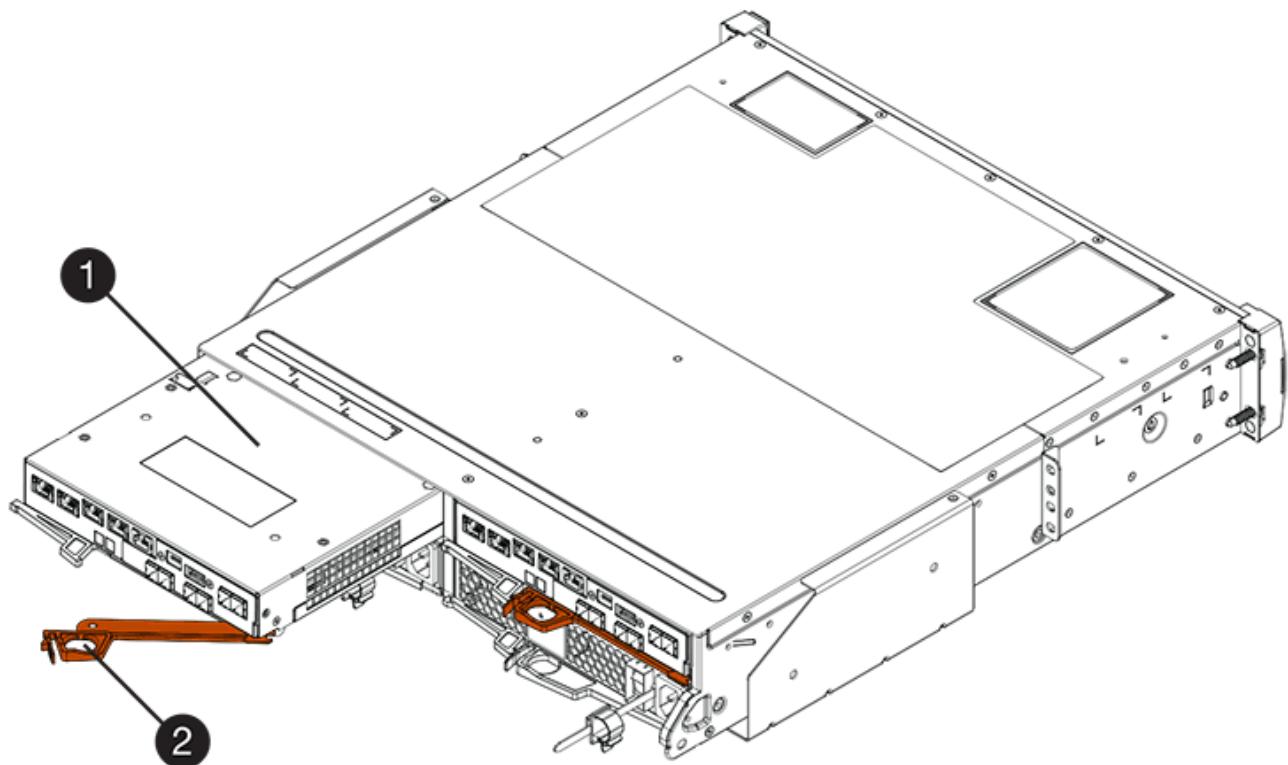
Step 5: Reinstall controller canister

Reinstall the controller canister into the controller shelf after installing the new host interface card (HIC).

Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

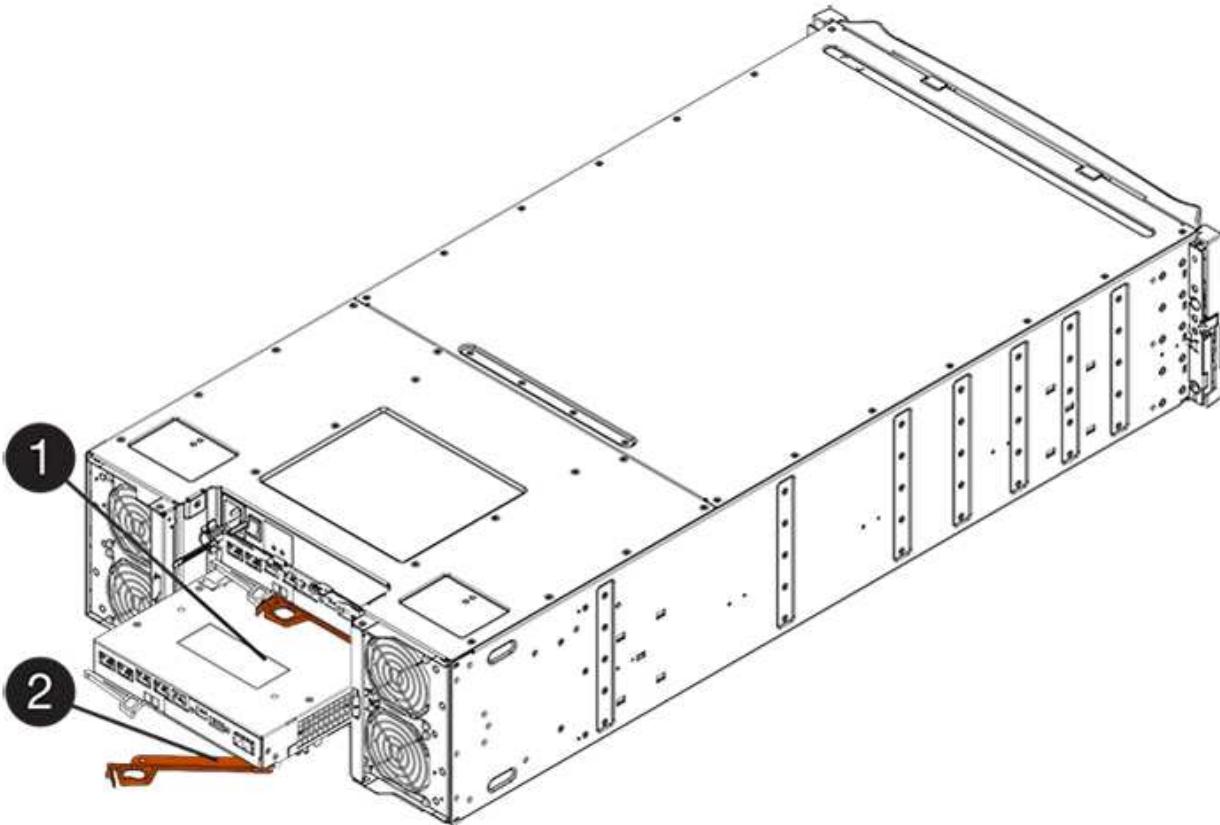
The following figure is an example of an E2824 controller shelf or EF280 flash array:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E2860 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

4. Move the cam handle to the left to lock the controller canister in place.
5. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

6. (Optional) If you are upgrading HICs in a duplex configuration, repeat all steps to remove the other controller canister, remove the HIC, install the new HIC, and replace the second controller canister.

Step 6: Complete host interface card upgrade

Complete the process of upgrading a host interface card by checking the controller LEDs and seven-segment display and confirming that the controller's status is Optimal.

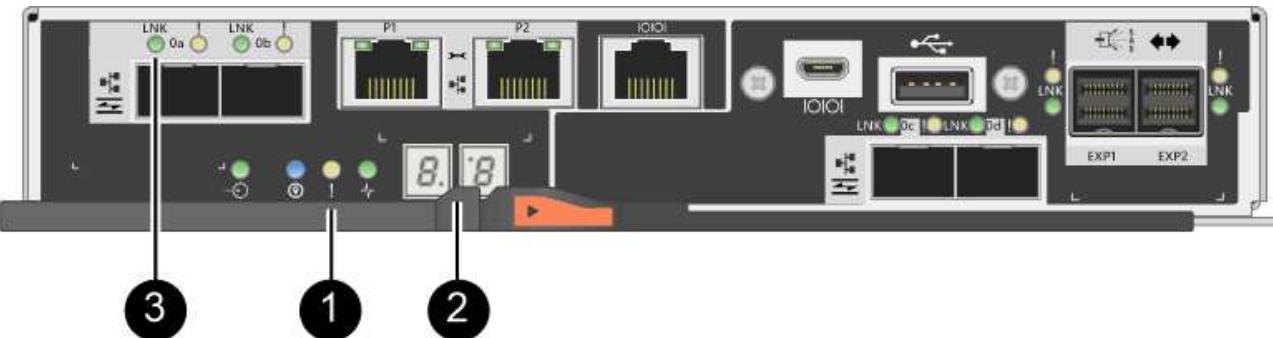
Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS, Sd, blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.

- The amber Attention LED on the controller turns on and then turns off, unless there is an error.
- The green Host Link LEDs remain off until you connect the host cables.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) *Attention LED (amber)*

(2) *Seven-segment display*

(3) *Host Link LEDs*

3. From SANtricity System Manager, confirm that the controller's status is Optimal.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

4. If the new HIC ports require SFP+ transceivers, install these SFPs.

5. Connect the cables from the controller's host ports to the data hosts.

What's next?

The process of upgrading a host interface card in your storage array is complete. You can resume normal operations.

Replace E2800 host interface card (HIC)

You can replace a host interface card (HIC) that has failed.

About this task

When you replace a HIC, you place the controller offline, remove the controller canister, install the new HIC, replace the controller canister, and then bring the controller online.

Before you begin

- Review [Requirements for E2800 HIC replacement](#).
- You must schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)

- Make sure that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.

What you'll need

- One or two HICs, based on whether you have one or two controllers in your storage array. The HICs must be compatible with your controllers. If two controllers are present, each controller must have identical HICs.
- Labels to identify each cable that is connected to the controller canister.
- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller offline

The steps to place a controller offline depend on whether you have one controller (simplex) or two controllers (duplex). Go to the appropriate instructions for:

- [Duplex: Place controller offline](#)
- [Simplex: Power down the controller shelf](#)

Duplex: Place controller offline

If you have a duplex configuration, follow this step to place the controller offline so you can safely remove the failed HIC.



Perform this task only if your storage array has two controllers (duplex configuration).

Steps

1. From the Details area of the Recovery Guru, determine which of the controller canisters has the failed HIC.
2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.
 - From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.
 - d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.
 - Alternatively, you can take the controllers offline by using the following CLI commands:
For controller A: set controller [a] availability=offline
For controller B: set controller [b] availability=offline



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

5. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

Simplex: Power down the controller shelf

If you have a simplex configuration, power down the controller shelf so you can safely remove the failed HIC.



Perform this task only if your storage array has one controller (simplex configuration).

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that you have a failed HIC and to ensure no other items must be addressed before you can remove and replace the HIC.
2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.

b. Select **Collect Configuration Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

a. Select **Support > Support Center > Diagnostics**.

b. Select **Collect Support Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. 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.



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.

5. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

6. From the home page of SANtricity System Manager, select **View Operations in Progress**.

7. Confirm that all operations have completed before continuing with the next step.

8. Turn off both power switches on the controller shelf.

9. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can add the new host interface card (HIC).

Steps

1. Label each cable that is attached to the controller canister.

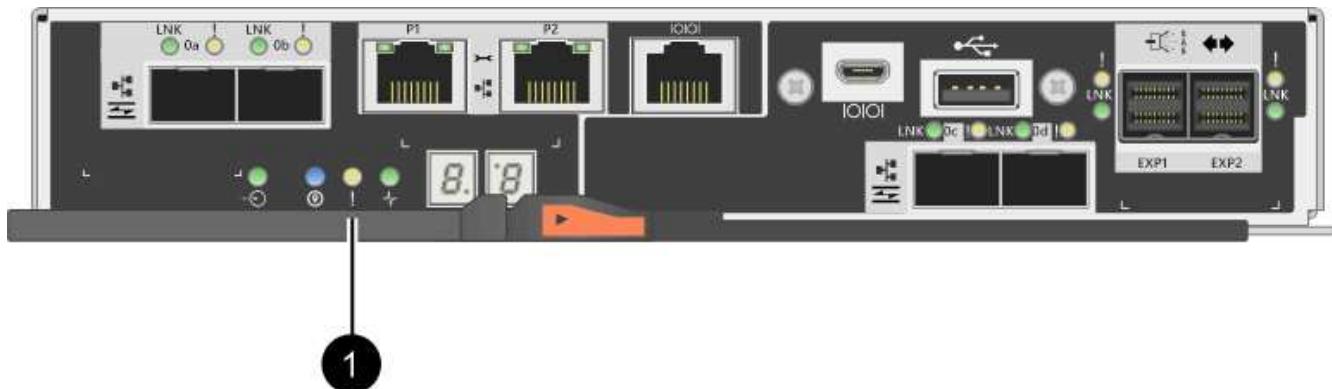
2. Disconnect all the cables from the controller canister.



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

3. Confirm that the Cache Active LED on the back of the controller is off.

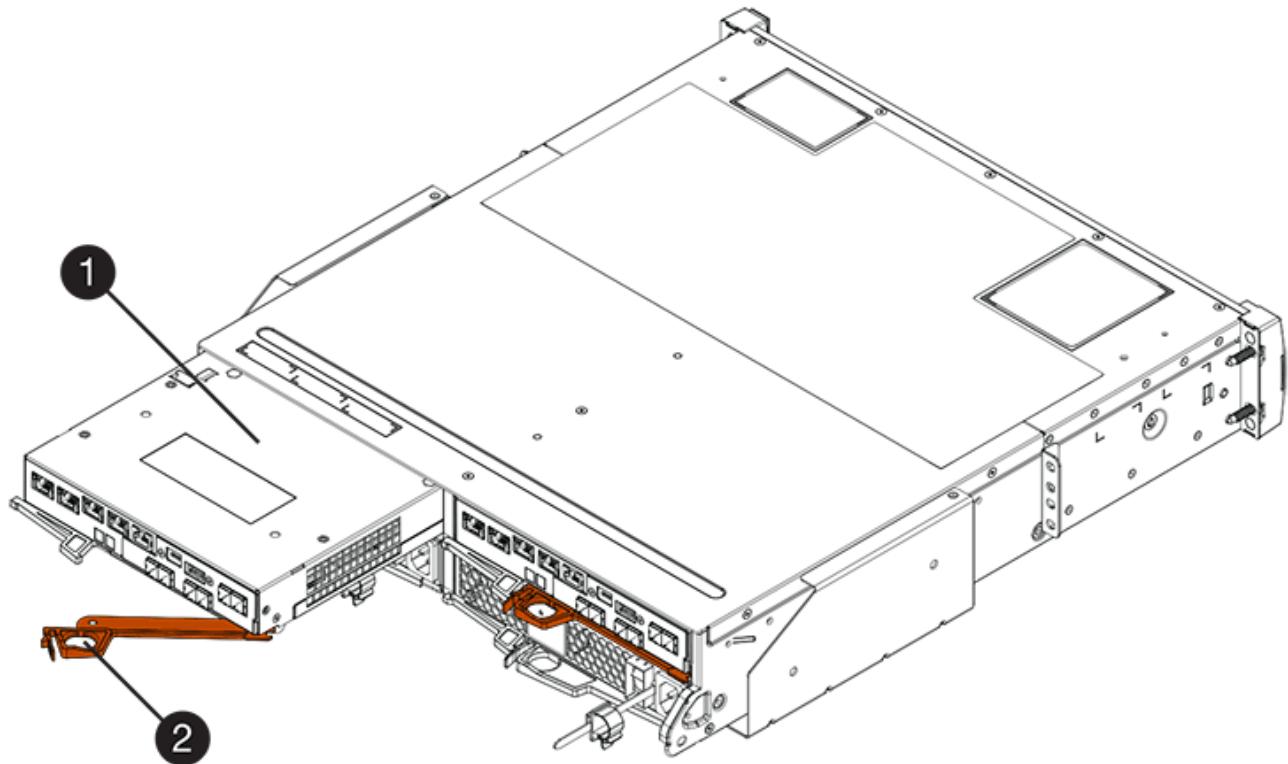
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

4. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

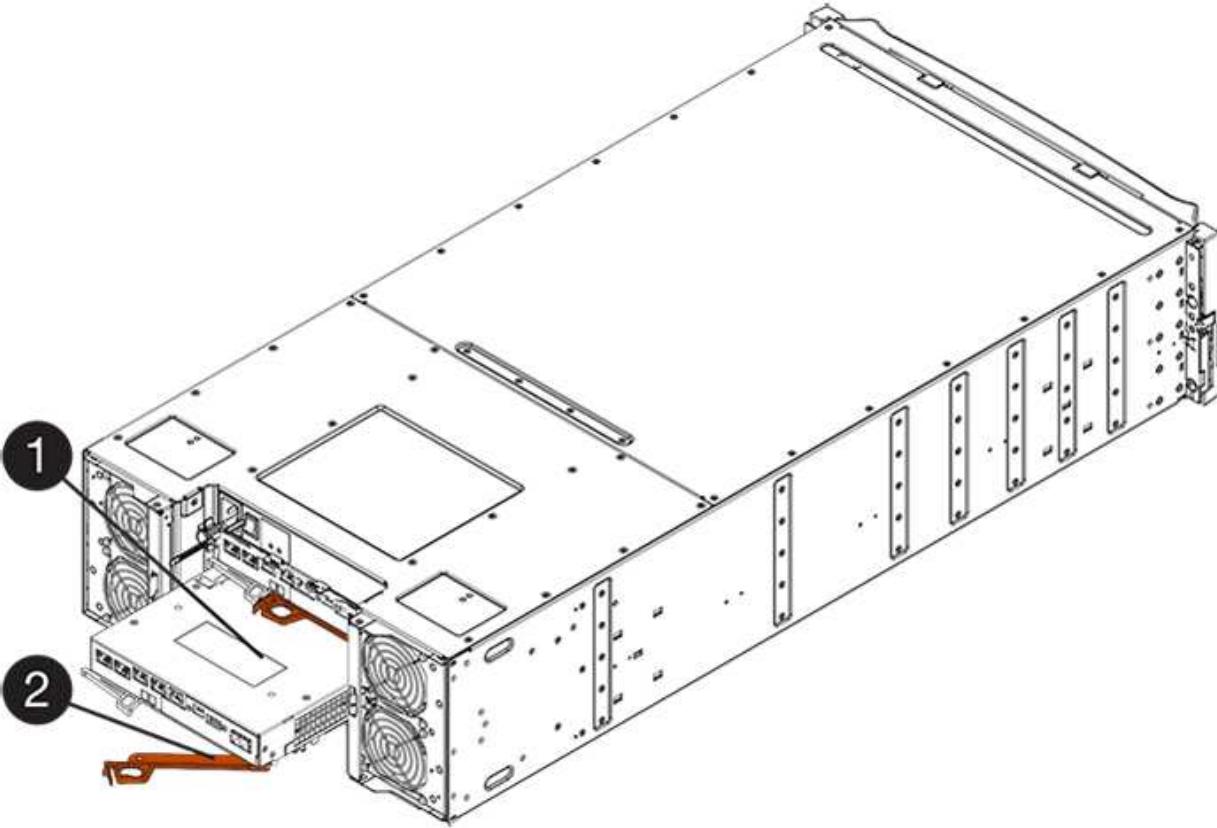
The following figure is an example of an E2812 controller shelf, E2824 controller shelf, or EF280 flash array:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

- Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E2812 controller shelf, E2824 controller shelf or EF280 flash array, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

- Turn the controller canister over, so that the removable cover faces up.
- Place the controller canister on a flat, static-free surface.

Step 3: Install a HIC

Install a HIC to replace the failed one with a new HIC.



Possible loss of data access — Never install a HIC in an E2800 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs will cause the controllers to lock down when you apply power.

Steps

- Unpack the new HIC and the new HIC faceplate.
- Press the button on the cover of the controller canister, and slide the cover off.
- Confirm that the green LED inside the controller (by the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active LED

(2) Battery

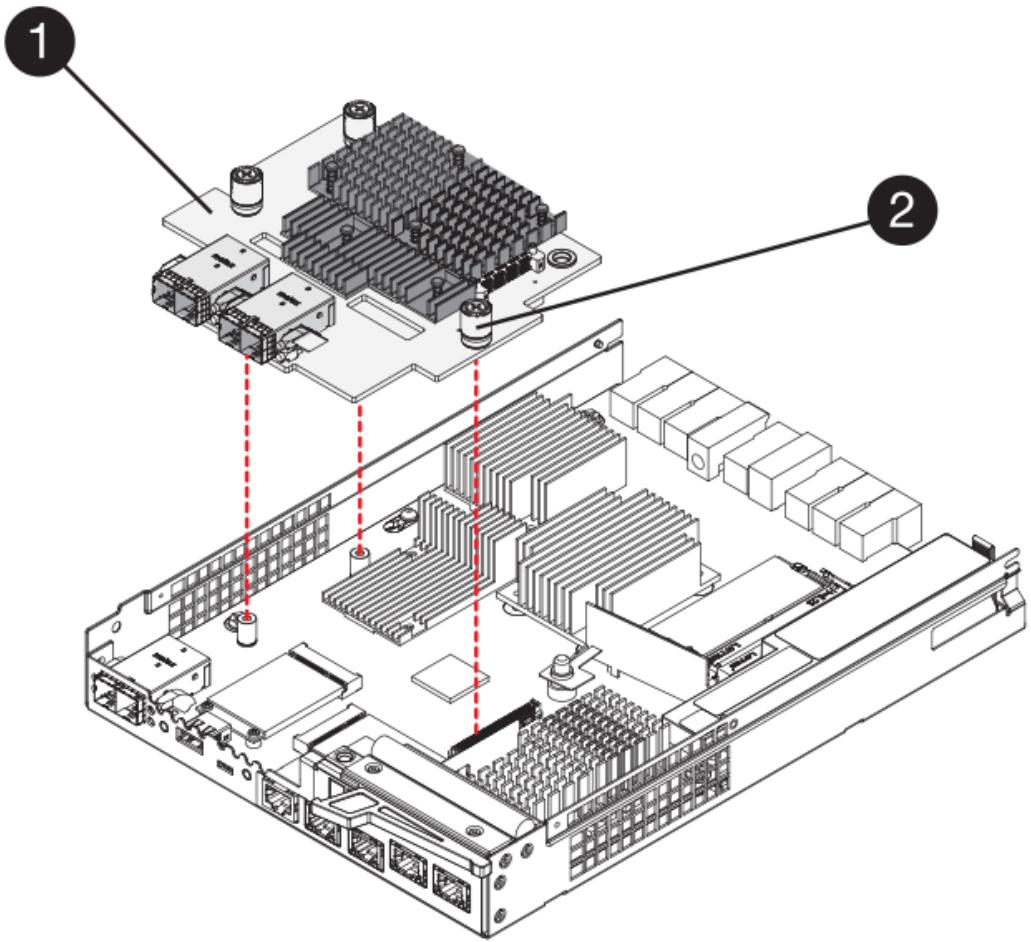
4. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the controller canister, and remove the faceplate.
5. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

6. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



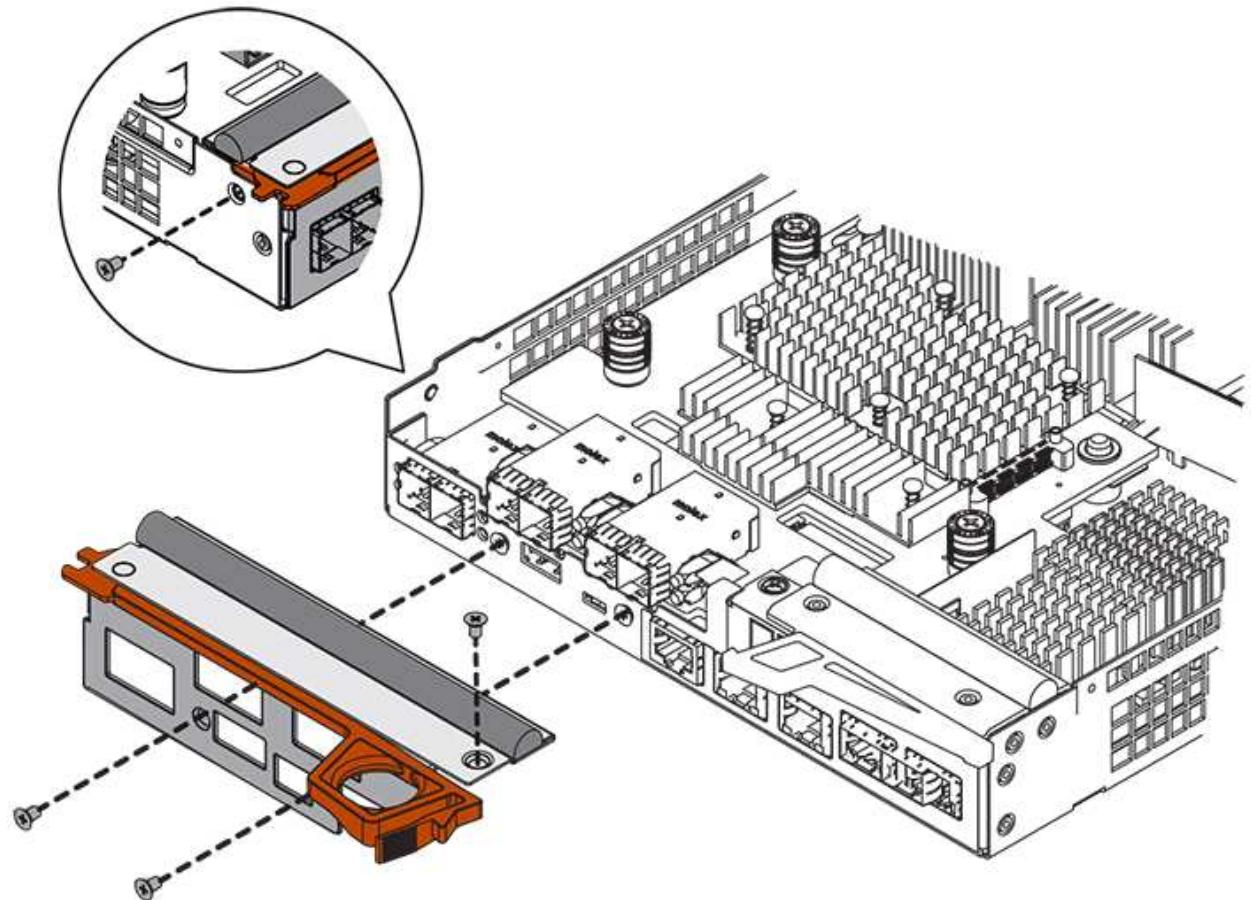
(1) *Host interface card*

(2) *Thumbscrews*

7. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over-tighten the screws.

8. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.



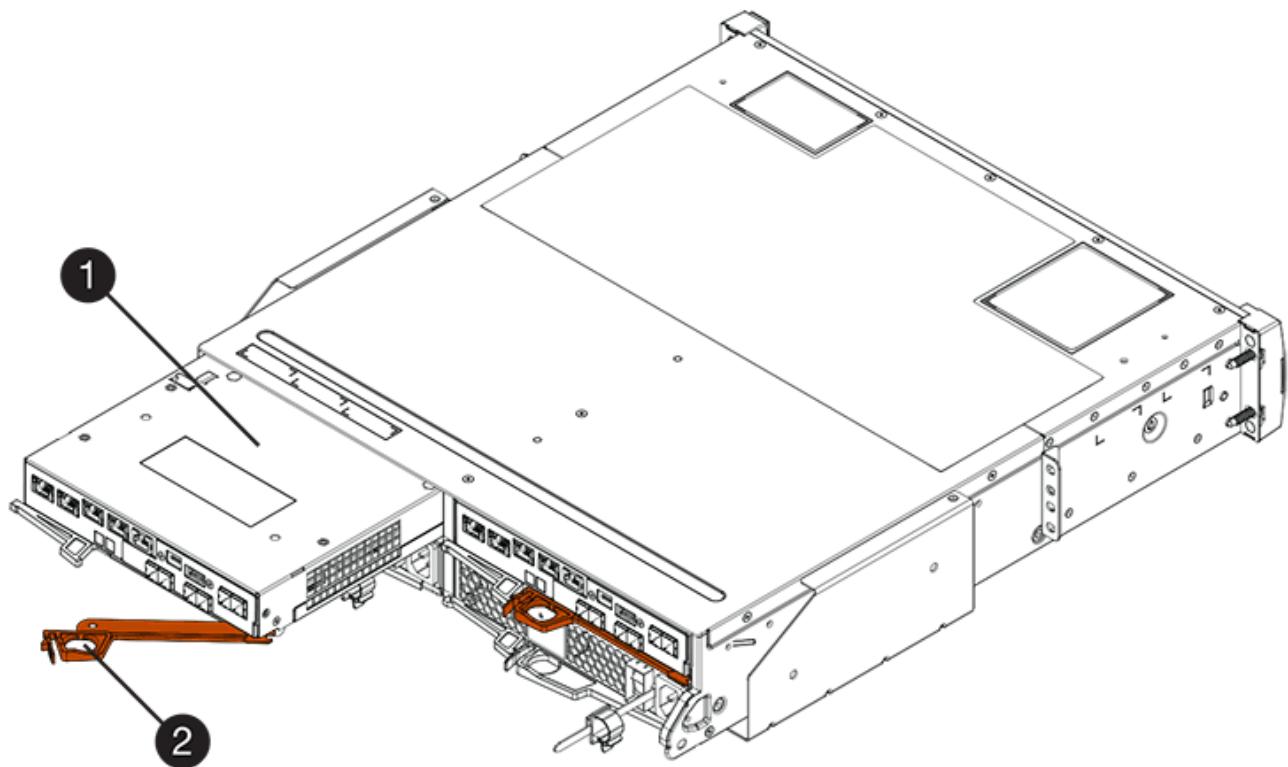
Step 4: Reinstall controller canister

After installing the HIC, reinstall the controller canister into the controller shelf.

Steps

1. Turn the controller canister over, so that the removable cover faces down.
2. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

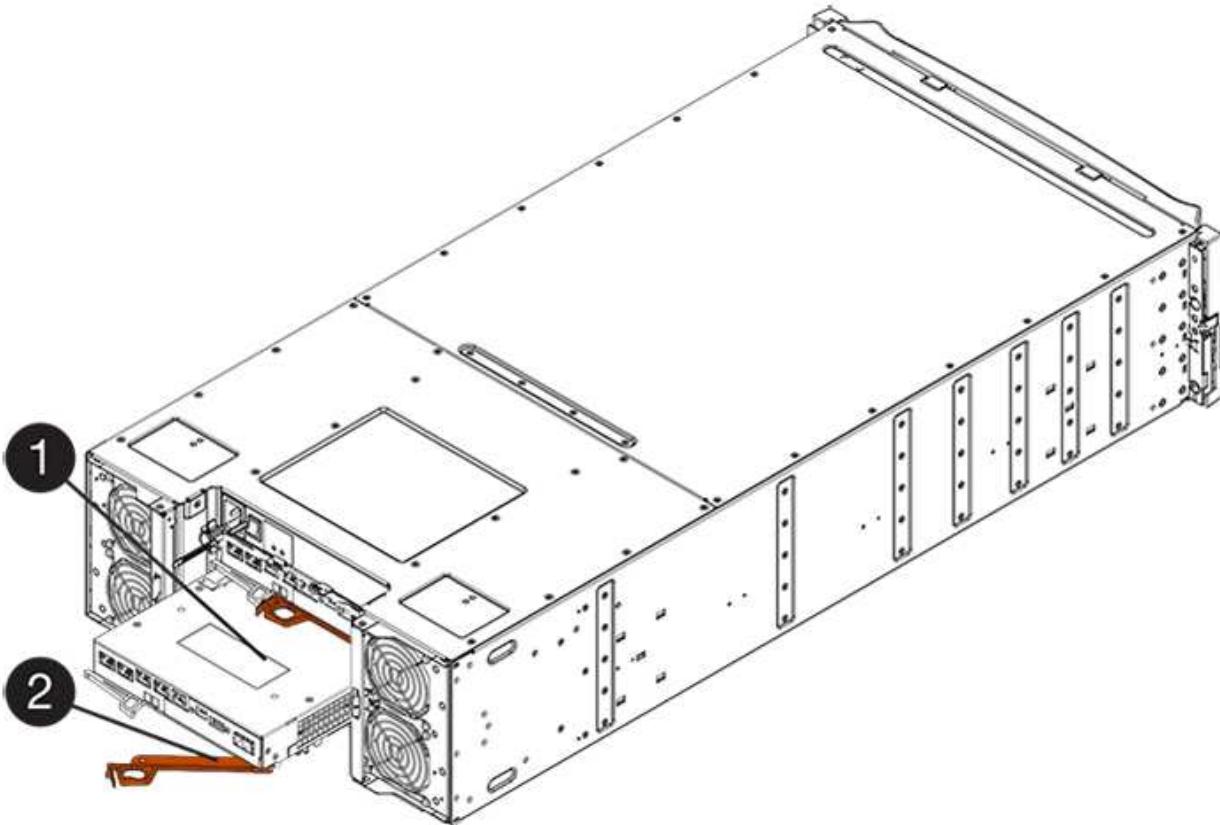
The following figure is an example of an E2824 controller shelf or EF280 flash array:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E2860 controller shelf:



(1) Controller canister

(2) Cam handle

3. Move the cam handle to the left to lock the controller canister in place.
4. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

5. (Optional) If you are adding HICs to a duplex configuration, repeat all steps to remove the second controller canister, install the second HIC, and reinstall the second controller canister.

Step 5: Place controller online

The steps to place a controller online depend on whether you have one controller (simplex) or two controllers (duplex).

Duplex: Place controller online

For a duplex configuration, bring the controller online, collect support data, and resume operations.



Perform this task only if your storage array has two controllers.

Steps

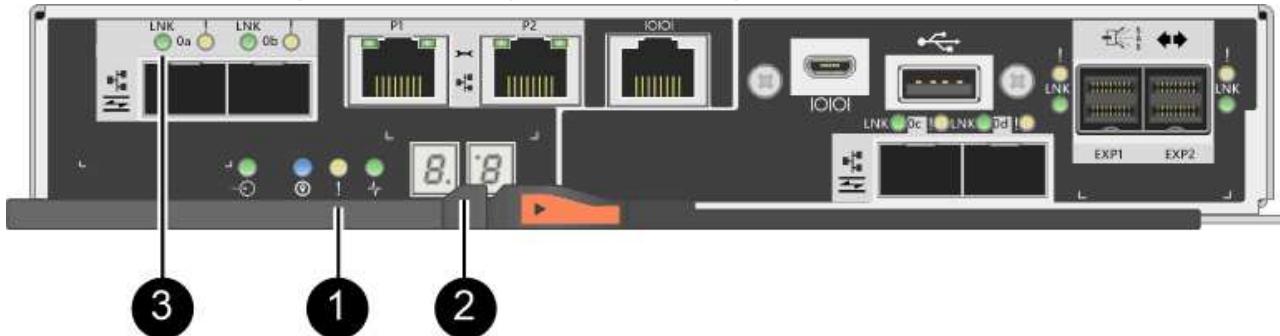
1. As the controller boots, check the controller LEDs and the seven-segment display.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS, OL, blank** to indicate that the controller is offline.
- The amber Attention LED remains lit.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) *Attention LED (amber)*

(2) *Seven-segment display*

(3) *Host Link LEDs*

2. Bring the controller online using SANtricity System Manager.

- From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf**.
 - c. Select the controller you want to place online.
 - d. Select **Place Online** from the context menu, and confirm that you want to perform the operation.

The system places the controller online.

- Alternatively, you can use the following CLI commands:

For controller A: set controller [a] availability=online;

For controller B: set controller [b] availability=online;

3. Check the codes on the controller's seven-segment display as it comes back online. If the display shows one of the following repeating sequences, immediately remove the controller.

- **OE, L0, blank** (mismatched controllers)
- **OE, L6, blank** (unsupported HIC)



Possible loss of data access — If the controller you just installed shows one of these codes, and the other controller is reset for any reason, the second controller could also lock down.

- When the controller is back online, confirm that its status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

- Collect support data for your storage array using SANtricity System Manager.

- Select **Support** > **Support Center** > **Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

- Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Contact technical support at [NetApp Support](#), 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number.

Simplex: Power up the controller shelf

For a simplex configuration, apply power to the controller shelf, collect support data, and resume operations.



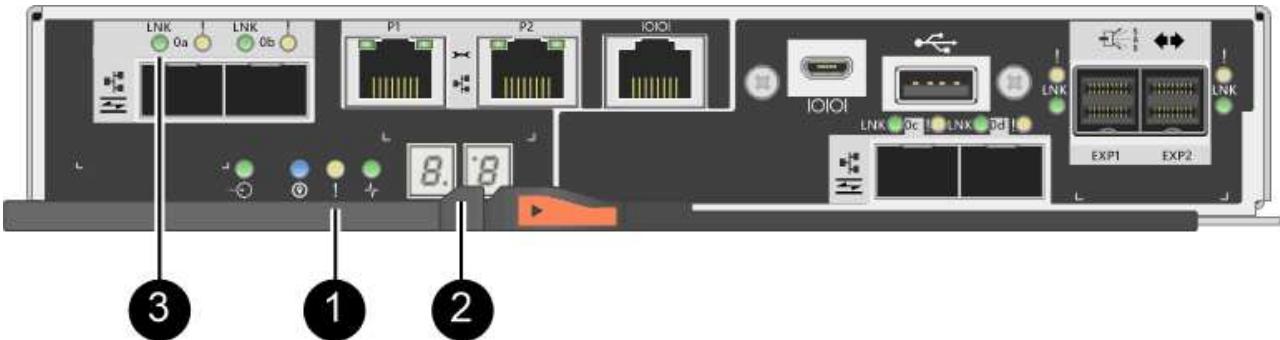
Perform this task only if your storage array has one controller.

Steps

- Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
- As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS**, **Sd**, **blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
 - The amber Attention LED on the controller turns on and then turns off, unless there is an error.
 - The green Host Link LEDs turn on.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Attention LED (amber)

(2) Seven-segment display

(3) Host Link LEDs

3. Confirm that the controller's status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

4. Collect support data for your storage array using SANtricity System Manager.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Contact technical support at [NetApp Support](#), 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number.

What's next?

Your HIC replacement is complete. You can resume normal operations.

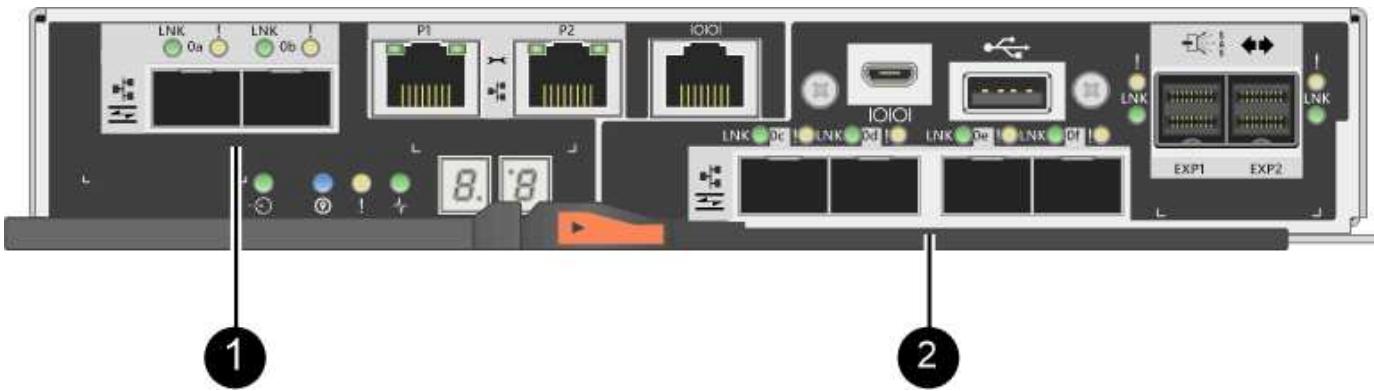
Host port protocol conversion

Requirements for changing E2800 host port protocol

Before converting the host protocol for an E2800 array, review the requirements.

Host ports you can change

The following figure shows the back of an E2800 controller that has two SFP+ (optical) baseboard host ports **(1)** and four SFP+ (optical) HIC ports **(2)**.



i A two-port HIC is also available.

The E2800 controller or controllers in your storage array might have different types of baseboard host ports and different types of HIC ports. The table shows which host ports can be changed with a feature pack.

| If you have these baseboard host ports... | And you have these HIC ports... | You can change... |
|---|---------------------------------|-------------------------------|
| Two SFP+ (optical) ports | None | Only the baseboard host ports |
| Two SFP+ (optical) ports | Four SFP+ (optical) ports | All of the ports |
| Two SFP+ (optical) ports | Two SFP+ (optical) ports | All of the ports |
| Two SFP+ (optical) ports | Two or four SAS ports | Only the baseboard host ports |
| Two SFP+ (optical) ports | Two RJ-45 (base-T) ports | Only the baseboard host ports |
| Two RJ-45 (base-T) ports | None | None of the ports |
| Two RJ-45 (base-T) ports | Two RJ-45 (base-T) ports | None of the ports |

The baseboard host ports and the HIC ports can use the same host protocol or different host protocols.

Requirements for changing the host protocol

- You must schedule a downtime maintenance window for this procedure.
- You must stop host I/O operations when you perform the conversion, and you will not be able to access data on the storage array until you have successfully completed the conversion.
- You must use out-of-band management. (You cannot use in-band management to complete this procedure.)
- You have obtained the necessary hardware for the conversion. Your NetApp Sales Representative can help you determine what hardware you need and help you order the correct parts.
- If you are attempting to change the baseboard host ports of your storage array, and it currently uses dual-protocol (also referred to as *unified*) SFP transceivers that you purchased from NetApp, you do not need to change your SFP transceivers.

- Make sure that the dual-protocol SFP transceivers support both FC (at 4 Gbps, 16 Gbps,) and iSCSI (at 10 Gbps), but they do not support 1 Gbps iSCSI. See [Step 1: Determine whether you have dual-protocol SFPs](#) to determine what type of SFP transceivers are installed.

Considerations for changing the host protocol

The considerations for changing the host protocol depend on the starting and ending protocols of the baseboard host ports and the HIC ports.

If you use a Mirroring feature or the Data Assurance (DA) feature, you must understand what happens to these features when you change the host port protocol as described below.



The following considerations apply only if you are converting a storage array that has already been in use. These considerations do not apply if you are converting a new storage array that does not yet have hosts and volumes defined.

Converting from FC to iSCSI

- If your configuration contains SAN Boot hosts connected to the FC baseboard ports, check the [NetApp Interoperability Matrix](#) tool to ensure that the configuration is supported on iSCSI. If it is not, you cannot convert the host protocol to iSCSI.
- The DA feature is not supported for iSCSI.
 - If you are currently using DA and you want to convert FC host ports to iSCSI, you must disable DA on all volumes.
 - If you do not deactivate DA before converting to iSCSI, the storage array will be out of compliance after the conversion.
- The Synchronous Mirroring feature is not supported for iSCSI.
 - If you are currently using Synchronous Mirroring relationships and you want to convert FC host ports to iSCSI, you must deactivate Synchronous Mirroring.
 - Refer to the online help for SANtricity System Manager to remove all synchronous mirrored pairs, which removes mirror relationships on the local storage array and on the remote storage array. In addition, follow the instructions in the online help to deactivate Synchronous Mirroring.



If you do not deactivate Synchronous Mirroring relationships before converting to iSCSI, your system will lose data access and data loss might occur.

- Asynchronous Mirroring requires both the local storage array and the remote storage array to use the same protocol.
 - If you are currently using Asynchronous Mirroring and you want to convert all host ports from FC to iSCSI, you must deactivate Asynchronous Mirroring before applying the feature pack.
 - Refer to the online help for SANtricity System Manager to delete all mirror consistency groups and remove all mirrored pairs from the local and remote storage arrays. In addition, follow the instructions in the online help to deactivate Asynchronous Mirroring.

Converting from iSCSI to FC

- Asynchronous Mirroring requires both the local storage array and the remote storage array to use the same protocol. If you are currently using Asynchronous Mirroring with the baseboard ports, you must deactivate Asynchronous Mirroring before changing the protocol.

- Refer to the online help for SANtricity System Manager to delete all mirror consistency groups and remove all mirrored pairs from the local and remote storage arrays. In addition, follow the instructions in the online help to deactivate Asynchronous Mirroring.

Converting from FC to FC/iSCSI

Mirroring considerations:

- Synchronous Mirroring is not supported for iSCSI.
- If a storage array used for mirroring currently has only FC ports, and you want to convert some of them to iSCSI, you must determine which ports are used for mirroring.
- You do not need to convert the ports on the local storage array and the remote storage array to the same protocol as long as both storage arrays have at least one active FC port after the conversion.
- If you plan to convert the ports that are being used for mirrored relationships, you must deactivate any synchronous or asynchronous mirror relationships before applying the feature pack.
- If you plan to convert the ports that are *not* being used for mirroring, asynchronous mirroring operations will be unaffected.
- Before applying the feature pack, you should confirm that all mirror consistency groups are synchronized. After applying the feature pack, you should test the communication between the local storage array and the remote storage array.

Data Assurance considerations:

- The Data Assurance (DA) feature is not supported for iSCSI.

To ensure that data access remains uninterrupted, you might need to remap or remove DA volumes from host clusters before applying the feature pack.

| If you have... | You must... |
|--|--|
| DA volumes in the default cluster | <p>Remap all the DA volumes in the default cluster.</p> <ul style="list-style-type: none"> • If you do not want to share DA volumes between hosts, follow these steps: <ol style="list-style-type: none"> a. Create a host partition for each set of FC host ports (unless this has already been done). b. Remap the DA volumes to the appropriate host ports. • If you want to share DA volumes between hosts, follow these steps: <ol style="list-style-type: none"> a. Create a host partition for each set of FC host ports (unless this has already been done). b. Create a host cluster that includes the appropriate host ports. c. Remap the DA volumes to the new host cluster. <p> This approach eliminates volume access to any volumes that remain in the default cluster.</p> |
| DA volumes in a host cluster that contains FC-only hosts, and you want to add iSCSI-only hosts | <p>Remove any DA volumes belonging to the cluster, using one of these options.</p> <p> DA volumes cannot be shared in this scenario.</p> <ul style="list-style-type: none"> • If you do not want to share DA volumes between hosts, remap all DA volumes to individual FC hosts within the cluster. • Segregate the iSCSI-only hosts into their own host cluster, and keep the FC host cluster as is (with shared DA volumes). • Add an FC HBA to the iSCSI-only hosts to allow for sharing of both DA and non-DA volumes. |
| DA volumes in a host cluster that contains FC-only hosts, or DA volumes that are mapped to an individual FC host partition | No action is needed before applying the feature pack. DA volumes will remain mapped to their respective FC host. |

| If you have... | You must... |
|-----------------------|---|
| No partitions defined | No action is needed before applying the feature pack because no volumes are currently mapped. After converting the host protocol, follow the proper procedure to create host partitions and, if desired, host clusters. |

Converting from iSCSI to FC/iSCSI

- If you plan to convert a port that is being used for mirroring, you must move the mirroring relationships to a port that will remain iSCSI after the conversion.

Otherwise, the communication link might be down after the conversion because of a protocol mismatch between the new FC port on the local array and the existing iSCSI port on the remote array.

- If you plan to convert the ports that are not being used for mirroring, asynchronous mirroring operations will be unaffected.

Before applying the feature pack, you should confirm that all mirror consistency groups are synchronized. After applying the feature pack, you should test the communication between the local storage array and the remote storage array.

Converting from FC/iSCSI to FC

- When converting all host ports to FC, keep in mind that asynchronous mirroring over FC must occur on the highest-numbered FC port.
- If you plan to convert the ports being used for mirrored relationships, you must deactivate these relationships before applying the feature pack.



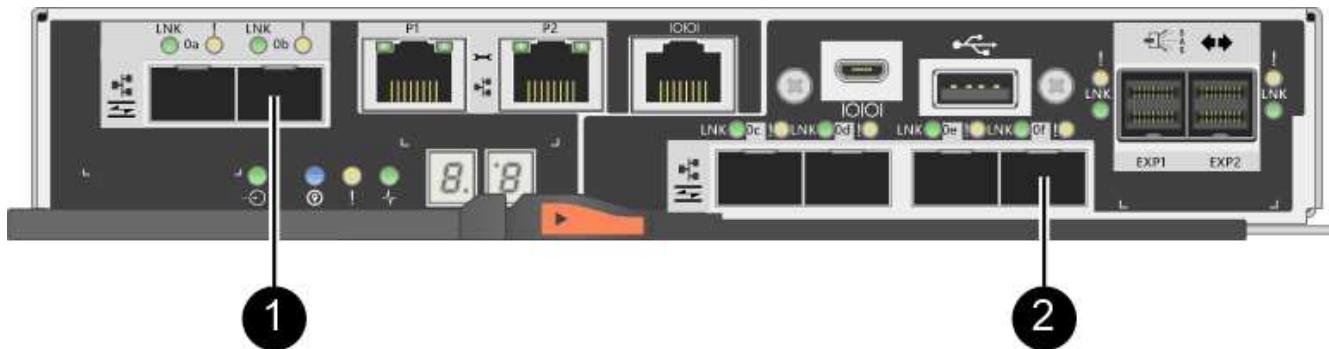
Possible data loss — If you do not delete the asynchronous mirroring relationships that occurred over iSCSI before converting the ports to FC, the controllers might lock down, and you might lose data.

- If the storage array currently has iSCSI baseboard ports and FC HIC ports, asynchronous mirroring operations will be unaffected.

Before and after the conversion, mirroring will occur on the highest-numbered FC port, which will remain the HIC port labeled **2** in the figure. Before applying the feature pack, you should confirm that all mirror consistency groups are synchronized. After applying the feature pack, you should test the communication between the local storage array and the remote storage array.

- If the storage array currently has FC baseboard ports and iSCSI HIC ports, you must delete any mirroring relationships that occur over FC before applying the feature pack.

When you apply the feature pack, mirroring support will move from the highest-numbered baseboard host port (labeled **1** in the figure) to the highest-numbered HIC port (labeled **2** in the figure).



| Before the conversion | | | After the conversion | | | Required steps |
|-----------------------|-----------|-------------------------|----------------------|-----------|-------------------------|--|
| Baseboard ports | HIC ports | Port used for mirroring | Baseboard ports | HIC ports | Port used for mirroring | |
| iSCSI | FC | (2) | FC | FC | (2) | Synchronize mirror consistency groups before and test communications after |
| FC | iSCSI | (1) | FC | FC | (2) | Delete mirroring relationships before and re-establish mirroring after |

Converting from FC/iSCSI to iSCSI

- Synchronous Mirroring is not supported for iSCSI.
- If you plan to convert the ports that are being used for mirrored relationships, you must deactivate mirroring relationships before applying the feature pack.



Possible data loss — If you do not delete the mirroring relationships that occurred over FC before converting the ports to iSCSI, the controllers might lock down, and you might lose data.

- If you do not plan to convert the ports that are being used for mirroring, mirroring operations will be unaffected.
- Before applying the feature pack, you should confirm that all mirror consistency groups are synchronized.
- After applying the feature pack, you should test the communication between the local storage array and the remote storage array.

Same host protocol and mirroring operations

Mirroring operations are not affected if the host ports being used for mirroring keep the same protocol after you apply the feature pack. Even so, before applying the feature pack, you should confirm that all mirror consistency groups are synchronized.

After applying the feature pack, you should test the communication between the local storage array and the remote storage array. Refer to the online help for SANtricity System Manager if you have questions on how to do this.

Change host protocol for E2800

If you have an E2800 storage array with SFP+ (optical) host ports, you can change the host port protocol from Fibre Channel (FC) to iSCSI or from iSCSI to FC.

You can change the protocol used by the host ports built into the controller (*baseboard host ports*), the protocol used by the host ports on the host interface card (*HIC ports*), or the protocol of all host ports.

Step 1: Determine whether you have dual-protocol SFPs

Use SANtricity System Manager to determine what type of SFP transceivers you have. Because these SFPs can be used with both FC and iSCSI protocols, they are referred to as *dual-protocol* or *unified* SFPs.

Steps

1. From SANtricity System Manager, select **Support**.
2. Select the **Support Center** tile.
3. On the Support Resources tab, locate and select the **Storage Array Profile** link.
4. Type **SFP** in the text box, and click **Find**.
5. For each SFP listed in the Storage Array Profile, locate the entry for **Supported data rate(s)**.

| | |
|--------------------------------|----------------------------------|
| SFP status: | Optimal |
| Attached to: | Host-side of controller B |
| Location: | Unknown |
| Supported data rate(s): | 16 Gbps, 10 Gbps, 8 Gbps, 4 Gbps |
| Link length: | Short |
| Connector: | LC |
| Transmitter type: | Shortwave Laser w/o OFC |
| Transmission media: | TM Multi-mode 62.5m (M6) |
| IEEE company ID: | 00 17 6a |
| Revision: | Not Available |
| Part number: | AFBR-57F5UMZ |
| Serial number: | AA1317J14X7 |
| Vendor: | AVAGO |
| Date of manufacture: | 4/28/13 |

6. Refer to the table to determine whether you can reuse the SFPs, as follows:

| Supported data rate(s) | SFP type | Supported protocol |
|----------------------------------|-------------------|---|
| 16 Gbps, 10 Gbps, 4 Gbps | Dual-protocol | <ul style="list-style-type: none"> • FC: 16 Gbps, 4 Gbps • iSCSI: 10 Gbps |
| 25 Gbps, 10 Gbps | 25 Gbps, 10 Gbps, | iSCSI only |
| 32 Gbps, 16 Gbps, 8 Gbps, 4 Gbps | 32 Gbps, 16 Gbps | FC only |

- If you have dual-protocol SFPs, you can continue using them after you convert the protocol.



The dual-protocol SFPs do not support 1 Gb iSCSI. If you are converting host ports to iSCSI, be aware that the dual-protocol SFPs support only a 10 Gb link to the connected port.

- If you have 16 Gbps SFPs, and you are converting host ports to iSCSI, you must remove the SFPs and replace them with dual-protocol or 10 Gbps SFPs after converting the protocol. As needed, you can also use 10 Gbps iSCSI copper by using a special Twin-Ax cable with SFPs.



8Gbps FC SFPs are NOT supported in the E28xx or E57xx controllers. ONLY 16Gbps and 32 Gbps FC SFPs are supported.

- If you have 10 Gbps SFPs, and you are converting host ports to FC, you must remove the SFPs from these ports and replace them with dual-protocol or 16 Gbps SFPs after converting the protocol.

Step 2: Obtain the feature pack

To obtain the feature pack, you need the serial number from the controller shelf, a Feature Activation Code, and the Feature Enable Identifier for the storage array.

Steps

1. Locate the serial number.
 - a. From SANtricity System Manager, select **Support > Support Center**.
 - b. With the **Support Resources** tab selected, scroll to the **View top storage array properties** section.
 - c. Locate the **Chassis Serial Number**, and copy this value to a text file.

View top storage array properties

| | |
|--|----------------------------------|
| Storage array world-wide identifier (ID): | 600A0980006CEF9B00000000574DB18C |
| Chassis serial number: | 1142FG00061 |
| Number of shelves: | 2 |
| Number of drives: | 41 |
| Drive media types: | HDD |
| Number of controllers: | 2 |
| Controller board ID: | 2806 |

2. Locate the **feature pack submodel ID**.

- On the Support Resources tab, locate and select the **Storage Array Profile** link.
- Type **feature pack submodel ID** in the text box, and click **Find**.
- Locate the feature pack submodel ID for the starting configuration.

Storage Array Profile X

Feature pack submodel ID Find

Results: 1 of 1

Feature pack submodel ID: 318

Additional feature information

| | |
|---|-----|
| Snapshot groups allowed per base volume (see note below): | 4 |
| Volume assignments per host or host cluster: | 256 |

Note: If a volume is a member of a snapshot consistency group, that membership (member volume) counts against both the snapshot group and the volume assignment limit.

FIRMWARE INVENTORY

| | |
|---|--------------------------|
| Storage Array | |
| Report Date: | 2/13/17 4:56:33 PM UTC |
| Storage Array Name: | LDAPandCLI-Cfg04-Arapaho |
| Current SANtricity OS Software Version: | 88.40.39.74.001 |
| Management Software Version: | 11.40.0010.0051 |
| Controller Firmware Version: | 88.40.39.74 |
| Supervisor Software Version: | 88.40.39.74 |
| IOM (ESM) Version: | 81.40.0G00.0006 |
| Current NVSRAM Version: | N280X-840834-402 |
| Staged SANtricity OS Software Version: | None |
| Staged NVSRAM Version: | None |

- Using the feature pack submodel ID, locate the corresponding Controller submodel ID for the starting configuration and find the Feature Activation Code for the desired ending configuration within the table below. Then, copy that Feature Activation Code to a text file.

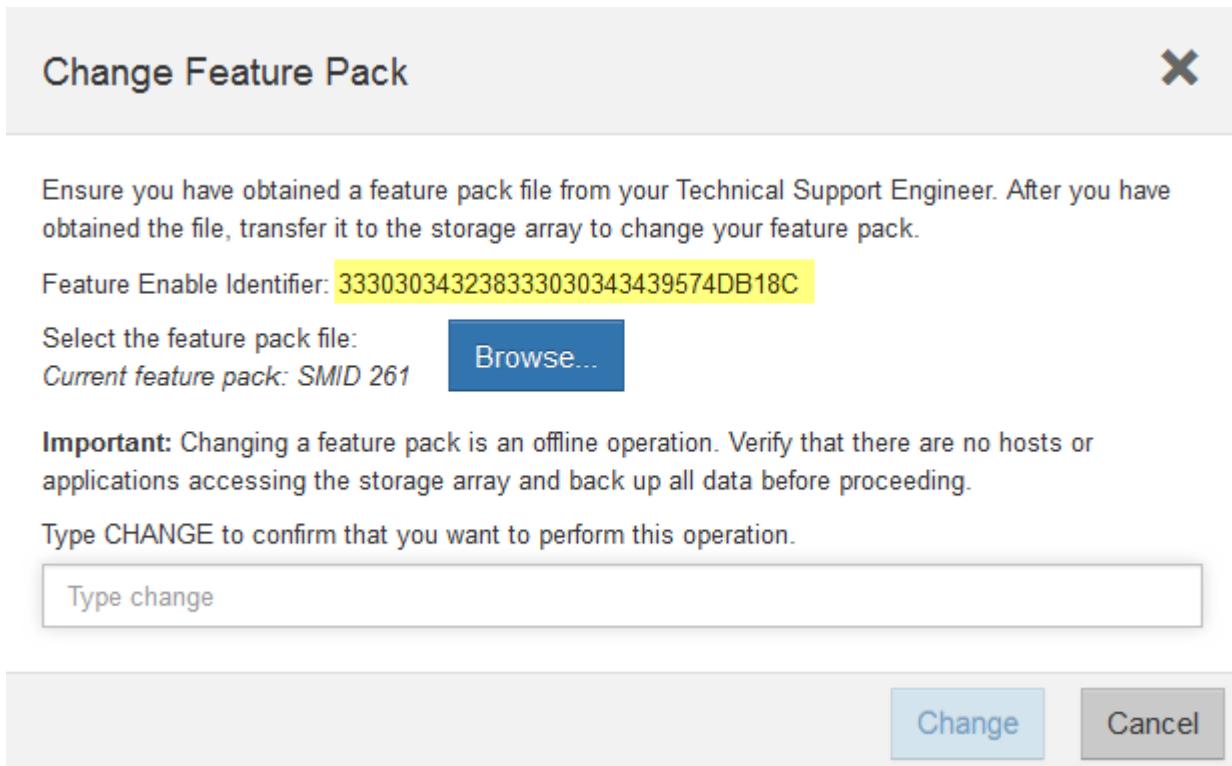
| Starting configuration | | | Ending configuration | | | Feature Activation Code |
|------------------------|-----------------|-----------|-------------------------------------|-----------------|-----------|-------------------------|
| Controller submodel ID | Baseboard ports | HIC ports | Controller submodel ID | Baseboard ports | HIC ports | |
| 318 | FC | FC | 319 | FC | iSCSI | ZGW-4L2-Z36IJ |
| | | | 320 | iSCSI | FC | 4GZ-NL2-Z4NRP |
| | | | 321 | iSCSI | iSCSI | TG2-7L2-Z5485 |
| | | | <i>no HIC or not an optical HIC</i> | 321 | iSCSI | TG2-7L2-Z5485 |
| 319 | FC | iSCSI | 318 | FC | FC | 1G5-QL2-Z7LFC |
| | | | 320 | iSCSI | FC | FG7-AL2-Z82RW |
| | | | 321 | iSCSI | iSCSI | 5G7-0K2-Z0G8X |
| 320 | iSCSI | FC | 318 | FC | FC | 4GP-HL2-ZYRKP |
| | | | 319 | FC | iSCSI | PGU-KL2-Z1P7I |
| | | | 321 | iSCSI | iSCSI | BGA-8K2-ZQWM5 |
| 321 | iSCSI | iSCSI | 318 | FC | FC | SGH-UK2-ZUCJG |
| | | | 319 | FC | iSCSI | 1GK-EK2-ZVSW1 |
| | | | 320 | iSCSI | FC | AGM-XL2-ZWA8A |

| Starting configuration | | | Ending configuration | | | Feature Activation Code |
|------------------------|-----------------|-----------|-------------------------------------|-----------------|-----------|-------------------------|
| Controller submodel ID | Baseboard ports | HIC ports | Controller submodel ID | Baseboard ports | HIC ports | |
| 338 | FC | FC | 339 | FC | iSCSI | PGC-RK2-ZREUT |
| | | | 340 | iSCSI | FC | MGF-BK2-ZSU3Z |
| | | | 341 | iSCSI | iSCSI | NGR-1L2-ZZ8QC |
| | | | <i>no HIC or not an optical HIC</i> | 341 | iSCSI | NGR-1L2-ZZ8QC |
| 339 | FC | iSCSI | 338 | FC | FC | DGT-7M2-ZKBMD |
| | | | 340 | iSCSI | FC | GGA-TL2-Z9J50 |
| | | | 341 | iSCSI | iSCSI | WGC-DL2-ZBZIB |
| 340 | iSCSI | FC | 338 | FC | FC | 4GM-KM2-ZGWS1 |
| | | | 339 | FC | iSCSI | PG0-4M2-ZHDZ6 |
| | | | 341 | iSCSI | iSCSI | XGR-NM2-ZJUGR |
| 341 | iSCSI | iSCSI | 338 | FC | FC | 3GE-WL2-ZCHNY |
| | | | 339 | FC | iSCSI | FGH-HL2-ZDY3R |
| | | | 340 | iSCSI | FC | VGJ-1L2-ZFFEW |



If your Controller submodel ID is not listed, contact [NetApp Support](#).

4. In System Manager, locate the Feature Enable Identifier.
 - a. Go to **Settings > System**.
 - b. Scroll down to **Add-ons**.
 - c. Under **Change Feature Pack**, locate the **Feature Enable Identifier**.
 - d. Copy and paste this 32-digit number to a text file.



5. Go to [NetApp License Activation: Storage Array Premium Feature Activation](#), and enter the information required to obtain the feature pack.
 - Chassis serial number
 - Feature Activation Code
 - Feature Enable Identifier



The Premium Feature Activation web site includes a link to "Premium Feature Activation Instructions." Do not attempt to use those instructions for this procedure.

6. Choose whether to receive the key file for the feature pack in an email or download it directly from the site.

Step 3: Stop host I/O

You must stop all I/O operations from the host before converting the protocol of the host ports. You cannot access data on the storage array until you successfully complete the conversion.

Steps

1. 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.



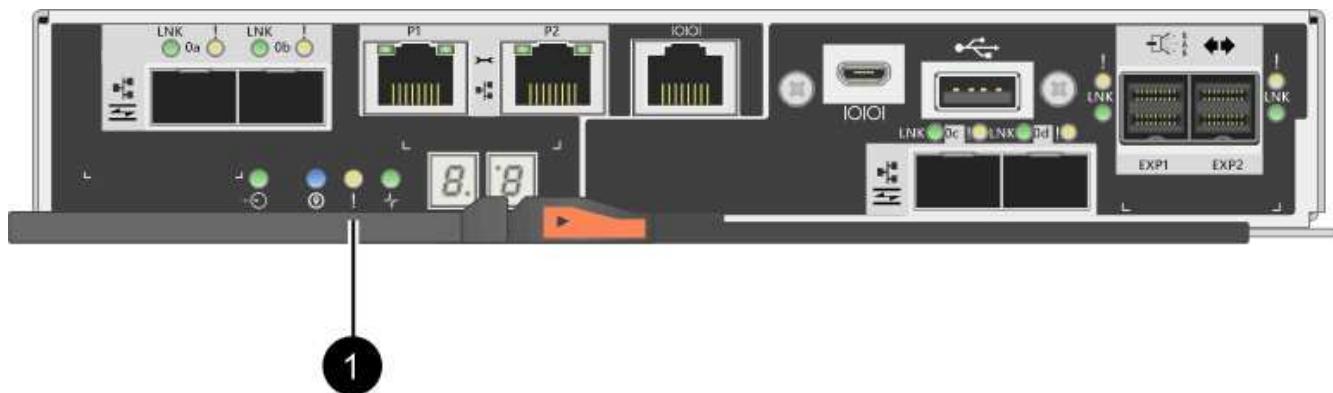
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose access to the data because the storage is not accessible.

2. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
3. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



| Callout | Type of host ports |
|---------|--------------------|
| (1) | Cache Active LED |

4. From the Home page of SANtricity System Manager, select **View Operations in Progress**.
5. Wait for all operations to complete before continuing with the next step.

Step 4: Change the feature pack

Change the feature pack to convert the host protocol of the baseboard host ports, the IB HIC ports, or both types of ports.

Steps

1. From SANtricity System Manager, select **Settings > System**.
2. Under **Add-ons**, select **Change Feature Pack**.

Add-ons

Enable Premium Feature
Obtain a key file to enable a premium feature by contacting support.
Feature Enable Identifier: 3330303435343330303435

Change Feature Pack
Change the feature pack that is currently installed. Click here to obtain a feature pack.
Feature Enable Identifier: 3330303435343330303435

3. Click **Browse**, and then select the feature pack you want to apply.
4. Type **CHANGE** in the field.
5. Click **Change**.

The feature pack migration begins. Both controllers automatically reboot twice to allow the new feature pack to take effect. The storage array returns to a responsive state after the reboot is complete.

6. Confirm the host ports have the protocol you expect.
 - a. From SANtricity System Manager, select **Hardware**.
 - b. Click **Show back of shelf**.
 - c. Select the graphic for either Controller A or Controller B.
 - d. Select **View settings** from the context menu.
 - e. Select the **Host Interfaces** tab.
 - f. Click **Show more settings**.
- g. Review the details shown for the baseboard ports and the HIC ports (labeled “slot 1”), and confirm that each type of port has the protocol you expect.

What's next?

Go to [Complete host protocol conversion](#).

Complete host protocol conversion for E2800

After converting the protocol of the host ports, you must perform additional steps before you can use the new protocol.

The steps depend on the starting and ending protocols of the baseboard host ports and the HIC ports.

Complete FC to iSCSI conversion

If you converted all host ports from FC to iSCSI, you must configure iSCSI networking.

Steps

1. Configure the switches.

You should configure the switches used to transport iSCSI traffic according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as

code updates.

2. From SANtricity System Manager, select **Hardware > Configure iSCSI ports**.
3. Select the port settings.

You can set up your iSCSI network in many ways. Consult your network administrator for tips on selecting the best configuration for your environment.

4. Update the host definitions in SANtricity System Manager.



If you need instructions for add hosts or host clusters, refer to the online help for SANtricity System Manager.

- a. Select **Storage > Hosts**.
- b. Select the host to which the port will be associated, and click **View/Edit Settings**.

The Host Settings dialog box appears.

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

The screenshot shows the 'Host Settings' dialog box. At the top, there are two tabs: 'Properties' (disabled) and 'Host Ports' (selected). Below the tabs are 'Add' and 'Delete' buttons. A table lists one host port entry: 'Host Port' is '12:34:56:78:91:12:34:56', 'Label' is 'ICT_1', and there is an 'Edit' button. Below the table, it says 'Total rows: 1'. At the bottom are 'Save' and 'Cancel' buttons.

| Host Port | Label | |
|-------------------------|-------|--|
| 12:34:56:78:91:12:34:56 | ICT_1 | |

- d. Click **Add**, and use the **Add Host Port** dialog box to associate a new host port identifier to the host.

The length of the host port identifier name is determined by the host interface technology. FC host port identifier names must have 16 characters. iSCSI host port identifier names have a maximum of 223 characters. The port must be unique. A port number that has already been configured is not allowed.

- e. Click **Delete**, and use the **Delete Host Port** dialog box to remove (unassociate) a host port identifier.

The **Delete** option does not physically remove the host port. This option removes the association between the host port and the host. Unless you remove the host bus adapter or the iSCSI initiator, the host port is still recognized by the controller.

- f. Click **Save** to apply your changes to the host port identifier settings.
- g. Repeat these steps to add and remove any additional host port identifiers.

5. Reboot the host or perform a rescan so that the host properly discovers the LUNs.
6. Remount volumes or start using block volume.

Complete iSCSI to FC conversion

If you converted all host ports from iSCSI to FC, you must configure FC networking.

Steps

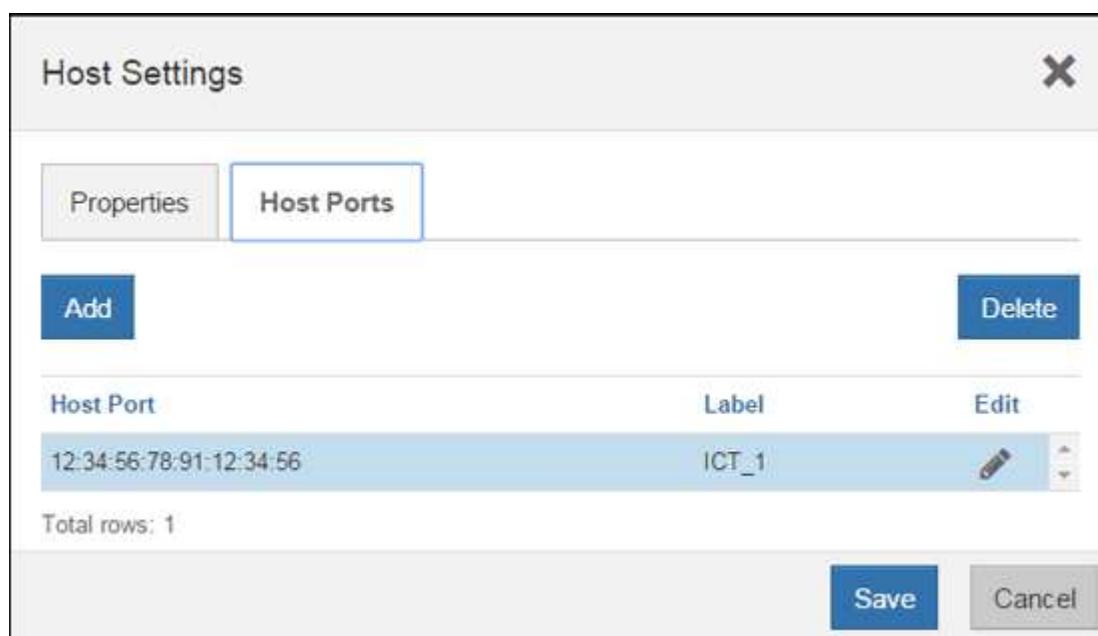
1. Install the HBA utility and determine initiator WWPNs.
2. Zone the switches.

Zoning the switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

3. Update the host definitions in SANtricity System Manager.
 - a. Select **Storage > Hosts**.
 - b. Select the host to which the port will be associated, and click **View/Edit Settings**.

The Host Settings dialog box appears.

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



- d. Click **Add**, and use the **Add Host Port** dialog box to associate a new host port identifier to the host.

The length of the host port identifier name is determined by the host interface technology. FC host port identifier names must have 16 characters. iSCSI host port identifier names have a maximum of 223 characters. The port must be unique. A port number that has already been configured is not allowed.

- e. Click **Delete**, and use the **Delete Host Port** dialog box to remove (unassociate) a host port identifier.

The **Delete** option does not physically remove the host port. This option removes the association between the host port and the host. Unless you remove the host bus adapter or the iSCSI initiator, the host port is still recognized by the controller.

- f. Click **Save** to apply your changes to the host port identifier settings.
 - g. Repeat these steps to add and remove any additional host port identifiers.
4. Reboot the host or perform a rescan so that the host properly discovers mapped storage.
 5. Remount volumes or start using block volume.

Complete FC to FC/iSCSI conversion

If you previously had all FC host ports and you converted some of them to iSCSI, you might need to modify your existing configuration to support iSCSI.

You can use either of the following options to use the new iSCSI ports. The exact steps depend on your current and planned network topologies. Option 1 assumes that you want to attach new iSCSI hosts to the array. Option 2 assumes that you want to convert the hosts connected to the converted ports from FC to iSCSI.

Option 1: Move FC hosts and add new iSCSI hosts

1. Move any FC hosts from the new iSCSI ports to the ports that remain FC.
2. If you are not already using dual-protocol SFPs, remove any FC SFPs.
3. Attach new iSCSI hosts to these ports, either directly or by using a switch.
4. Configure iSCSI networking for the new hosts and ports. For instructions, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

Option 2: Convert FC hosts to iSCSI

1. Shut down the FC hosts connected to the converted ports.
2. Provide an iSCSI topology for the converted ports. For example, convert any switches from FC to iSCSI.
3. If you are not already using dual-protocol SFPs, remove the FC SFPs from the converted ports, and replace them with iSCSI SFPs or dual-protocol SFPs.
4. Attach cables to the SFPs in the converted ports, and confirm they are connected to the correct iSCSI switch or host.
5. Power on the hosts.
6. Use the [NetApp Interoperability Matrix](#) tool to configure the iSCSI hosts.
7. Edit the host partition to add the iSCSI host port IDs and remove the FC host port IDs.
8. After the iSCSI hosts reboot, use the applicable procedures on the hosts to register the volumes and to make them available to your operating system.
 - Depending on your operating system, two utilities are included with the storage management software (`hot_add` and `SMdevices`). These utilities help register the volumes with the hosts and also show the applicable device names for the volumes.
 - You might need to use specific tools and options that are provided with your operating system to make the volumes available (that is, assign drive letters, create mount points, and so on). Refer to your host operating system documentation for details.

Complete iSCSI to FC/iSCSI conversion

If you previously had all iSCSI host ports and you converted some of them to FC, you might need to modify your existing configuration to support FC.

You can use either of the following options to use the new FC ports. The exact steps depend on your current

and planned network topologies. Option 1 assumes that you want to attach new FC hosts to the array. Option 2 assumes that you want to convert the hosts connected to the converted ports from iSCSI to FC.

Option 1: Move iSCSI hosts and add new FC hosts

1. Move any iSCSI hosts from the new FC ports to the ports that remain iSCSI.
2. If you are not already using dual-protocol SFPs, remove any FC SFPs.
3. Attach new FC hosts to these ports, either directly or by using a switch.
4. Configure FC networking for the new hosts and ports. For instructions, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

Option 2: Convert iSCSI hosts to FC

1. Shut down the iSCSI hosts connected to the converted ports.
2. Provide an FC topology for the converted ports. For example, convert any switches from iSCSI to FC.
3. If you are not already using dual-protocol SFPs, remove the iSCSI SFPs from the converted ports, and replace them with FC SFPs or dual-protocol SFPs.
4. Attach cables to the SFPs in the converted ports, and confirm they are connected to the correct FC switch or host.
5. Power on the hosts.
6. Use the [NetApp Interoperability Matrix](#) tool to configure the FC hosts.
7. Edit the host partition to add the FC host port IDs and remove the iSCSI host port IDs.
8. After the new FC hosts reboot, use the applicable procedures on the hosts to register the volumes and to make them available to your operating system.
 - Depending on your operating system, two utilities are included with the storage management software (hot_add and SMdevices). These utilities help register the volumes with the hosts and also show the applicable device names for the volumes.
 - You might need to use specific tools and options that are provided with your operating system to make the volumes available (that is, assign drive letters, create mount points, and so on). Refer to your host operating system documentation for details.

Complete FC/iSCSI to FC conversion

If you previously had a combination of FC host ports and iSCSI host ports and you converted all ports to FC, you might need to modify your existing configuration to use the new FC ports.

You can use either of the following options to use the new FC ports. The exact steps depend on your current and planned network topologies. Option 1 assumes that you want to attach new FC hosts to the array. Option 2 assumes that you want to convert the hosts connected to ports 1 and 2 from iSCSI to FC.

Option 1: Remove iSCSI hosts and add FC hosts

1. If you are not already using dual-protocol SFPs, remove any iSCSI SFPs, and replace them with FC SFPs or dual-protocol SFPs.
2. If you are not already using dual-protocol SFPs, remove any FC SFPs.
3. Attach new FC hosts to these ports, either directly or by using a switch
4. Configure FC networking for the new hosts and ports. For instructions, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

Option 2: Convert iSCSI hosts to FC

1. Shut down the iSCSI hosts connected to the ports you converted.
2. Provide an FC topology for these ports. For example, convert any switches connected to those hosts from iSCSI to FC.
3. If you are not already using dual-protocol SFPs, remove the iSCSI SFPs from the ports, and replace them with FC SFPs or dual-protocol SFPs.
4. Attach cables to the SFPs, and confirm they are connected to the correct FC switch or host.
5. Power on the hosts.
6. Use the [NetApp Interoperability Matrix](#) tool to configure the FC hosts.
7. Edit the host partition to add the FC host port IDs and remove the iSCSI host port IDs.
8. After the new FC hosts reboot, use the applicable procedures on the hosts to register the volumes and to make them available to your operating system.
 - Depending on your operating system, two utilities are included with the storage management software (`hot_add` and `SMdevices`). These utilities help register the volumes with the hosts and also show the applicable device names for the volumes.
 - You might need to use specific tools and options that are provided with your operating system to make the volumes available (that is, assign drive letters, create mount points, and so on). Refer to your host operating system documentation for details.

Complete FC/iSCSI to iSCSI conversion

If you previously had a combination of FC host ports and iSCSI host ports and you converted all ports to iSCSI, you might need to modify your existing configuration to use the new iSCSI ports.

You can use either of the following options to use the new iSCSI ports. The exact steps depend on your current and planned network topologies. Option 1 assumes that you want to attach new iSCSI hosts to the array. Option 2 assumes that you want to convert the hosts from FC to iSCSI.

Option 1: Remove FC hosts and add iSCSI hosts

1. If you are not already using dual-protocol SFPs, remove any FC SFPs, and replace them with iSCSI SFPs or dual-protocol SFPs.
2. Attach new iSCSI hosts to these ports, either directly or by using a switch.
3. Configure iSCSI networking for the new hosts and ports. For instructions, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

Option 2: Convert FC hosts to iSCSI

1. Shut down the FC hosts connected to the ports you converted.
2. Provide an iSCSI topology for these ports. For example, convert any switches connected to those hosts from FC to iSCSI.
3. If you are not already using dual-protocol SFPs, remove the FC SFPs from the ports, and replace them with iSCSI SFPs or dual-protocol SFPs.
4. Attach cables to the SFPs, and confirm they are connected to the correct iSCSI switch or host.
5. Power on the hosts.
6. Use the [NetApp Interoperability Matrix](#) tool to configure the ISCSI hosts.

7. Edit the host partition to add the iSCSI host port IDs and remove the FC host port IDs.
8. After the new iSCSI hosts reboot, use the applicable procedures on the hosts to register the volumes and to make them available to your operating system.
 - Depending on your operating system, two utilities are included with the storage management software (hot_add and SMdevices). These utilities help register the volumes with the hosts and also show the applicable device names for the volumes.
 - You might need to use specific tools and options that are provided with your operating system to make the volumes available (that is, assign drive letters, create mount points, and so on). Refer to your host operating system documentation for details.

E5700

Maintain E5700 hardware

For the E5700 storage system, you can perform maintenance procedures on the following components.

Batteries

A battery is included with a controller canister and preserves cached data if the AC power fails.

Controllers

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

Canisters

Canisters consist of three different types: power-fan canisters (power supplies) that supply a redundant power source and adequate cooling in a 12-drive or 24-drive controller shelf or drive shelf; power canisters that are used for power redundancy in a 60-drive controller shelf or drive shelf; and fan canisters that are used for cooling the 60-drive controller shelf or drive shelf.

Drives

A drive is an electromagnetic mechanical device that provides the physical storage media for data.

Host interface cards (HICs)

A host interface card (HIC) can optionally be installed within a controller canister. The E5700 controller includes built-in host ports on the controller card itself, as well as host ports on the optional HIC. Host ports that are built into the controller are called baseboard host ports. Host ports that are built into the HIC are called HIC ports.

Host port protocol

You can convert the protocol of a host to a different protocol so that compatibility and communication can be established.

Batteries

Requirements for E5700 battery replacement

Before you replace an E5700 battery, review the requirements and considerations.

Each controller canister includes a battery that preserves cached data if the AC power fails.

Recovery Guru alerts

If the Recovery Guru in SANtricity System Manager reports one of following statuses, you must replace the affected battery:

- Battery Failed
- Battery Replacement Required

From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.

Procedure overview

To protect your data, you must replace a failed battery as soon as possible.

The following is an overview of the steps to replace a battery in E5700 controllers (E5724, EF570, or E5760):

1. Take controller offline (duplex only).
2. Remove the controller canister.
3. Replace the battery.
4. Replace the controller canister.
5. Bring the controller online (duplex only).

Requirements

If you plan to replace a failed battery, you must have:

- A replacement battery.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Optionally, you can use the command line interface (CLI) to perform some of the procedures. If you do not have access to the CLI, you can do one of the following:

- **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
- **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Replace E5700 battery

You can replace a failed battery in an E5700 storage system.

About this task

Each E5700 controller canister includes a battery that preserves cached data if the AC power fails. If the Recovery Guru in SANtricity System Manager reports either a Battery Failed status or a Battery Replacement Required status, you must replace the affected battery.

Before you begin

- Verify that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.
- Review [Requirements for E5700 battery replacement](#).

What you'll need

- A replacement battery.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller offline (duplex)

If you have a duplex configuration, place the affected controller offline so you can safely remove the failed battery. The controller that you are not placing offline must be online (in the optimal state).



Perform this task only if your storage array has two controllers (duplex configuration).

Steps

1. From SANtricity System Manager, review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
2. From the Details area of the Recovery Guru, determine which battery to replace.
3. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From SANtricity System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
```

```
file="filename";
```

4. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

5. If the controller is not already offline, take it offline now using SANtricity System Manager.

- From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - c. Select the controller that you want to place offline.
 - d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

- Alternatively, you can take the controllers offline by using the following CLI commands:

For controller A: set controller [a] availability=offline

For controller B: set controller [b] availability=offline

6. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

Step 2: Remove controller canister

Before you can remove the failed battery, you must remove the controller canister.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all of the cables from the controller canister.

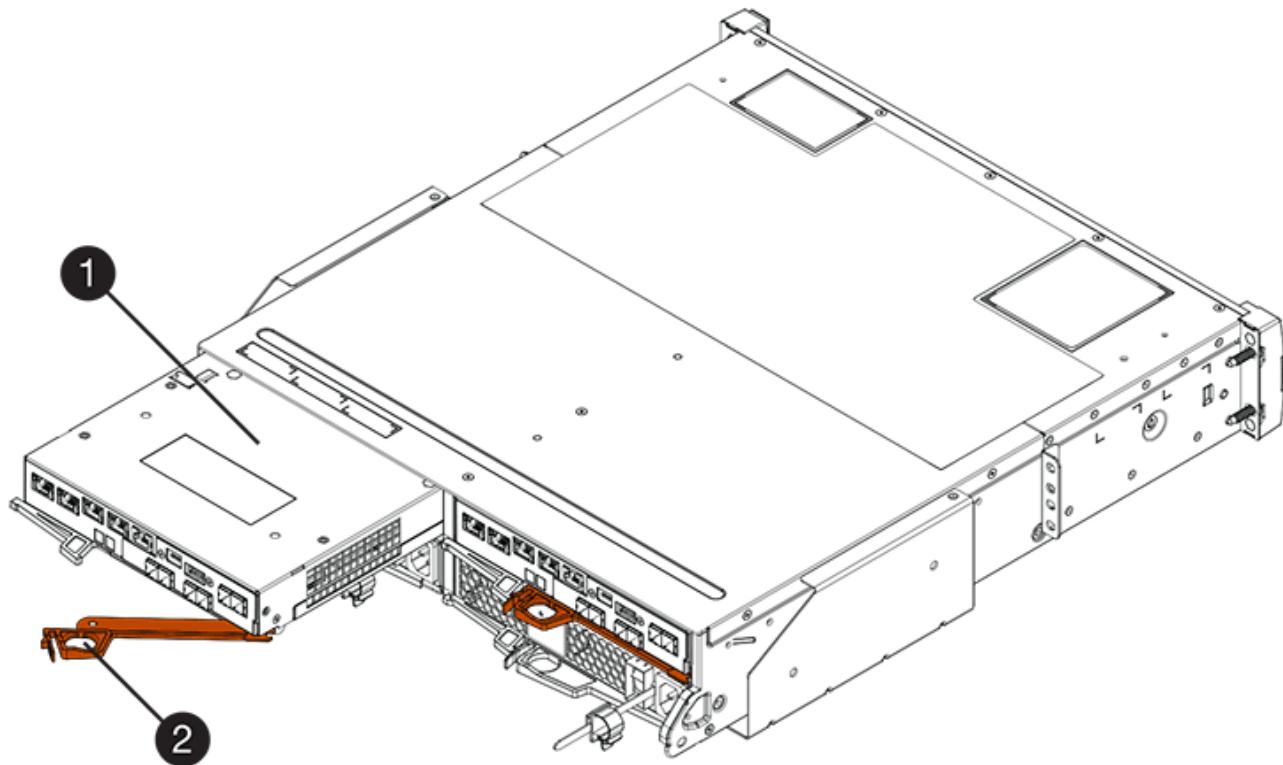


To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

4. If the host ports on the controller canister use SFP+ transceivers, leave them installed.
5. Confirm that the Cache Active LED on the back of the controller is off.

6. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

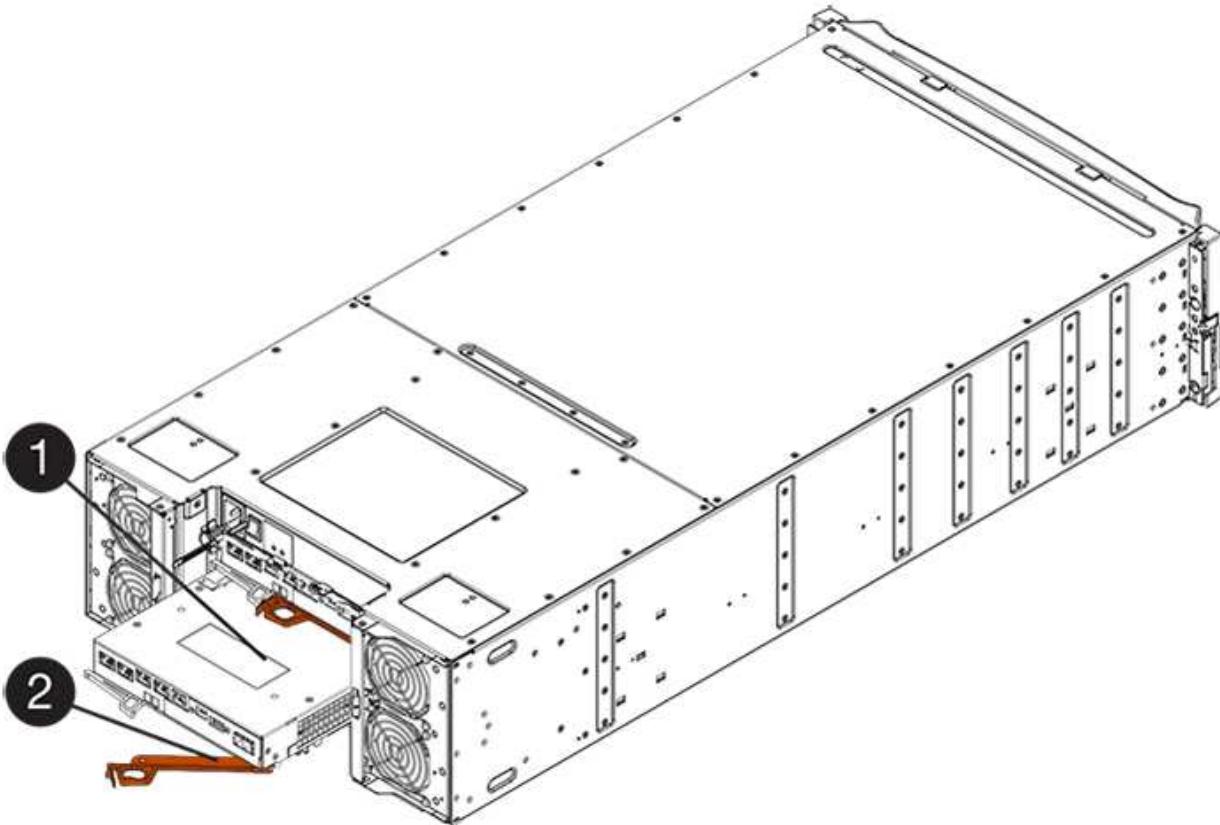
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

7. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E5724 controller shelf, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

8. Turn the controller canister over, so that the removable cover faces up.
9. Place the controller canister on a flat, static-free surface.

Step 3: Remove failed battery

After removing the controller canister from the controller shelf, remove the battery.

Steps

1. Remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

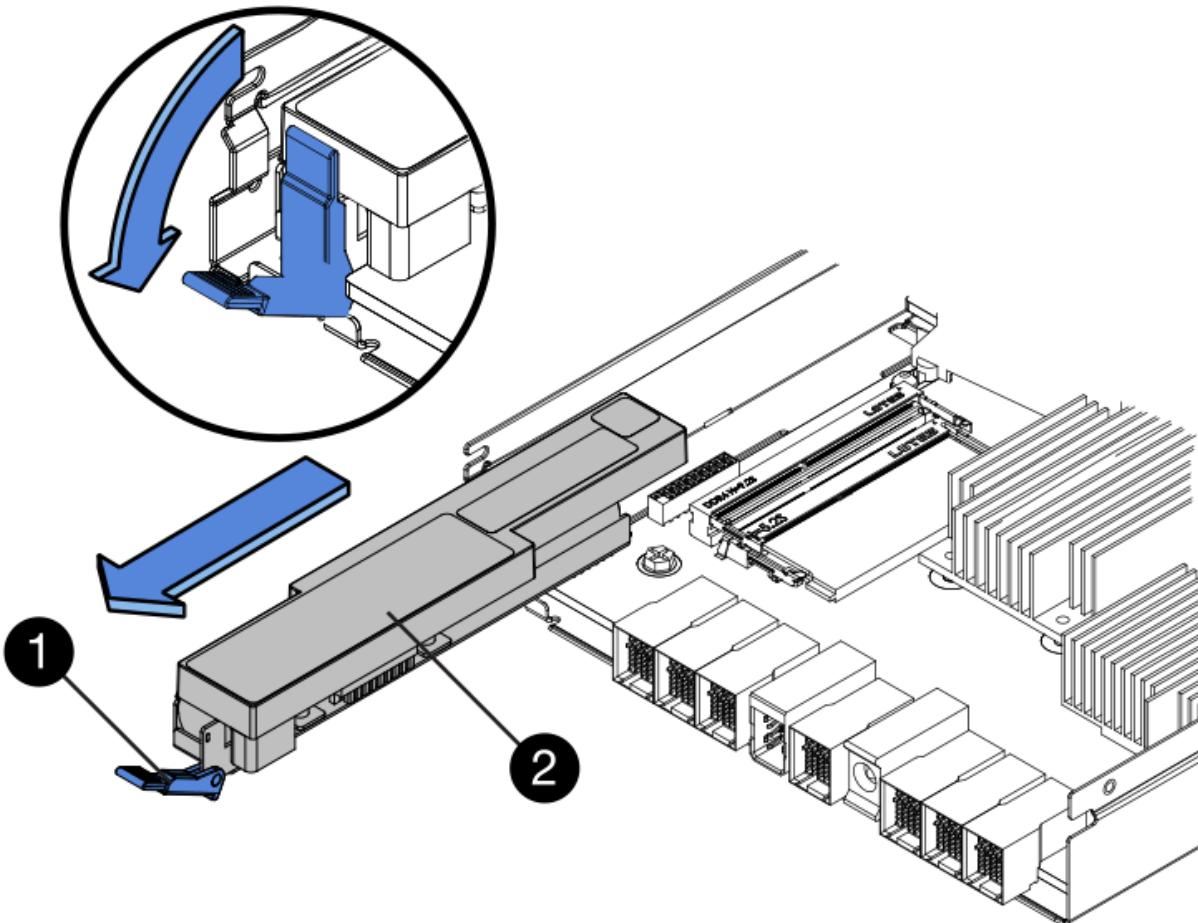
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active LED

(2) Battery

3. Locate the blue release latch for the battery.
4. Unlatch the battery by pushing the release latch down and away from the controller canister.



(1) Battery release latch

(2) Battery

5. Lift up on the battery, and slide it out of the controller canister.
6. Follow the appropriate procedures for your location to recycle or dispose of the failed battery.



To comply with International Air Transport Association (IATA) regulations, never ship a lithium battery by air unless it is installed within the controller shelf.

Step 4: Install new battery

After removing the failed battery, install a new one.

Steps

1. Unpack the new battery, and set it on a flat, static-free surface.



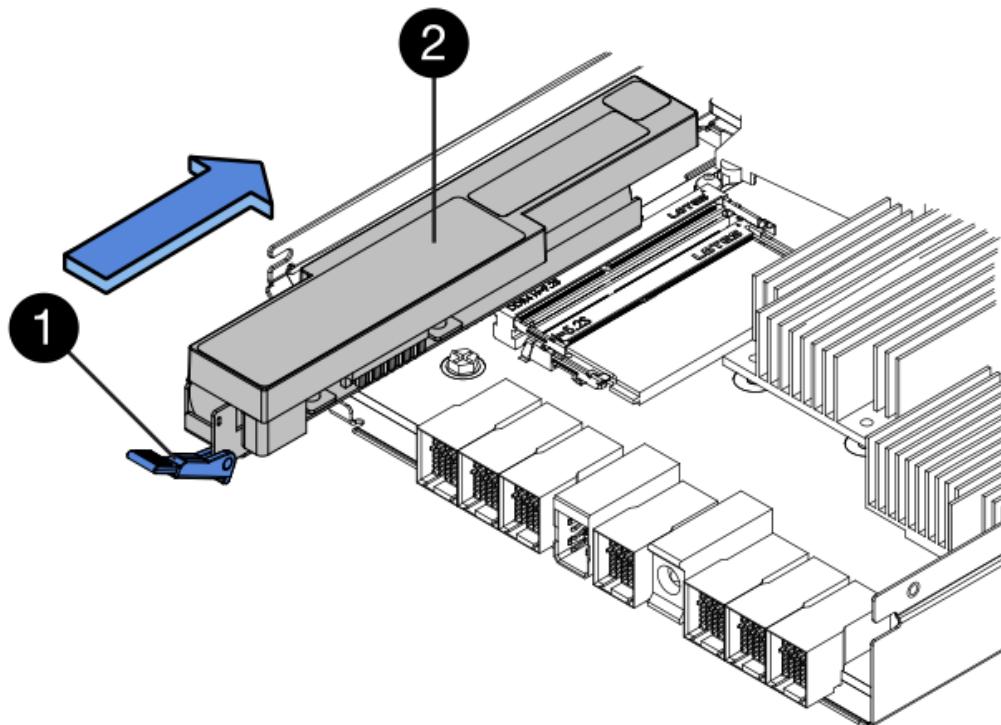
To comply with IATA safety regulations, replacement batteries are shipped with a state of charge (SoC) of 30 percent or less. When you reapply power, keep in mind that write caching will not resume until the replacement battery is fully charged and it has completed its initial learn cycle.

- Orient the controller canister so that the slot for the battery faces toward you.
- Insert the battery into the controller canister at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller canister, and slide the top of the battery beneath the small alignment pin on the left side of the canister.

- Move the battery latch up to secure the battery.

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



(1) *Battery release latch*

(2) *Battery*

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



Possible hardware damage — The metal flange at the front of the battery must be completely inserted into the slot on the controller canister (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage to the controller when you apply power.

- **Correct** — The battery's metal flange is completely inserted in the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:

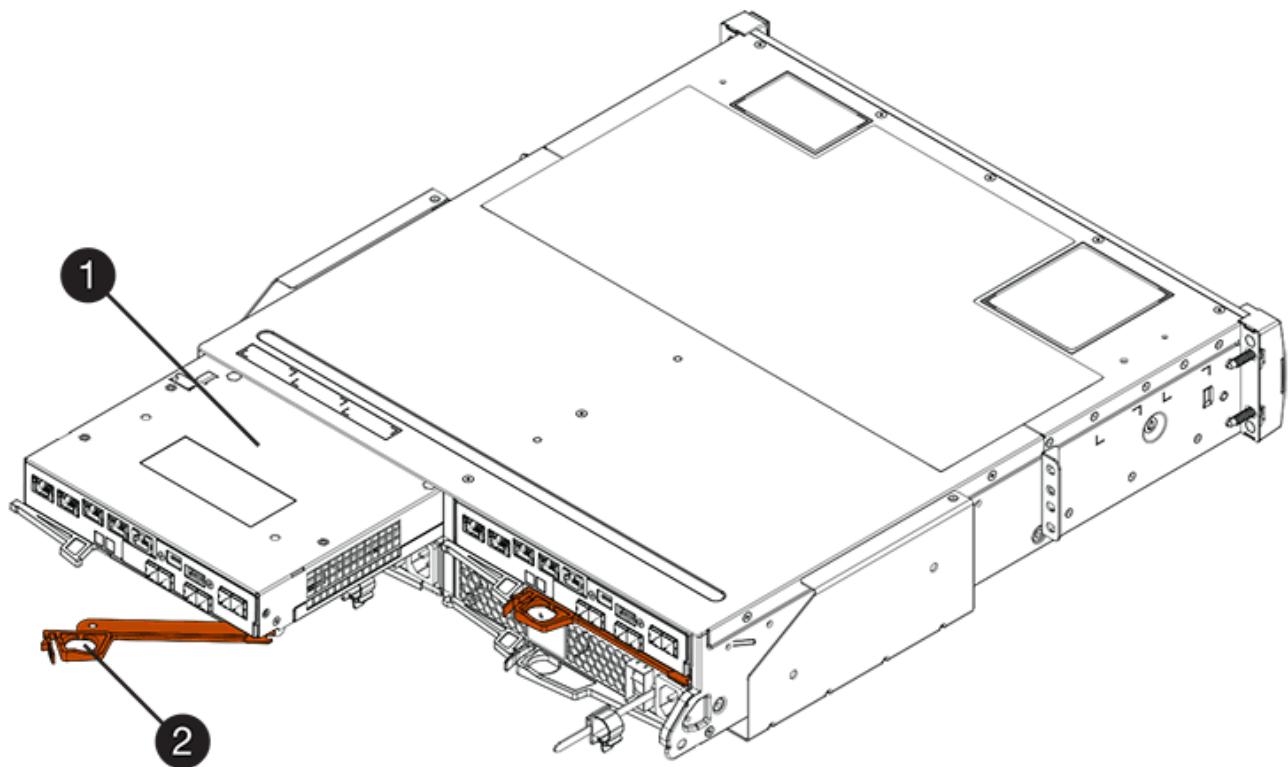


Step 5: Re-install controller canister

After installing the new battery, reinstall the controller canister into the controller shelf.

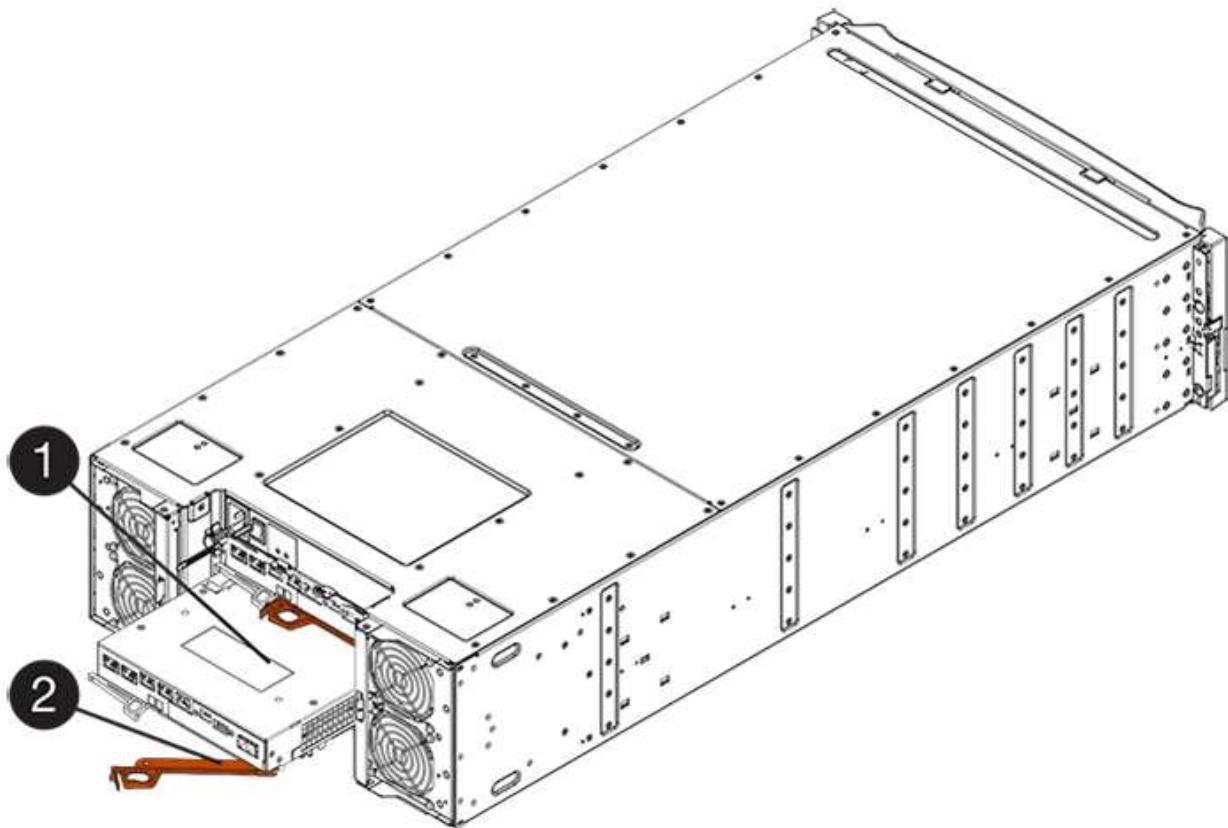
Steps

1. You reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle



(1) Controller canister

(2) Cam handle

4. Move the cam handle to the left to lock the controller canister in place.
5. Reconnect all the cables.

Step 6: Place controller online (duplex)

For a duplex configuration, place the controller online, collect support data, and resume operations.



Perform this task only if your storage array has two controllers.

Steps

1. As the controller boots, check the controller LEDs and the seven-segment display.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS, OL, blank** to indicate that the controller is offline.
- The amber Attention LED remains lit.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) Host Link LEDs

(2) Attention LED (Amber)

(3) Seven-segment display

2. Bring the controller online using SANtricity System Manager.

- From SANtricity System Manager:
 - a. Select **Hardware**.
 - b. If the graphic shows the drives, select **Show back of shelf**.
 - c. Select the controller you want to place online.
 - d. Select **Place Online** from the context menu, and confirm that you want to perform the operation.

The system places the controller online.

- Alternatively, you can bring the controllers online by using the following CLI commands:

For controller A: set controller [a] availability=online;

For controller B: set controller [b] availability=online;

- When the controller is back online, confirm that its status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the battery and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the battery.



If you cannot resolve the problem, contact technical support.

- If needed, collect support data for your storage array using SANtricity System Manager.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your battery replacement is complete. You can resume normal operations.

Controllers

Requirements for E5700 controller replacement

Before you replace an E5700 controller, review the requirements and considerations.

Each controller canister contains a controller card, a battery, and an optional host interface card (HIC).

Procedure overview

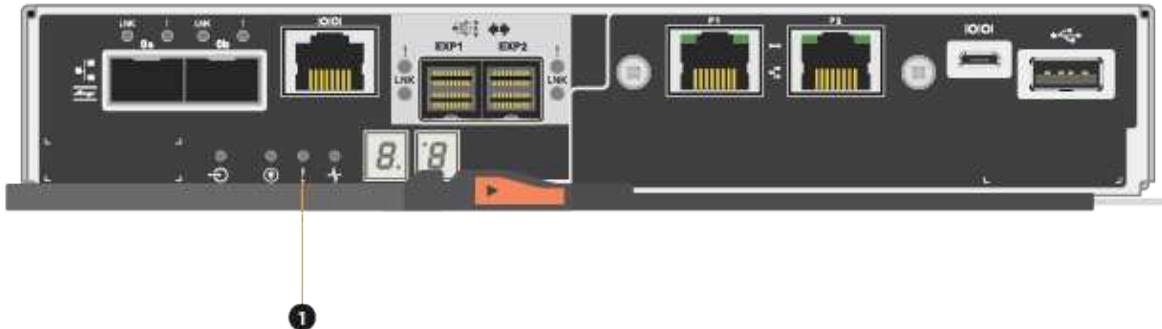
When you replace a failed controller canister, you must remove the battery and HIC, if one is installed, from the original controller canister, and install them in the replacement controller canister.

You can determine if you have a failed controller canister in two ways:

- The Recovery Guru in SANtricity System Manager directs you to replace the controller canister.
- The amber Attention LED on the controller canister is on, indicating that the controller has a fault.

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.)



(1) Attention LED



The figure shows an example controller canister; the host ports on your controller canister might be different.

Requirements for replacing a failed controller

Before you replace a controller, you must have:

- A replacement controller canister with the same part number as the controller canister you are replacing.
- An ESD wristband, or you have taken other antistatic precautions.
- Labels to identify each cable that is connected to the controller canister.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Optionally, you can use the command line interface (CLI) to perform some of the procedures. If you do not have access to the CLI, you can do one of the following:

- **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
- **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Duplex configuration requirements

For a controller shelf with two controllers (duplex configuration), you can replace a controller canister while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:

- The second controller canister in the shelf has Optimal status.
- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.

Replace controller in duplex configuration

You can replace a controller canister in a duplex (two-controller) configuration, for the following controller shelves:

- E5724 controller shelf
- E5760 controller shelf

About this task

Each controller canister contains a controller card, a battery, and an optional host interface card (HIC). When you replace a controller canister, you must remove the battery and HIC, if one is installed, from the original controller canister, and then install them in the replacement controller canister.



This task is only for storage arrays with two controllers (duplex configuration).

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.)

What you'll need

- A replacement controller canister with the same part number as the controller canister you are replacing. (See step 1 to verify the part number.)
- An ESD wristband, or you have taken other antistatic precautions.
- #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace controller (duplex)

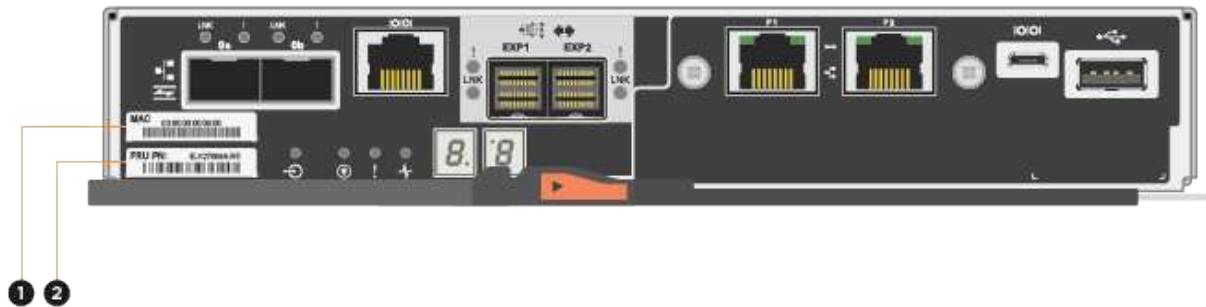
Prepare to replace a controller canister by verifying that the replacement controller canister has the correct FRU part number, backing up the configuration, and collecting support data. If the controller is still online, you must take it offline.

Steps

1. Unpack the new controller canister, and set it on a flat, static-free surface.

Save the packing materials to use when shipping the failed controller canister.

2. Locate the MAC address and FRU part number labels on the back of the controller canister.



(1) MAC address: The MAC address for management port 1 (“P1”). If you used DHCP to obtain the original controller’s IP address, you need this address to connect to the new controller.

(2) FRU part number: This number must match the replacement part number for the currently installed controller.

3. From SANtricity System Manager, locate the replacement part number for the controller canister you are replacing.

When a controller has a fault and needs to be replaced, the replacement part number is displayed in the Details area of the Recovery Guru. If you need to find this number manually, follow these steps:

- a. Select **Hardware**.
 - b. Locate the controller shelf, which is marked with the controller icon
 - c. Click the controller icon.
 - d. Select the controller, and click **Next**.
 - e. On the **Base** tab, make a note of the **Replacement Part Number** for the controller.
4. Confirm that the replacement part number for the failed controller is the same as the FRU part number for the replacement controller.



Possible loss of data access — If the two part numbers are not the same, do not attempt this procedure. In addition, if the failed controller canister includes a host interface card (HIC), you must install that HIC into the new controller canister. The presence of mismatched controllers or HICs causes the new controller to lock down when you bring it online.

5. Back up the storage array’s configuration database using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - Select **Support > Support Center > Diagnostics**.
 - Select **Collect Configuration Data**.
 - Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

6. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs when you remove a controller, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

7. If the controller is not already offline, take it offline now using SANtricity System Manager.

- From SANtricity System Manager:
 - Select **Hardware**.
 - If the graphic shows the drives, select **Show back of shelf** to show the controllers.
 - Select the controller that you want to place offline.
 - From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

- Alternatively, you can take the controllers offline by using the following CLI commands:

For controller A: set controller [a] availability=offline

For controller B: set controller [b] availability=offline

8. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

9. Select **Recheck** from the Recovery Guru, and confirm that the **OK to remove** field in the Details area displays **Yes**, indicating that it is safe to remove this component.

Step 2: Remove controller canister (duplex)

Remove a controller canister to replace the failed canister with a new one.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label each cable that is attached to the controller canister.
3. Disconnect all the cables from the controller canister.



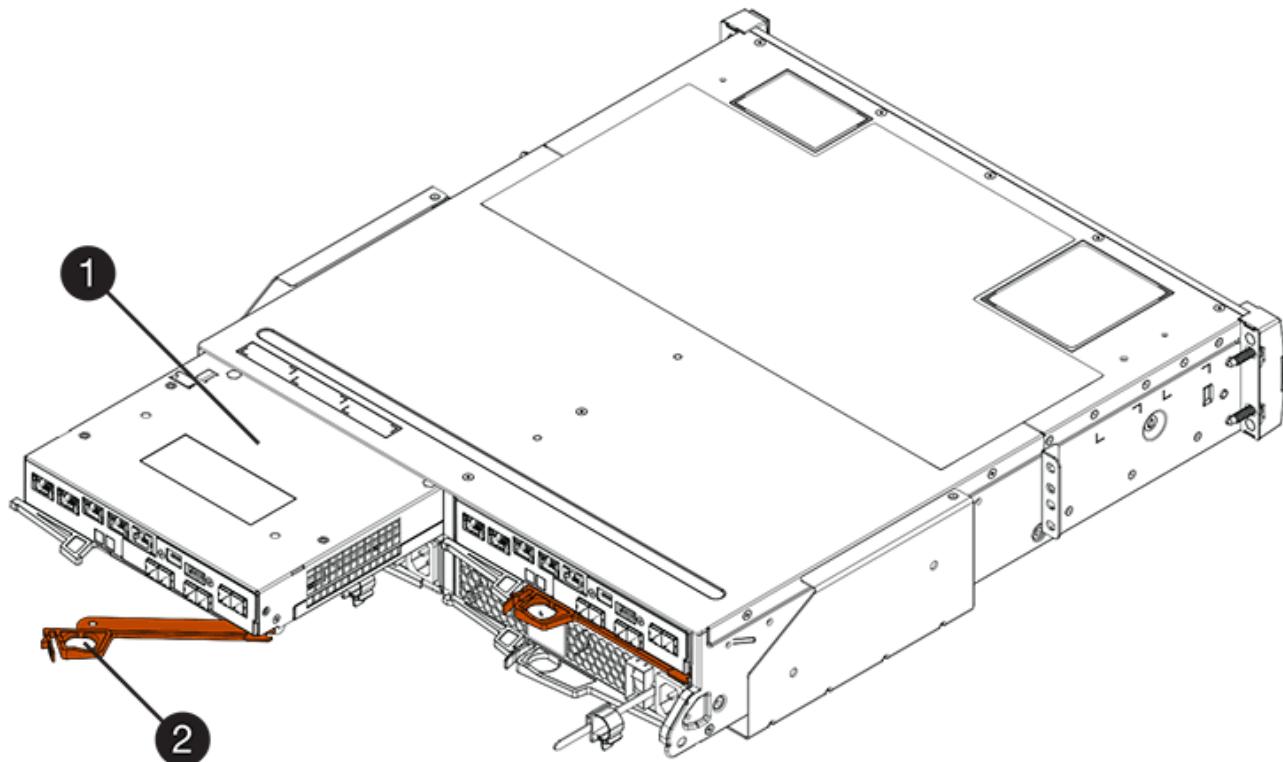
To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

4. If the controller canister has a HIC that uses SFP+ transceivers, remove the SFPs.

Because you must remove the HIC from the failed controller canister, you must remove any SFPs from the HIC ports. However, you can leave any SFPs installed in the baseboard host ports. When you reconnect the cables, you can move those SFPs to the new controller canister.

5. Confirm that the Cache Active LED on the back of the controller is off.
6. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

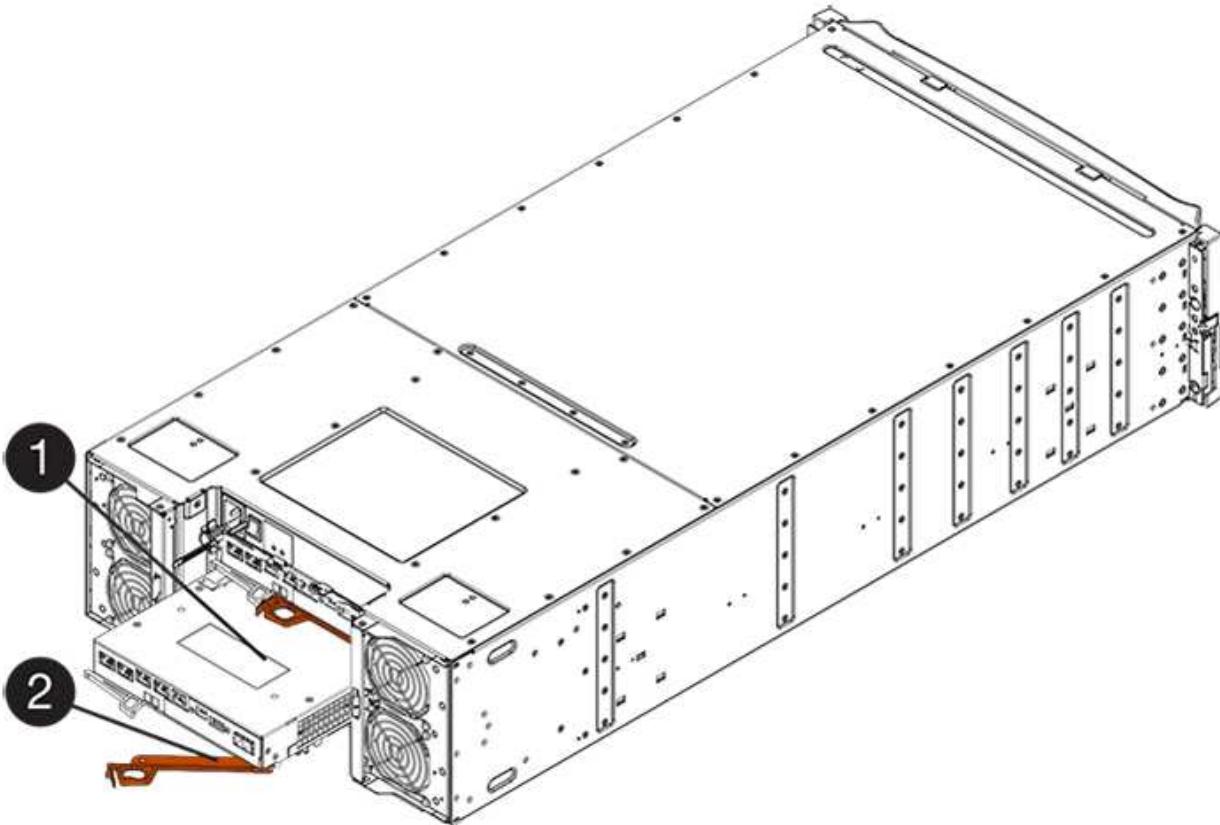
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

7. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E5724 controller shelf, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

8. Turn the controller canister over, so that the removable cover faces up.
9. Place the controller canister on a flat, static-free surface.

Step 3: Remove battery (duplex)

Remove the battery so you can install the new controller.

Steps

1. You remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

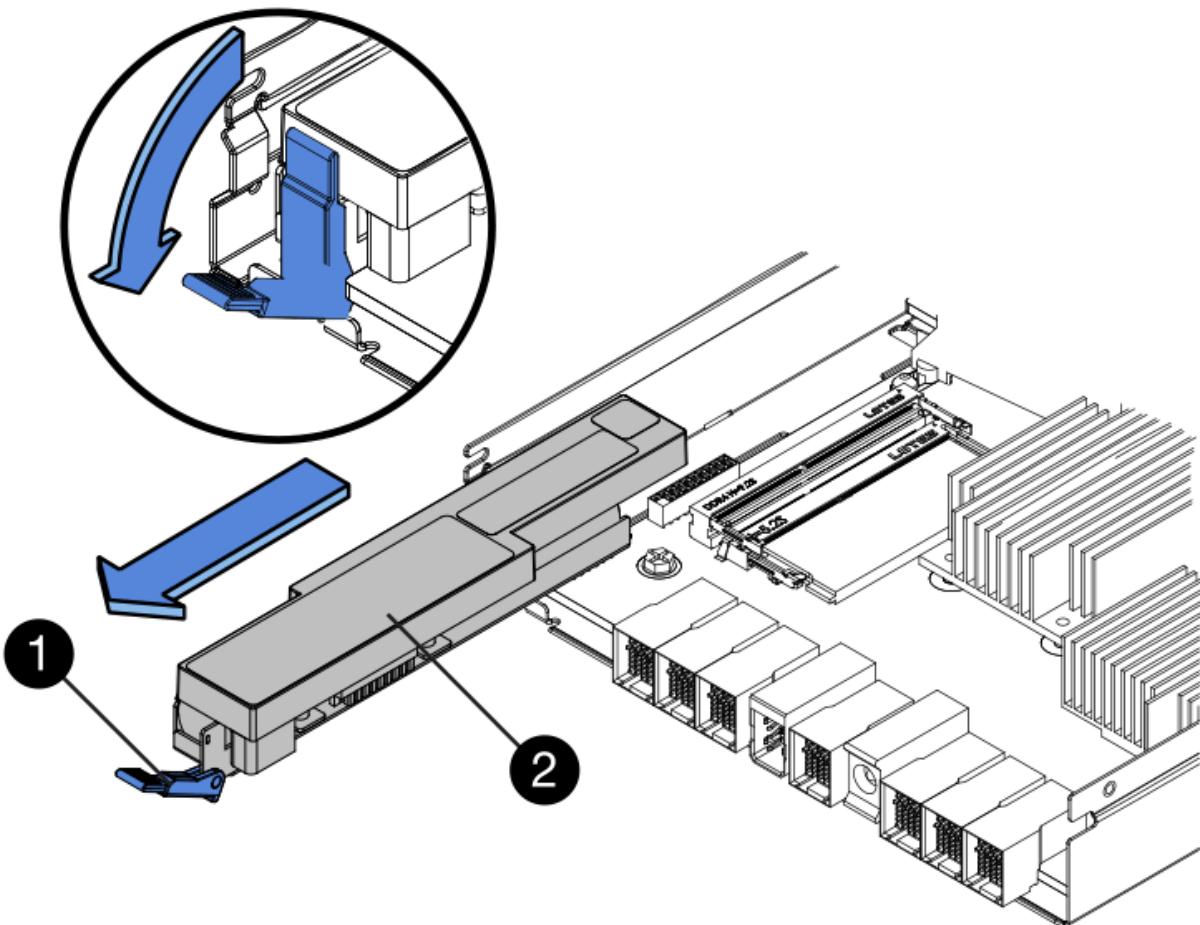
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active LED

(2) Battery

3. Locate the blue release latch for the battery.
4. Unlatch the battery by pushing the release latch down and away from the controller canister.



(1) *Battery release latch*

(2) *Battery*

5. Lift up on the battery, and slide it out of the controller canister.

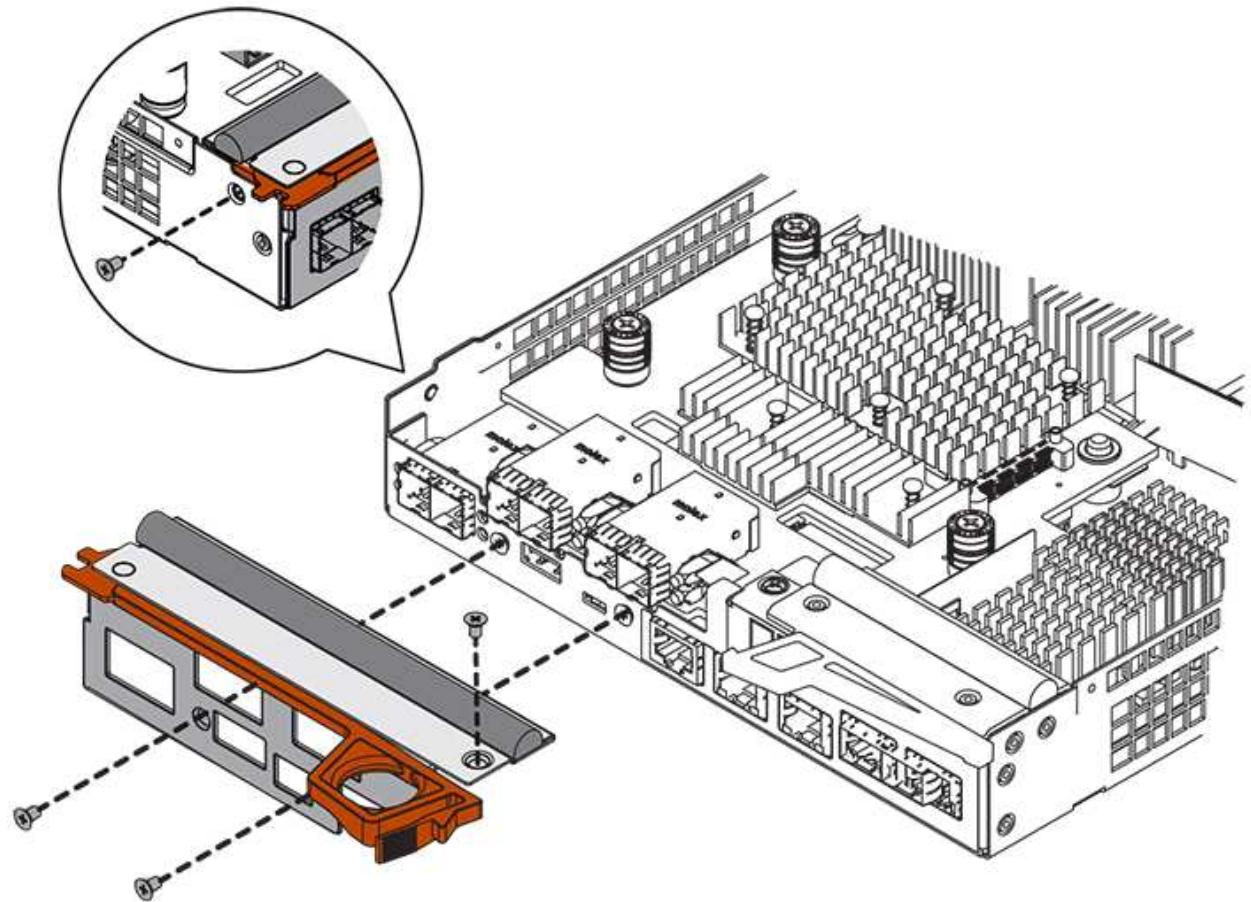
Step 4: Remove host interface card (duplex)

If the controller canister includes a host interface card (HIC), remove the HIC from the original controller canister so you can reuse it in the new controller canister.

Steps

1. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller canister.

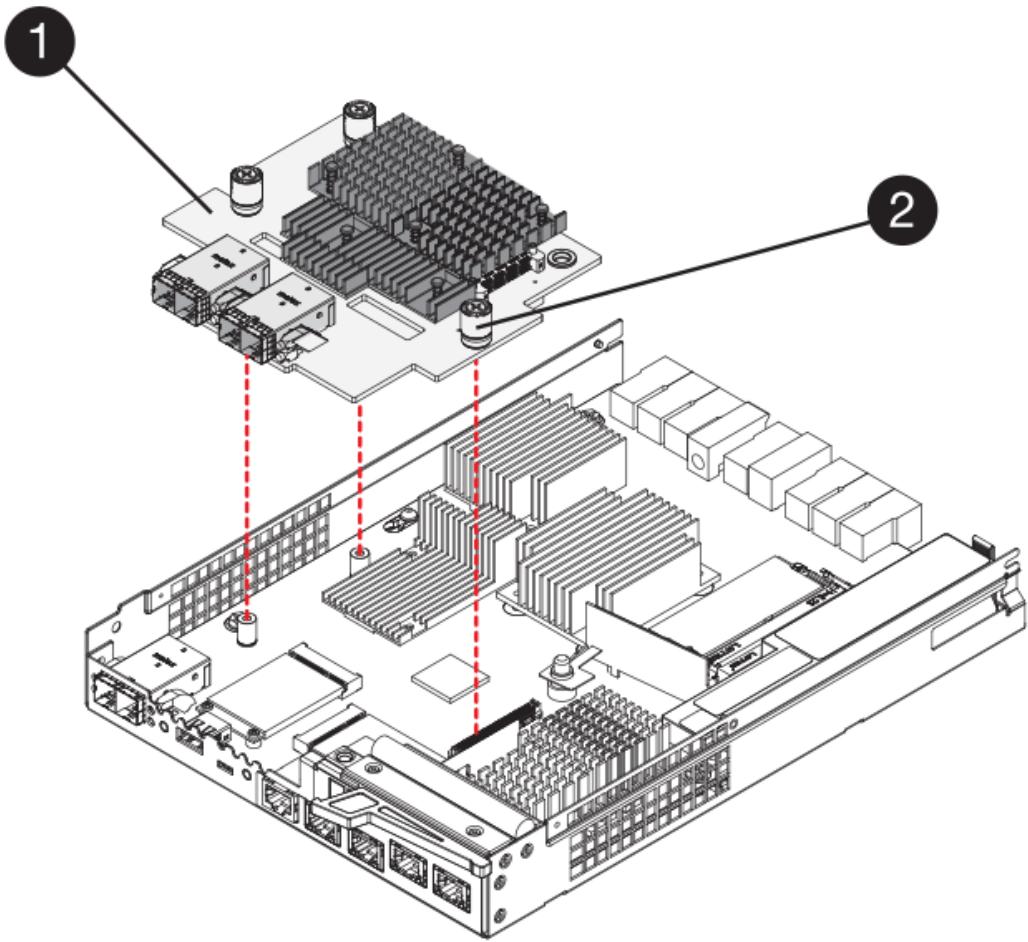
There are four screws: one on the top, one on the side, and two on the front.



2. Remove the HIC faceplate.
3. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
4. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



(1) *Host interface card (HIC)*

(2) *Thumbscrews*

5. Place the HIC on a static-free surface.

Step 5: Install battery (duplex)

Install the battery into the replacement controller canister. You can install the battery that you removed from the original controller canister or install a new battery that you ordered.

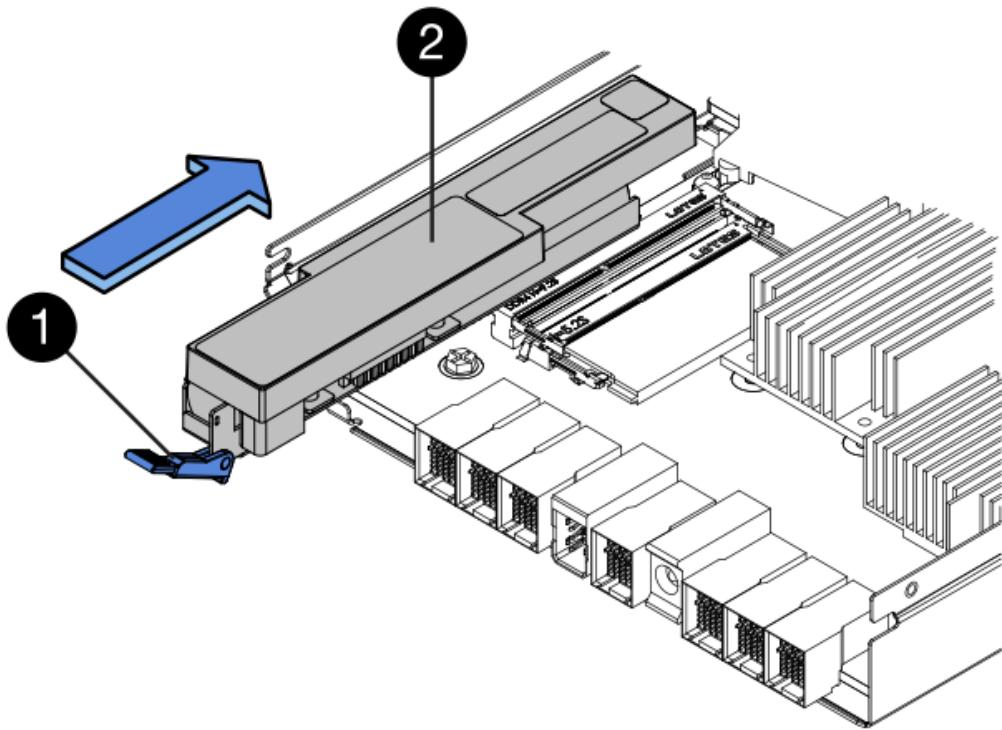
Steps

1. Turn the replacement controller canister over, 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 controller canister at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller canister, and slide the top of the battery beneath the small alignment pin on the left side of the canister.

5. Move the battery latch up to secure the battery.

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



(1) *Battery release latch*

(2) *Battery*

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



Possible hardware damage — The metal flange at the front of the battery must be completely inserted into the slot on the controller canister (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage to the controller when you apply power.

- **Correct** — The battery's metal flange is completely inserted in the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



Step 6: Install host interface card (duplex)

If you removed a HIC from the original controller canister, you must install that HIC in the new controller canister.

Steps

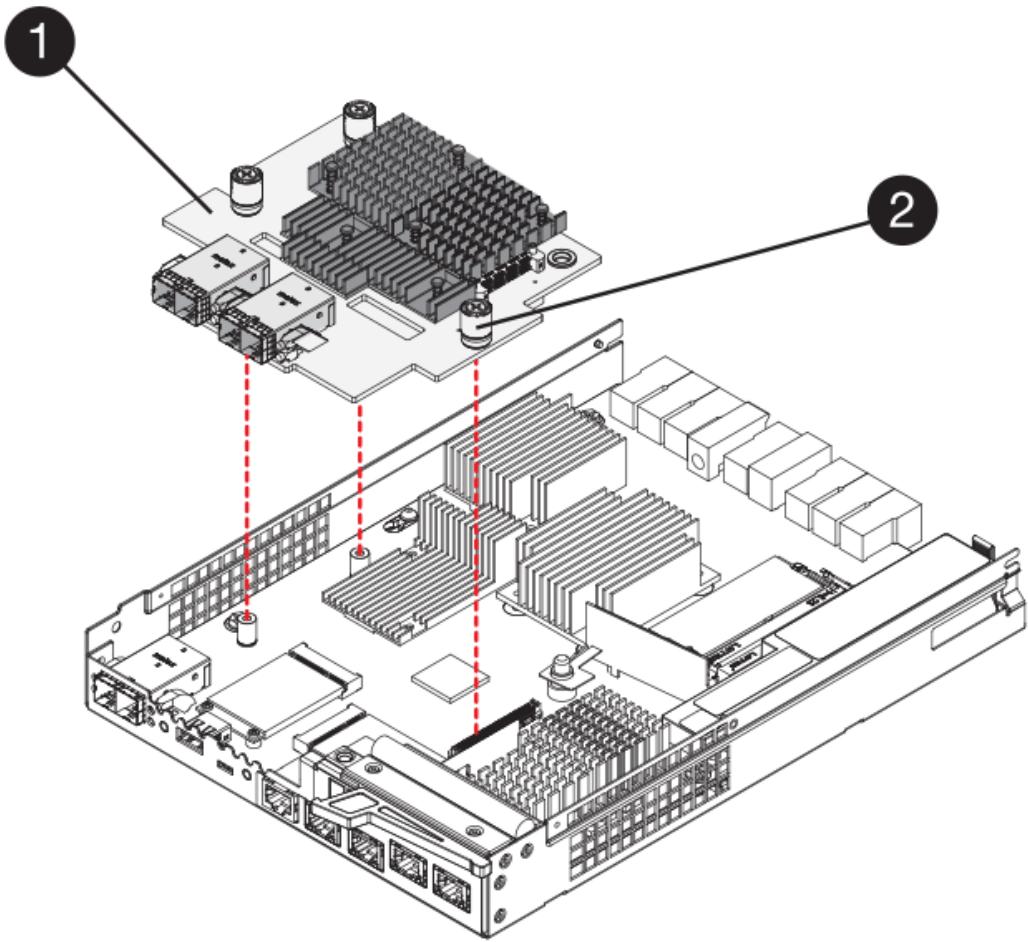
1. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller canister, and remove the faceplate.
2. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

3. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



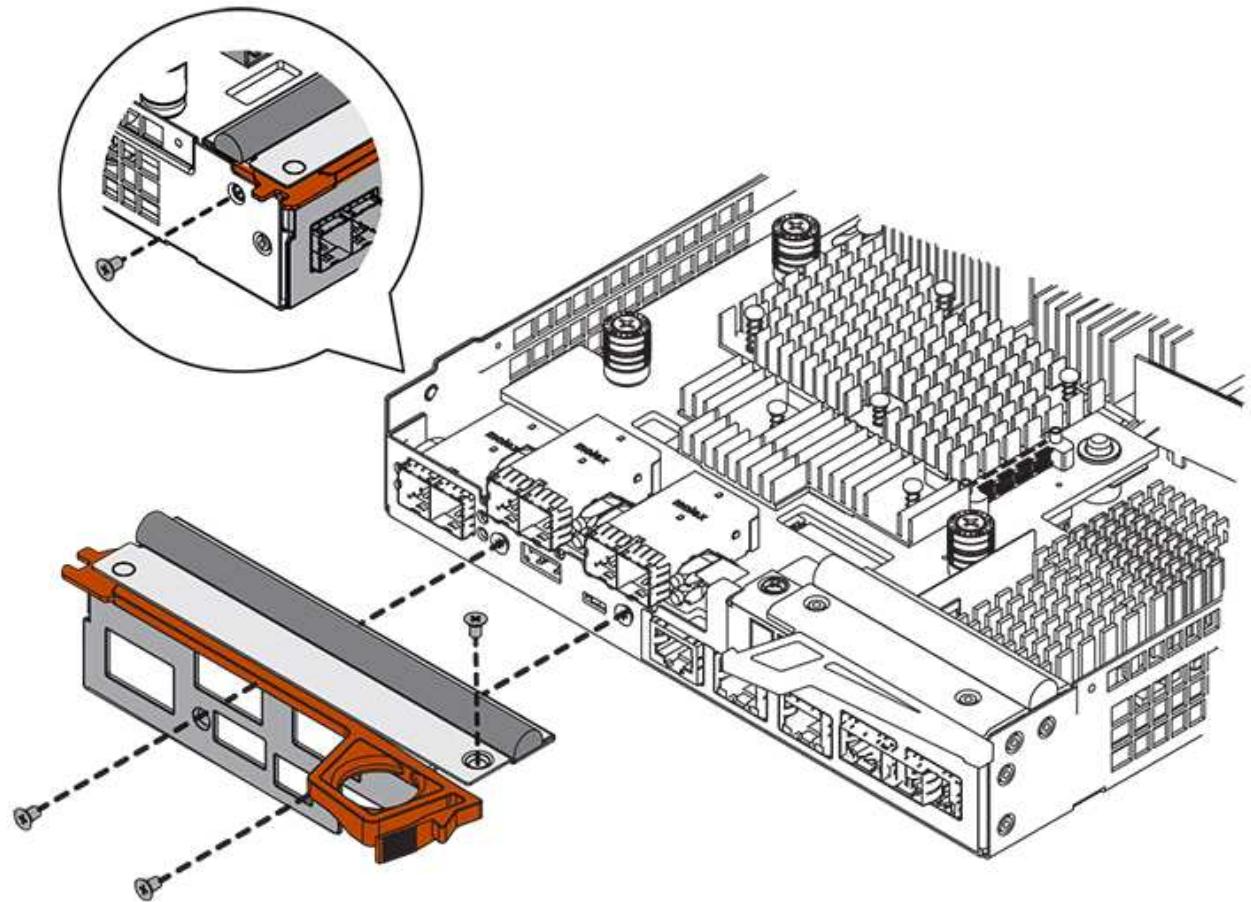
(1) *Host interface card (HIC)*

(2) *Thumbscrews*

4. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

5. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller canister to the new controller canister with four screws.

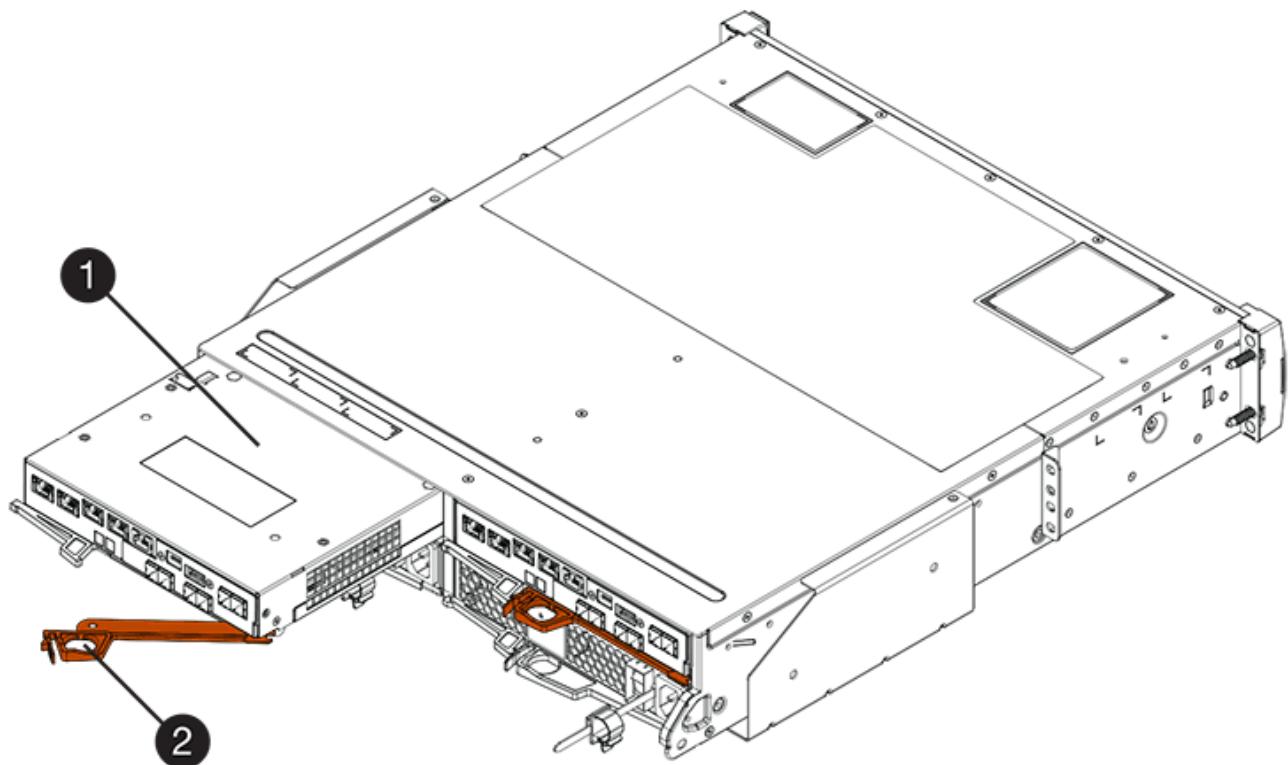


Step 7: Install new controller canister (duplex)

After installing the battery and the host interface card (HIC), if one was initially installed, you can install the new controller canister into the controller shelf.

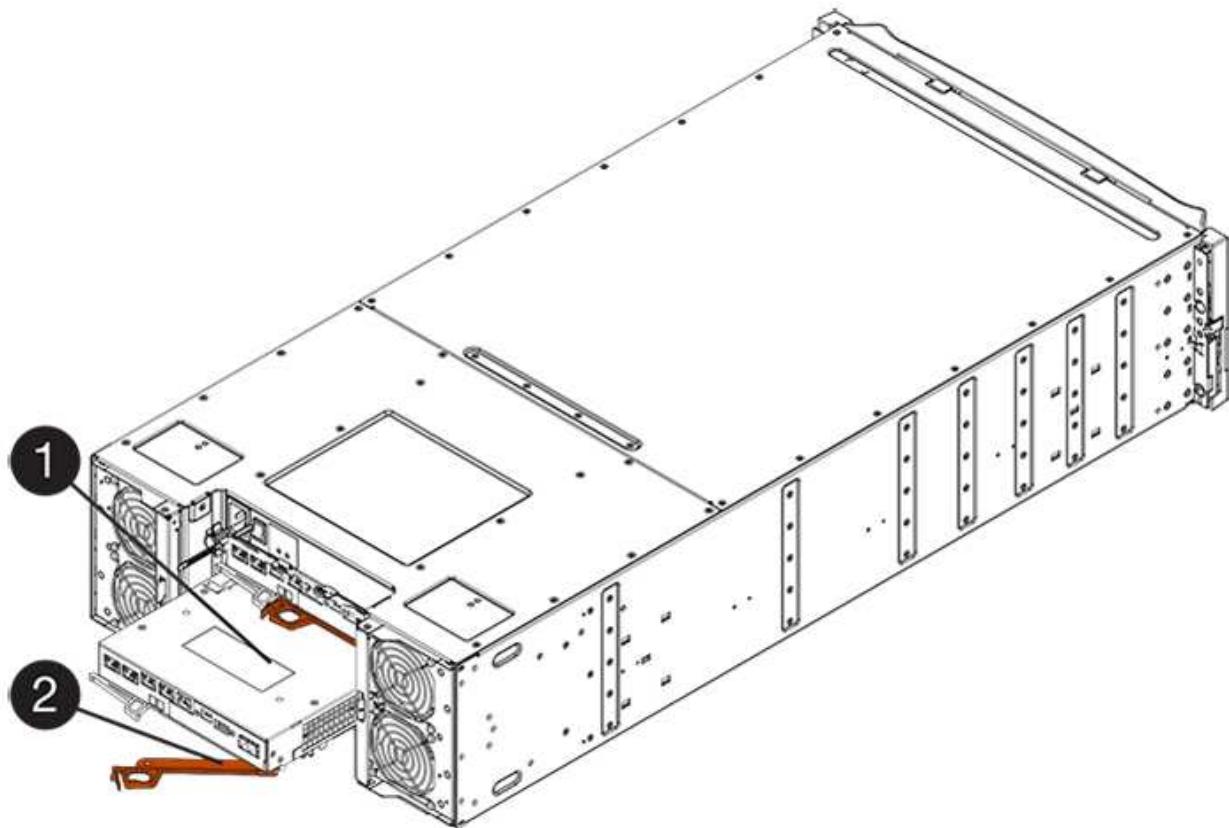
Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.



(1) Controller canister

(2) Cam handle



(1) Controller canister

(2) Cam handle

4. Move the cam handle to the left to lock the controller canister in place.
5. Install the SFPs from the original controller in the host ports on the new controller, and reconnect all the cables.

If you are using more than one host protocol, be sure to install the SFPs in the correct host ports.

6. If the original controller used DHCP for the IP address, locate the MAC address on the label on the back of the replacement controller. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



If the original controller did not use DHCP for the IP address, the new controller will adopt the IP address of the controller you removed.

Step 8: Complete controller replacement (duplex)

Place the controller online, collect support data, and resume operations.

Steps

1. As the controller boots, check the controller LEDs and the seven-segment display.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS, OL, blank** to indicate that the controller is offline.
- The amber Attention LED remains on.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) Host Link LEDs

(2) Attention LED (Amber)

(3) Seven-segment display

2. Check the codes on the controller's seven-segment display as it comes back online. If the display shows one of the following repeating sequences, immediately remove the controller.
 - **OE, L0, blank** (mismatched controllers)

- OE, L6, **blank** (unsupported HIC)



Possible loss of data access — If the controller you just installed shows one of these codes, and the other controller is reset for any reason, the second controller also could lock down.

3. When the controller is back online, confirm that its status is Optimal and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated and the controller canister is installed correctly. If necessary, remove and reinstall the controller canister.



If you cannot resolve the problem, contact technical support.

4. If required, redistribute all volumes back to their preferred owner.
 - a. Select **Storage > Volumes**.
 - b. Select **More > Redistribute volumes**.
5. Click **Hardware > Support > Upgrade Center** to ensure that the latest version of SANtricity OS software (controller firmware) is installed.

As needed, install the latest version.

6. If needed, collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

What's next?

Your controller replacement is complete. You can resume normal operations.

Canisters

Requirements for E5700 canister replacement

Before you replace an E5700 canister, review the requirements and considerations.

Canisters consist of three different types: power-fan canisters (power supplies) that supply a redundant power source and adequate cooling in a 12-drive or 24-drive controller shelf or drive shelf; power canisters that are used for power redundancy in a 60-drive controller shelf or drive shelf; and fan canisters that are used for cooling the 60-drive controller shelf or drive shelf.

Power supply



The power supply replacement procedure is applicable for IOM replacements. To replace your IOM perform the power supply replacement procedure.

Each 24-drive controller shelf or drive shelf includes two power supplies with integrated fans. These are referred to as *power-fan canisters* in SANtricity System Manager. If a power-fan canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source and adequate cooling.

Shelf types for a power supply

You can replace a power supply in the following shelves:

- E5724 controller shelf
- DE224C drive shelf

The following figure shows an example E5724 controller shelf with two power supplies (power-fan canisters). The DE224C drive shelves are identical, but they include I/O modules (IOMs) instead of controller canisters.



(1) Controller shelf with two power supplies (power-fan canisters) below the controller canisters.

The *Replace power supply* topics do not describe how to replace a failed power-fan canister in a DE1600 or DE5600 drive tray, which might be connected to the E5700 or E2800 controller shelves. For instructions for those drive tray models, refer to [Replacing a Power-Fan Canister in the DE1600 Drive Tray or the DE5600 Drive Tray](#).

Requirements for replacing a power supply

If you plan to replace a power supply, keep the following requirements in mind.

- You must have a replacement power supply (power-fan canister) that is supported for your controller shelf or drive shelf model.
- You must have an ESD wristband, or you have taken other antistatic precautions.
- You can replace a power supply (power-fan canister) while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:
 - The second power supply (power-fan canister) in the shelf has an Optimal status.
 - The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second power supply (power-fan canister) in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the power-fan canister, contact technical support.

Power canister

Each 60-drive controller shelf or drive shelf includes two power canisters for power redundancy.

Shelf types for a power canister

You can replace a power canister in the following shelves:

- E5760 controller shelves
- DE460C drive shelf

The *Replace power canister* topics do not describe how to replace a failed power canister in a DE6600 drive tray, which might be connected to the controller shelf.

The following figure shows the back of a DE460C drive shelf with the two power canisters:



The following figure shows a power canister:



Requirements for replacing a power canister

If you plan to replace a power canister, keep the following requirements in mind.

- You have a replacement power canister that is supported for your controller shelf or drive shelf model.

- You have one power canister that is installed and running.
- You have an ESD wristband, or you have taken other antistatic precautions.
- You can replace a power canister while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:
- The other power canister in the shelf has Optimal status.



While you perform the procedure, the other power canister supplies power to both fans to ensure that the equipment does not overheat.

- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second power canister in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the power canister, contact technical support.

Fan canister

Each 60-drive controller shelf or drive shelf includes two fan canisters.

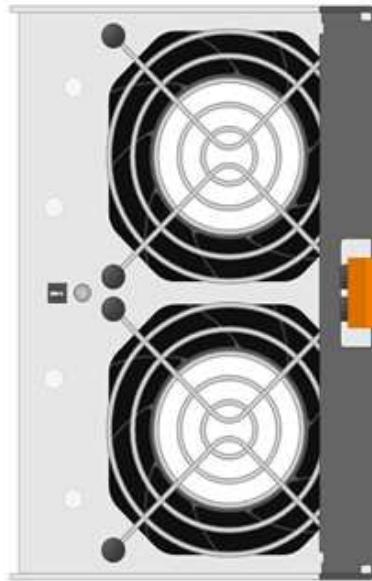
Shelf types for a fan canister

You can replace a fan canister in the following shelves:

- E5760 controller shelves
- DE460C drive shelf

The *Replace fan canister* topics do not describe how to replace a failed fan canister in a DE6600 drive tray, which might be connected to the controller shelf.

The following figure shows a fan canister:



The following figure shows the back of a DE460C shelf with two fan canisters:



Possible equipment damage — If you replace a fan canister with the power turned on, you must complete the replacement procedure within 30 minutes to prevent the possibility of overheating the equipment.

Requirements for replacing a fan canister

If you plan to replace a fan canister, keep the following requirements in mind.

- You have a replacement fan canister (fan) that is supported for your controller shelf or drive shelf model.
- You have one fan canister that is installed and running.
- You have an ESD wristband, or you have taken other antistatic precautions.
- If you perform this procedure with the power turned on, you must complete it within 30 minutes to prevent the possibility of overheating the equipment.
- You can replace a fan canister while your storage array is powered on and performing host I/O operations, as long as the following conditions are true:
 - The second fan canister in the shelf has an Optimal status.
 - The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



If the second fan canister in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the fan canister, contact technical support.

Replace E5700 power supply (24-drive)

You can replace a power supply in an E5700 array with a 24-drive shelf, which include the following shelf types:

- E5724 controller shelf
- DE224C drive shelf

About this task

Each 24-drive controller shelf or drive shelf includes two power supplies with integrated fans. These are referred to as *power-fan canisters* in SANtricity System Manager. If a power-fan canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source and adequate cooling.

You can replace a power supply while your storage array is powered on and performing host I/O operations, as long as the second power supply in the shelf has an Optimal status and the **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**.

Before you begin

- Review [Requirements for E5700 canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with the power supply. Select **Recheck** from the Recovery Guru to ensure no other items must be addressed first.
- Check that the amber Attention LED on the power supply is on, indicating that the power supply or its integrated fan has a fault. Contact technical support for assistance if both power supplies in the shelf have their amber Attention LEDs on.

What you'll need

- A replacement power supply that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace power supply

Prepare to replace a power supply in a 24-drive controller shelf or drive shelf.

Steps

1. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which power supply has failed. You can find this information in the Details area of the Recovery Guru, or you can review the information displayed for the shelf.
 - a. Select **Hardware**.
 - b. Look at the power  and fan  icons to the right of the **Shelf** drop-down lists to determine which shelf has the failed power supply.
If a component has failed, either or both icons are red.
 - c. When you find the shelf with a red icon, select **Show back of shelf**.
 - d. Select either power supply.
 - e. On the **Power Supplies** and **Fans** tabs, look at the statuses of the power-fan canisters, the power supplies, and the fans to determine which power supply must be replaced.

A component with a **Failed** status must be replaced.



If the second power supply canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed power supply. Instead, contact technical support for assistance.

3. From the back of the storage array, look at the Attention LEDs to locate the power supply you need to remove.

You must replace the power supply that has its Attention LED on.



- If the Power LED is **solid green**, the power supply is functioning correctly. If it is **Off**, the power supply failed, the AC switch is turned off, the AC power cord is not properly installed, or the AC power cord input voltage is not within margin (there is a problem at the source end of the AC power cord).

If the Attention LED is **solid amber**, the power supply or its integrated fan has a fault.

Step 2: Remove failed power supply

Remove a failed power supply so you can replace it with a new one.

Steps

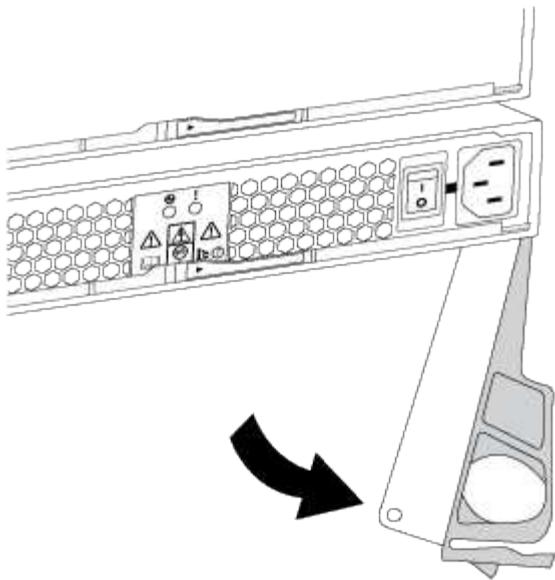
1. Unpack the new power supply, and set it on a level surface near the drive shelf.

Save all packing materials for use when returning the failed power supply.

2. Turn off the power supply and disconnect the power cables:

- a. Turn off the power switch on the power supply.
- b. Open the power cord retainer, and then unplug the power cord from the power supply.
- c. Unplug the power cord from the power source.

3. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.



4. Use the cam handle to slide the power supply out of the system.



When removing a power supply, always use two hands to support its weight.

As you remove the power supply, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

Step 3: Install new power supply

Install a new power supply to replace the failed one.

Steps

1. Make sure that the on/off switch of the new power supply is in the **Off** position.
2. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis using the cam handle.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system; you can damage the connector.

3. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
4. Reconnect the power supply cabling:
 - a. Reconnect the power cord to the power supply and the power source.
 - b. Secure the power cord to the power supply using the power cord retainer.
5. Turn on the power to the new power-fan canister.

Step 4: Complete power supply replacement

Confirm that the new power supply is working correctly, gather support data, and resume normal operations.

Steps

1. On the new power supply, check that the green Power LED is on and the amber Attention LED is OFF.
2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed power supply is still being reported, repeat the steps in [Step 2: Remove failed power supply](#) and in [Step 3: Install new power supply](#). If the problem persists, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Support Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your power supply replacement is complete. You can resume normal operations.

Replace E5700 power canister (60-drive)

You can replace a power supply in an E5700 array with a 60-drive shelf, which include the following shelf types:

- E5760 controller shelf
- DE460C drive shelf

About this task

Each 60-drive controller shelf or drive shelf includes two power canisters for power redundancy. If a power canister fails, you must replace it as soon as possible to ensure that the shelf has a redundant power source.

You can replace a power canister while your storage array is powered on and performing host I/O operations, as long as the second power canister in the shelf has an Optimal status and the **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**.

While you perform this task, the other power canister supplies power to both fans to ensure that the equipment does not overheat.

Before you begin

- Review [Requirements for E5700 canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
- Check that the amber Attention LED on the power canister is on, indicating that the canister has a fault. Contact technical support for assistance if both power canisters in the shelf have their amber Attention LEDs on.

What you'll need

- One power canister that is installed and running.
- A replacement power canister that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace power canister

Prepare to replace a power canister in a 60-drive controller shelf or drive shelf.

Steps

1. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which power canister has failed.

- a. Select **Hardware**.
- b. Look at the power  icon to the right of the **Shelf** drop-down lists to determine which shelf has the failed power canister.

If a component has failed, this icon is red.

- c. When you find the shelf with a red icon, select **Show back of shelf**.
- d. Select either power canister or the red power icon.
- e. On the **Power Supplies** tab, look at the statuses of the power canisters to determine which power canister must be replaced.

A component with a **Failed** status must be replaced.



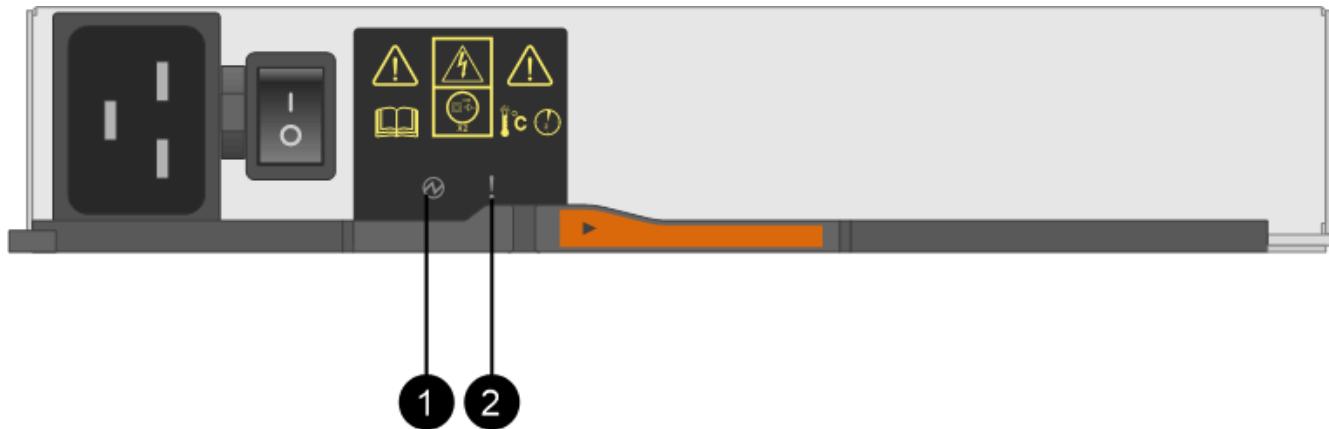
If the second power canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed power canister. Instead, contact technical support for assistance.



You can also find information about the failed power canister in the Details area of the Recovery Guru, or you can review the information displayed for the shelf, or you can review the Event Log under Support and filter by Component Type.

3. From the back of the storage array, look at the Attention LEDs to locate the power canister you need to remove.

You must replace the power canister that has its Attention LED on.



(1) Power LED. If it is **Solid green**, the power canister is functioning correctly. If it is **Off**, the power canister failed, the AC switch is turned off, the AC power cord is not properly installed, or the AC power cord input voltage is not within margin (there is a problem at the source end of the AC power cord).

(2) Attention LED. If it is **Solid amber**, the power canister has a fault, or there is no input power to this power canister, but the other power canister is operating.

Step 2: Remove failed power canister

Remove a failed power canister so you can replace it with a new one.

Steps

1. Put on antistatic protection.
 2. Unpack the new power canister, and set it on a level surface near the shelf.
- Save all packing materials for use when returning the failed power canister.
3. Turn off the power switch on the power canister that you need to remove.
 4. Open the power cord retainer of the power canister that you need to remove, and then unplug the power cord from the power canister.
 5. Press the orange latch on the power canister cam handle, and then open the cam handle to fully release the power canister from the mid plane.
 6. Use the cam handle to slide the power canister out of the shelf.



When removing a power canister, always use two hands to support its weight.

Step 3: Install new power canister

Install a new power canister to replace the failed one.

Steps

1. Make sure the on/off switch of the new power canister is in the Off position.
2. Using both hands, support and align the edges of the power canister with the opening in the system chassis, and then gently push the power canister into the chassis using the cam handle until it locks into place.



Do not use excessive force when sliding the power canister into the system; you can damage the connector.

3. Close the cam handle so that the latch clicks into the locked position and the power canister is fully seated.
4. Reconnect the power cord to the power canister, and secure the power cord to the power canister using the power cord retainer.
5. Turn on the power to the new power canister.

Step 4: Complete power canister replacement

Confirm that the new power canister is working correctly, gather support data, and resume normal operations.

Steps

1. On the new power canister, check that the green Power LED is on and the amber Attention LED is OFF.
2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed power canister is still being reported, repeat the steps in [Step 2: Remove failed power canister](#) and in [Step 3: Install new power canister](#). If the problem persists, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your power canister replacement is complete. You can resume normal operations.

Replace E5700 fan canister (60-drive)

You can replace a fan canister in an E5700 array with a 60-drive shelf, which include the following shelf types:

- E5760 controller shelf
- DE460C drive shelf

About this task

Each 60-drive controller shelf or drive shelf includes two fan canisters. If a fan canister fails, you must replace it as soon as possible to ensure that the shelf has adequate cooling.



Possible equipment damage—If you perform this procedure with the power turned on, you must complete it within 30 minutes to prevent the possibility of overheating the equipment.

Before you begin

- Review [Requirements for E5700 canister replacement](#).
- Review the details in the Recovery Guru to confirm that there is an issue with a battery and to ensure no other items must be addressed first.
- Check that the amber Attention LED on the fan canister is on, indicating that the fan has a fault. Contact technical support for assistance if both fan canisters in the shelf have their amber Attention LEDs on.

What you'll need

- A replacement fan canister (fan) that is supported for your controller shelf or drive shelf model.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace fan canister

Prepare to replace a fan canister in a 60-drive controller shelf or drive shelf.

Steps

1. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

2. From SANtricity System Manager, determine which fan canister has failed.

- a. Select **Hardware**.
- b. Look at the fan  icon to the right of the **Shelf** drop-down lists to determine which shelf has the failed fan canister.

If a component has failed, this icon is red.

- c. When you find the shelf with a red icon, select **Show back of shelf**.
- d. Select either fan canister or the red fan icon.
- e. On the **Fans** tab, look at the statuses of the fan canisters to determine which fan canister must be replaced.

A component with a **Failed** status must be replaced.

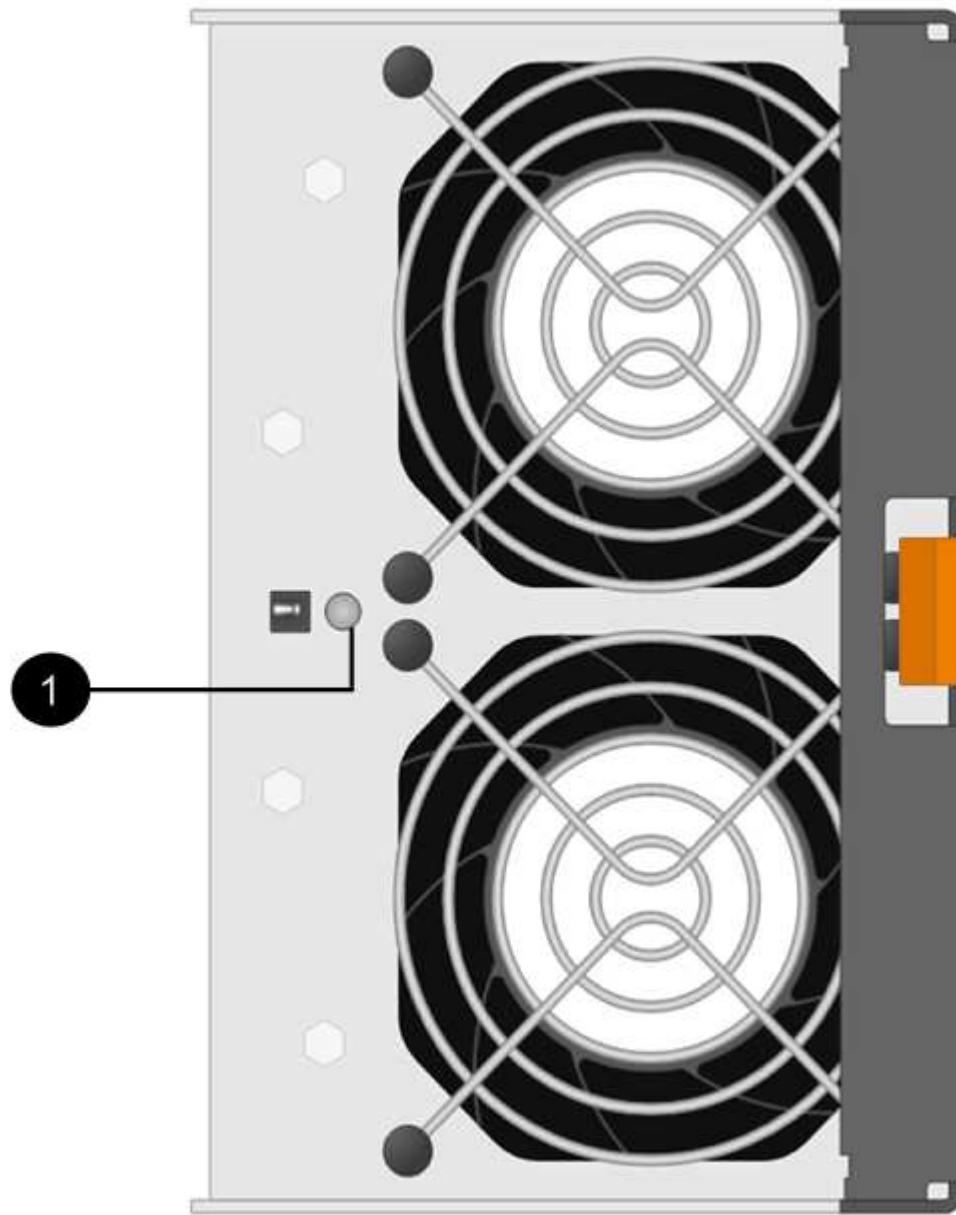


If the second fan canister in the shelf does not have **Optimal** status, do not attempt to hot-swap the failed fan canister. Instead, contact technical support for assistance.

You can also find information about the failed fan canister in the Details area of the Recovery Guru, or you can review the Event Log under Support and filter by Component Type.

3. From the back of the storage array, look at the Attention LEDs to locate the fan canister you need to remove.

You must replace the fan canister that has its Attention LED on.



(1) Attention LED. If this LED displays as **Solid amber**, then the fan has a fault.

Step 2: Remove failed fan canister and install new one

Remove a failed fan canister so you can replace it with a new one.



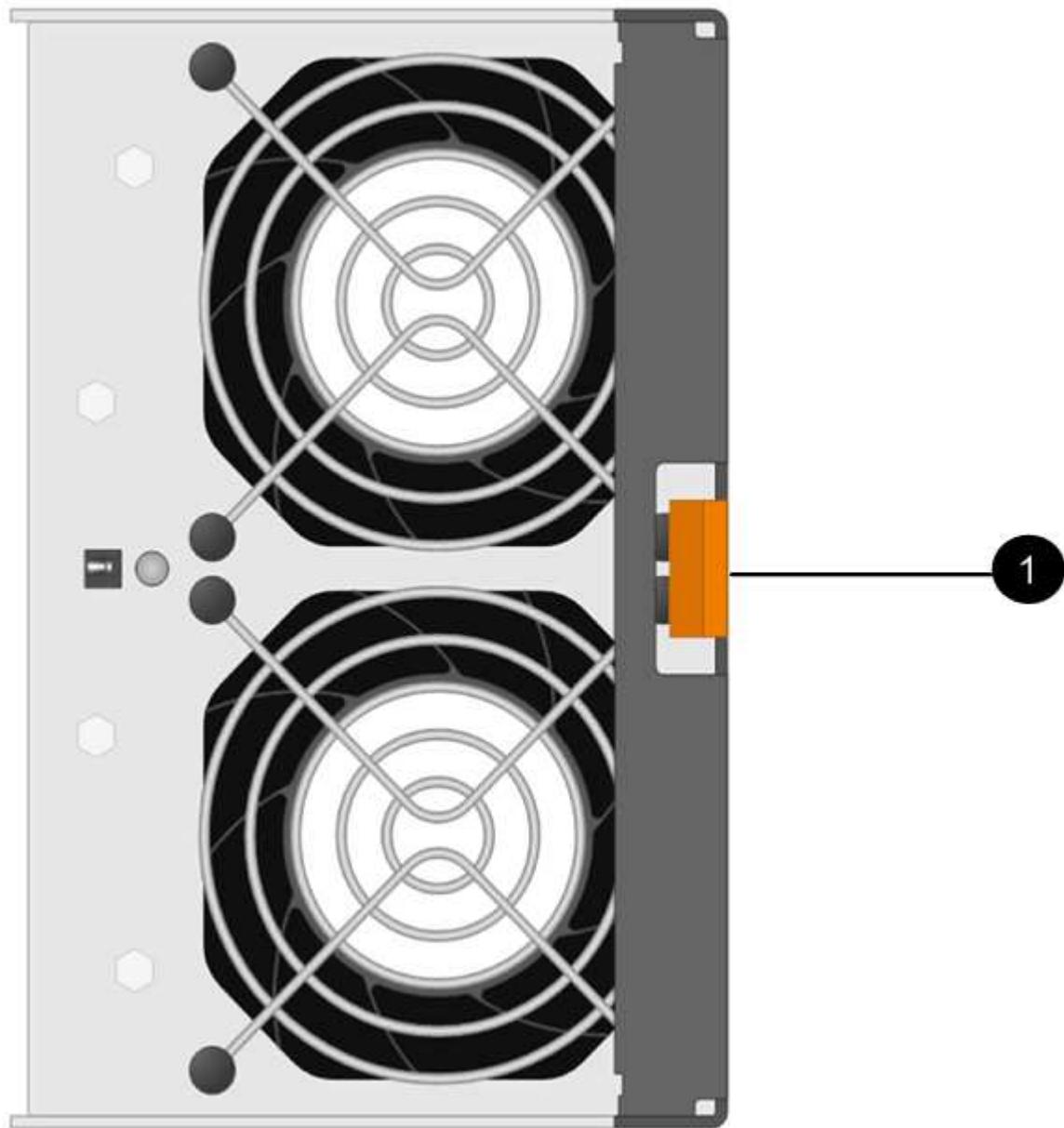
If you do not turn off the power to your storage array, ensure that you remove and replace the fan canister within 30 minutes to prevent the system from overheating.

Steps

1. Unpack the new fan canister, and place it on a level surface near the shelf.

Save all packing material for use when returning the failed fan.

2. Press the orange tab to release the fan canister handle.



(1) Tab that you press to release the fan canister handle.

3. Use the fan canister handle to pull the fan canister out of the shelf.



(1) Handle to pull the fan canister out.

4. Slide the replacement fan canister all the way into the shelf, and then move the fan canister handle until it latches with the orange tab.

Step 3: Complete fan canister replacement

Confirm that the new fan canister is working correctly, gather support data, and resume normal operations.

Steps

1. Check the amber Attention LED on the new fan canister.



After you replace the fan canister, the Attention LED stays on (solid amber) while the firmware checks that the fan canister was installed correctly. The LED goes off after this process is complete.

2. From the Recovery Guru in SANtricity System Manager, select **Recheck** to ensure the problem has been resolved.
3. If a failed fan canister is still being reported, repeat the steps in [Step 2: Remove failed fan canister and install new one](#). If the problem persists, contact technical support.
4. Remove the antistatic protection.
5. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your fan canister replacement is complete. You can resume normal operations.

Drives

Requirements for E5700 drive replacement

Before you replace a drive, review the requirements and considerations.

Shelf types

You can replace a drive in a 24-drive shelf, in a 60-drive shelf, or in a drive drawer.

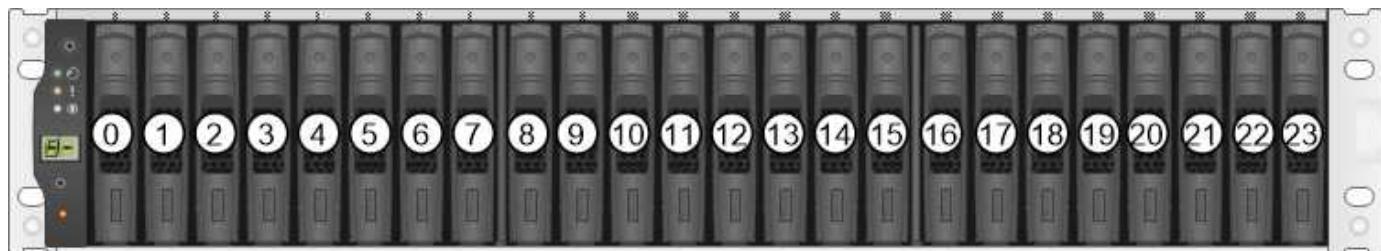
This procedure applies to IOM12 and IOM12B drive shelves, and DCM and DCM2 drive shelves.

 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.)

24-drive shelves

The figures show how the drives are numbered in each type of shelf (the shelf's front bezel or end caps have been removed).

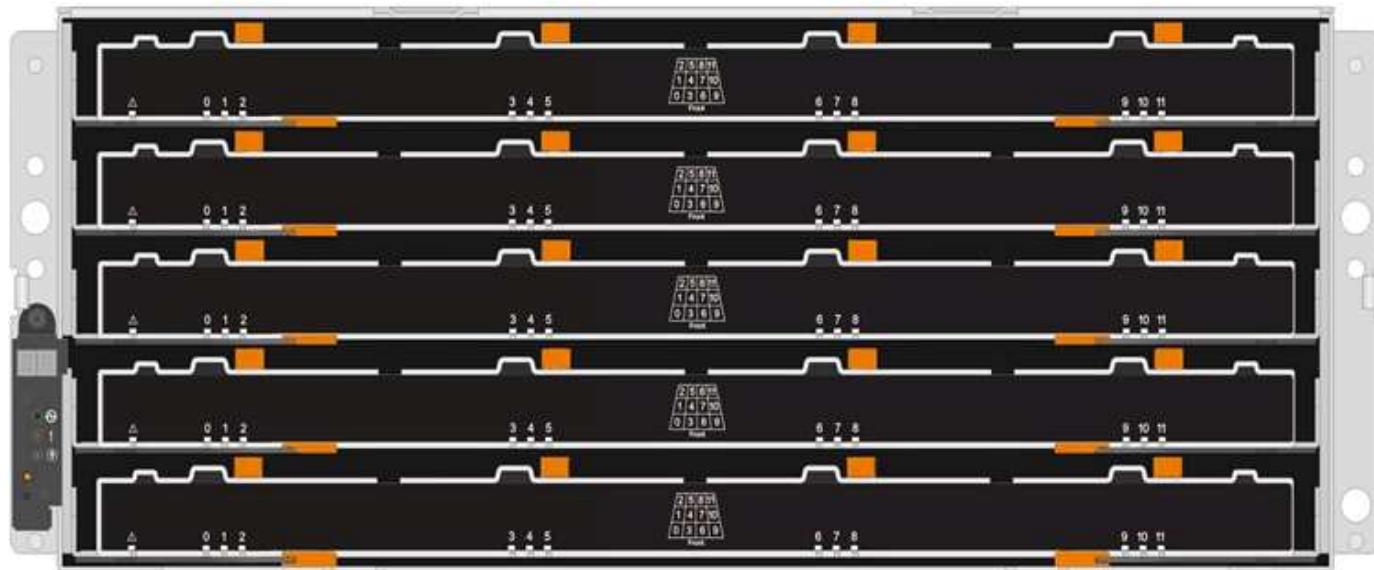
Drive numbering in an E5724 controller shelf or DE224C drive shelf



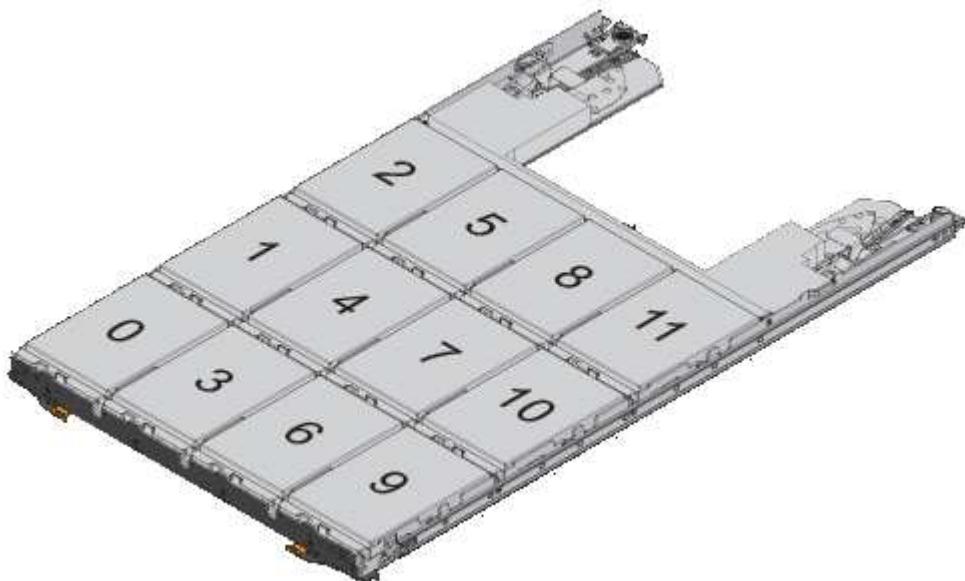
 Your E5724 storage array might include one or more SAS-2 legacy expansion drive trays, including the DE5600 24-drive tray or the DE6600 60-drive tray. For instructions for replacing a drive in one of these drive trays, see [Replacing a Drive in E2660, E2760, E5460, E5560, or E5660 Drive Trays](#) and [Replacing a Drive in E2600, E2700, E5400, E5500, and E5600 12-Drive or 24-Drive Trays](#).

60-drive shelves

Both the E5760 controller shelf and the DE460C drive shelf consist of five drive drawers that each contain 12 drive slots. Drive drawer 1 is at the top, and drive drawer 5 is at the bottom.



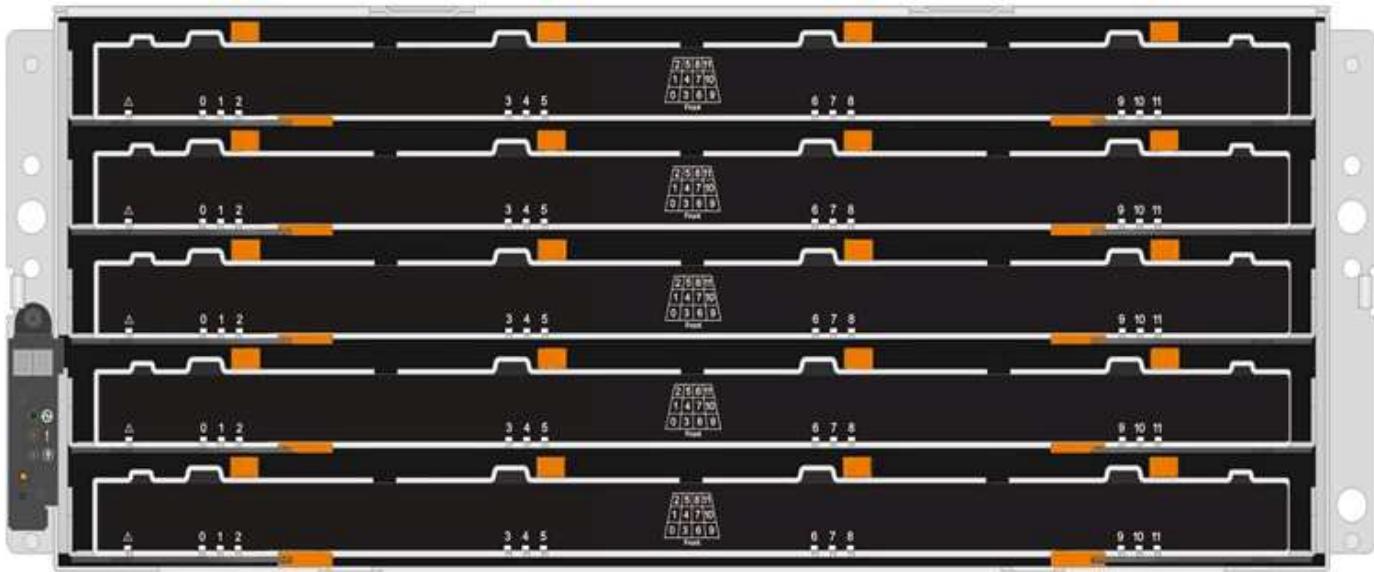
For both an E5760 controller shelf drawer and a DE460C drive shelf drawer, drives are numbered from 0 to 11 in each drive drawer within the shelf.



Your E5760 storage array might include one or more SAS-2 legacy expansion drive trays, including the DE1600 12-drive tray, the DE5600 24-drive tray, or the DE6600 60-drive tray. For instructions for replacing a drive in one of these drive trays, see [Replacing a Drive in E2660, E2760, E5460, E5560, or E5660 Drive Trays](#) and [Replacing a Drive in E2600, E2700, E5400, E5500, and E5600 12-Drive or 24-Drive Trays](#).

Drive drawer

You can replace a drive drawer in a E5760 controller shelf and a DE460C drive shelf. Each of these 60-drive shelves has five drive drawers.



Each of the five drawers can hold up to 12 drives.



Requirements for handling drives



The drives in your storage array are fragile. Improper drive handling is a leading cause of drive failure.

Follow these rules to avoid damaging the drives in your storage array:

- Prevent electrostatic discharge (ESD):
 - Keep the drive in the ESD bag until you are ready to install it.
 - Do not insert a metal tool or knife into the ESD bag.
- Open the ESD bag by hand or cut the top off with a pair of scissors.
- Keep the ESD bag and any packing materials in case you must return a drive later.

- Always wear an ESD wrist strap grounded to an unpainted surface on your storage enclosure chassis. If a wrist strap is unavailable, touch an unpainted surface on your storage enclosure chassis before handling the drive.
- Handle drives carefully:
 - Always use two hands when removing, installing, or carrying a drive.
 - Never force a drive into a shelf, and use gentle, firm pressure to completely engage the drive latch.
 - Place drives on cushioned surfaces, and never stack drives on top of each other.
 - Do not bump drives against other surfaces.
 - Before removing a drive from a shelf, unlatch the handle and wait 30 seconds for the drive to spin down.
 - Always use approved packaging when shipping drives.
- Avoid magnetic fields:
 - Keep drives away from magnetic devices.

Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry.

Replace drive in E5700 (24-drive shelf)

You can replace a drive in a 24-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O.

Before you begin

- Review drive handling requirements in [Requirements for E5700 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive (24-drive)

Prepare to replace a drive by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.

- c. Click the drive to display its context menu, and then select **View settings**.
- d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state drive (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within your storage array: From the drive's context menu, select **Turn on locator light**.

The drive's Attention LED (amber) blinks so you can identify which drive to replace.



If you are replacing a drive in a shelf that has a bezel, you must remove the bezel to see the drive LEDs.

Step 2: Remove failed drive (24-drive)

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials.

2. Press the release button on the failed drive.



- For drives in E5724 controller shelves or DE224C drive shelves, the release button is located at the top of the drive.

The cam handle on the drive springs open partially, and the drive releases from the midplane.

3. Open the cam handle, and slide out the drive slightly.
4. Wait 30 seconds.
5. Using both hands, remove the drive from the shelf.
6. Place the drive on an antistatic, cushioned surface away from magnetic fields.
7. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive (24-drive)

You install a new drive to replace the failed one. Install the replacement drive as soon as possible after removing the failed drive. Otherwise, there is a risk that the equipment might overheat.

Steps

1. Open the cam handle.
2. Using two hands, insert the replacement drive into the open bay, firmly pushing until the drive stops.
3. Slowly close the cam handle until the drive is fully seated in the midplane and the handle clicks into place.

The green LED on the drive comes on when the drive is inserted correctly.



Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement (24-drive)

Confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced.

When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.

- Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
- Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
- Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.

2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.
5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace drive in E5700 (60-drive shelf)

You can replace a drive in a 60-drive shelf.

About this task

The Recovery Guru in SANtricity System Manager monitors the drives in the storage array and can notify you of an impending drive failure or an actual drive failure. When a drive has failed, its amber Attention LED is on. You can hot-swap a failed drive while the storage array is receiving I/O operations.

This task applies to DCM and DCM2 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

- Review drive handling requirements in [Requirements for E5700 drive replacement](#).

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to replace drive (60-drive)

Prepare to replace a drive in a 60-drive shelf by checking the Recovery Guru in SANtricity System Manager and completing any prerequisite steps. Then, you can locate the failed component.

Steps

1. If the Recovery Guru in SANtricity System Manager has notified you of an *impending drive failure*, but the drive has not yet failed, follow the instructions in the Recovery Guru to fail the drive.
2. If needed, use SANtricity System Manager to confirm you have a suitable replacement drive.
 - a. Select **Hardware**.
 - b. Select the failed drive on the shelf graphic.
 - c. Click the drive to display its context menu, and then select **View settings**.
 - d. Confirm that the replacement drive has a capacity equal to or greater than the drive you are replacing and that it has the features you expect.

For example, do not attempt to replace a hard disk drive (HDD) with a solid-state disk (SSD). Similarly, if you are replacing a secure-capable drive, make sure the replacement drive is also secure-capable.

3. If needed, use SANtricity System Manager to locate the drive within the storage array.

- a. If the shelf has a bezel, remove it so you can see the LEDs.
- b. From the drive's context menu, select **Turn on locator light**.

The drive drawer's Attention LED (amber) blinks so you can open the correct drive drawer to identify which drive to replace.



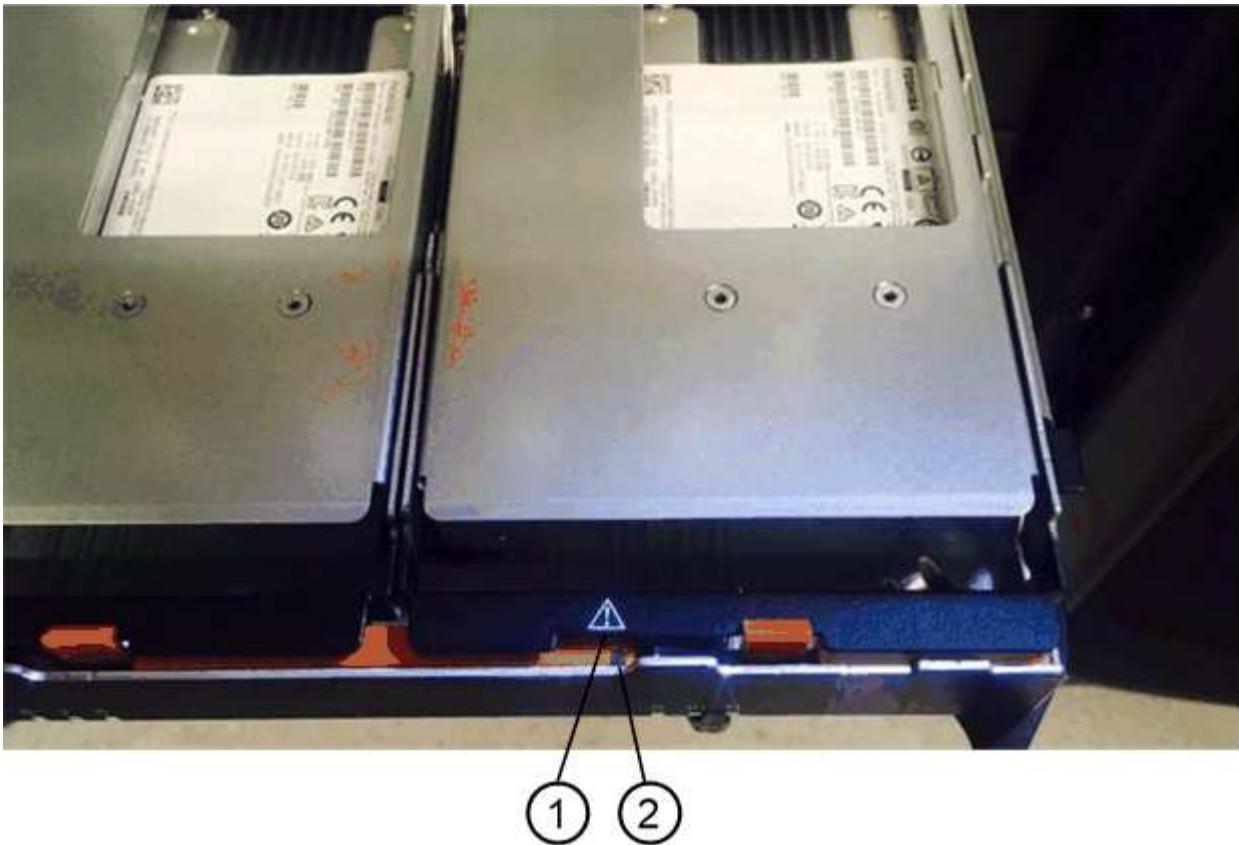
(1) Attention LED

- c. Unlatch the drive drawer by pulling on both levers.
- d. Using the extended levers, carefully pull the drive drawer out until it stops.
- e. Look at the top of the drive drawer to find the Attention LED in front of each drive.



(1) *Attention LED light on for the drive on the top right side*

The drive drawer Attention LEDs are on the left side in front of each drive, with an attention icon on the drive handle just behind the LED.



(1) Attention icon

(2) Attention LED

Step 2: Remove failed drive (60-drive)

Remove a failed drive to replace it with a new one.

Steps

1. Unpack the replacement drive, and set it on a flat, static-free surface near the shelf.

Save all packing materials for the next time you need to send a drive back.

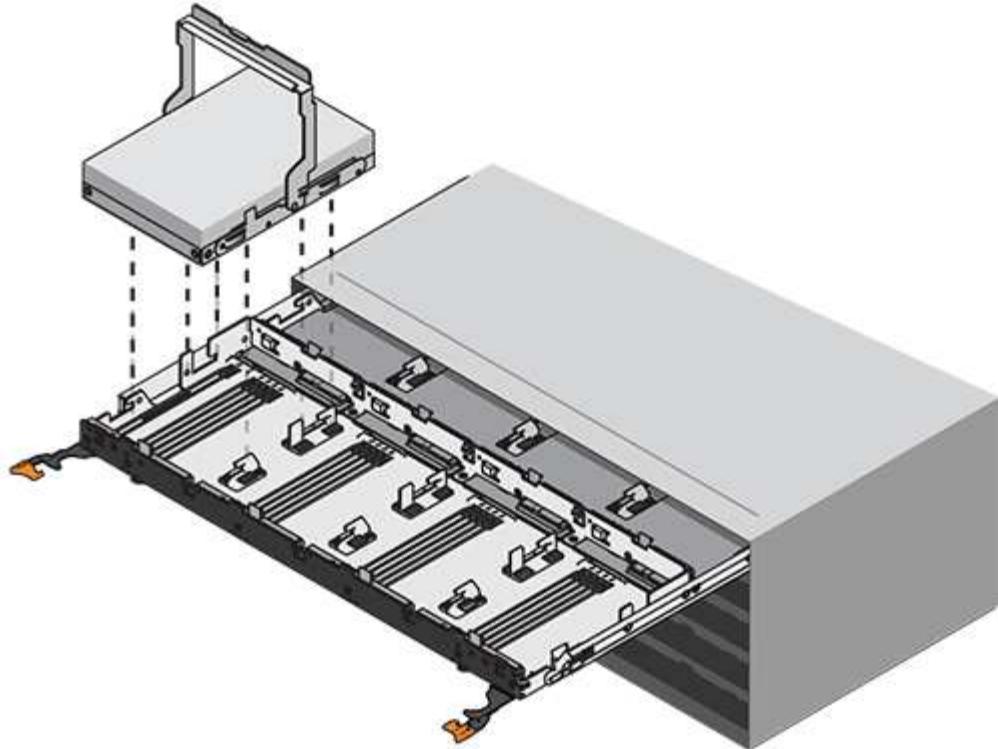
2. Release the drive drawer levers from the center of the appropriate drive drawer by pulling both towards the sides of the drawer.
3. Carefully pull on the extended drive drawer levers to pull out the drive drawer to its full extension without removing it from the enclosure.
4. Gently pull back the orange release latch that is in front of the drive you want to remove.

The cam handle on the drive springs open partially, and the drive is released from the drawer.



(1) Orange release latch

5. Open the cam handle, and lift out the drive slightly.
6. Wait 30 seconds.
7. Use the cam handle to lift the drive from the shelf.



8. Place the drive on an antistatic, cushioned surface away from magnetic fields.
9. Wait 30 seconds for the software to recognize that the drive has been removed.



If you accidentally remove an active drive, wait at least 30 seconds, and then reinstall it. For the recovery procedure, refer to the storage management software.

Step 3: Install new drive (60-drive)

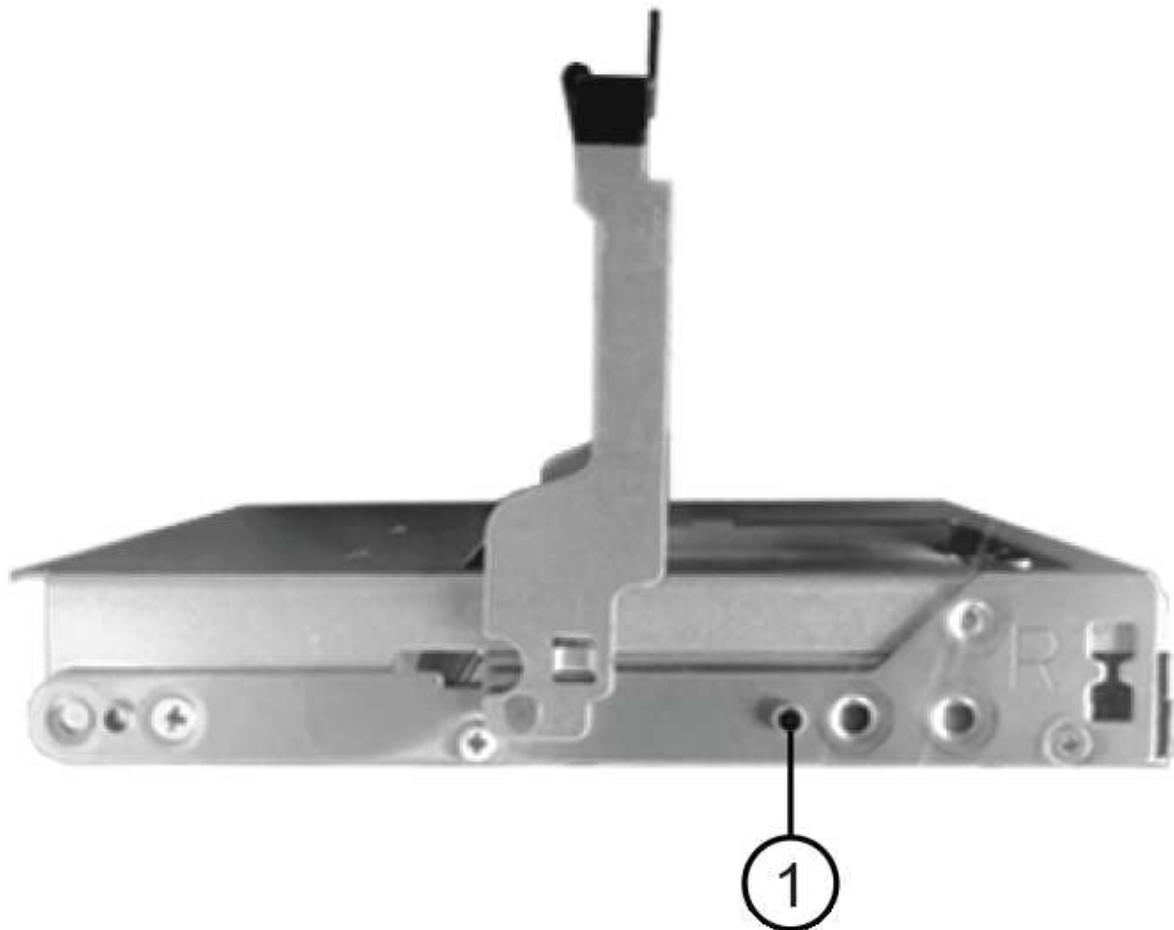
Install a new drive to replace the failed one.



Possible loss of data access — When pushing the drive drawer back into the enclosure, never slam the drawer shut. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.

Steps

1. Raise the cam handle on the new drive to vertical.
2. Align the two raised buttons on each side of the drive carrier with the matching gap in the drive channel on the drive drawer.



(1) Raised button on the right side of the drive carrier

3. Lower the drive straight down, and then rotate the cam handle down until the drive snaps into place under the orange release latch.
4. Carefully push the drive drawer back into the enclosure. Push the drawer in slowly to avoid jarring the drawer and causing damage to the storage array.
5. Close the drive drawer by pushing both levers towards the center.

The green Activity LED for the replaced drive on the front of the drive drawer comes on when the drive is inserted correctly.

Depending on your configuration, the controller might automatically reconstruct data to the new drive. If the shelf uses hot spare drives, the controller might need to perform a complete reconstruction on the hot spare before it can copy the data to the replaced drive. This reconstruction process increases the time that is required to complete this procedure.

Step 4: Complete drive replacement (60-drive)

Confirm that the new drive is working correctly.

Steps

1. Check the Power LED and the Attention LED on the drive you replaced. (When you first insert a drive, its Attention LED might be on. However, the LED should go off within a minute.)
 - Power LED is on or blinking, and the Attention LED is off: Indicates that the new drive is working correctly.
 - Power LED is off: Indicates that the drive might not be installed correctly. Remove the drive, wait 30 seconds, and then reinstall it.
 - Attention LED is on: Indicates that the new drive might be defective. Replace it with another new drive.
2. If the Recovery Guru in SANtricity System Manager still shows an issue, select **Recheck** to ensure the problem has been resolved.
3. If the Recovery Guru indicates that drive reconstruction did not start automatically, start reconstruction manually, as follows:



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

- a. Select **Hardware**.
- b. Click the drive that you replaced.
- c. From the drive's context menu, select **Reconstruct**.
- d. Confirm that you want to perform this operation.

When the drive reconstruction completes, the volume group is in an Optimal state.

4. As required, reinstall the bezel.
5. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

What's next?

Your drive replacement is complete. You can resume normal operations.

Replace E5700 drive drawer (60-drive)

You can replace a drive drawer in an E5700 array.

About this task

The steps to replace a failed drive drawer in an E5760 controller shelf or a DE460C drive shelf depend on whether the volumes in the drawer are protected by Drawer Loss Protection. If all volumes in the drive drawer are in disk pools or volume groups that have Drawer Loss Protection, you can perform this procedure online. Otherwise, you must stop all host I/O activity and power off the shelf before replacing the drive drawer.

Before you begin

- Review drive handling requirements in [Requirements for E5700 drive replacement](#).
- Make sure the drive shelf meets all of these conditions:
 - The drive shelf cannot be over temperature.
 - Both fans must be installed and have a status of Optimal.
 - All drive shelf components must be in place.
 - The volumes in the drive drawer cannot be in a Degraded state.



Possible loss of data access — If a volume is already in a Degraded state, and you remove drives from the drive drawer, the volume can fail.

What you'll need

- A replacement drive that is supported by NetApp for your controller shelf or drive shelf.
- An ESD wristband, or you have taken other antistatic precautions.
- A flashlight.
- A permanent marker to note the exact location of each drive as you remove the drive from the drawer.
- Access to the storage array's command line interface (CLI). If you do not have access to the CLI, you can do one of the following:
 - **For SANtricity System Manager (version 11.60 and above)** — Download the CLI package (zip file) from System Manager. Go to **Settings > System > Add-ons > Command Line Interface**. You can then issue CLI commands from an operating system prompt, such as the DOS C: prompt.
 - **For SANtricity Storage Manager/Enterprise Management Window (EMW)** — Follow the instructions in the express guide to download and install the software. You can run CLI commands from the EMW by selecting **Tools > Execute Script**.

Step 1: Prepare to replace drive drawer (60-drive)

Prepare to replace a drive drawer by determining if you can perform the replacement procedure while the drive shelf is online or if you need to stop host I/O activity and power off any of the shelves that are powered on. If you are replacing a drawer in a shelf with Drawer Loss Protection, there is no need to stop host I/O activity and power off any of the shelves.

Steps

1. Determine if the drive shelf is powered on.
 - If the power is off, you do not need to issue the CLI command. Go to [Step 2: Remove cable chains](#).
 - If the power is on, go to the next step.
2. Type the following command on the command line, and press **Enter**:

```
SMcli <ctrlr_IP1> -p "array_password" -c "set tray [trayID] drawer  
[drawerID]  
serviceAllowedIndicator=on;"
```

where:

- <ctrlr_IP1> is the identifier of the controller.
- array_password is the password for the storage array. You must enclose the value for array_password in double quotation marks ("").
- [trayID] is the identifier of the drive shelf that contains the drive drawer that you want to replace. Drive shelf ID values are 0 to 99. You must enclose the value for trayID in square brackets.
- [drawerID] is the identifier of the drive drawer that you want to replace. Drawer ID values are 1 (top drawer) to 5 (bottom drawer). You must enclose the value for drawerID in square brackets. This command ensures you can remove the top-most drawer in drive shelf 10:

```
SMcli <ctrlr_IP1> -p "safety-1" -c "set tray [10] drawer [1]  
serviceAllowedIndicator=forceOnWarning;"
```

3. Determine if you need to stop host I/O activity, as follows:

- If the command succeeds, you do not need to stop host I/O activity. All drives in the drawer are in pools or volume groups with Drawer Loss Protection. Go to [Step 2: Remove cable chains](#).



Possible damage to drives — Wait 30 seconds after the command completes before you open the drive drawer. Waiting 30 seconds allows the drives to spin down, which prevents possible damage to the hardware.

- If a warning is displayed indicating that this command could not be completed, you must stop host I/O activity before removing the drawer. The warning is displayed because one or more drives in the affected drawer are in pools or volume groups without Drawer Loss Protection. To avoid losing data, you must complete the next steps to stop host I/O activity and to power off the drive shelf and the controller shelf.

4. 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.



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.

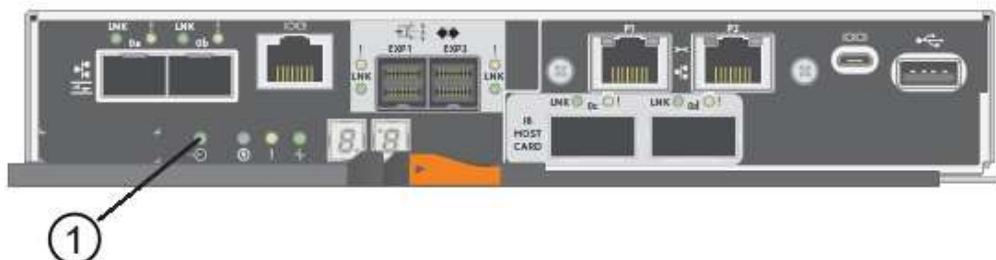
5. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose data because the storage array will not be accessible.

6. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**.
8. Wait for all operations to complete before continuing with the next step.
9. Power off the shelves as follows:

- *If you are replacing a drawer in a shelf **with** Drawer Loss Protection:*

There is NO need to power off any of the shelves.

You can perform the replace procedure while the drive drawer is online, because the Set Drawer Service Action Allowed Indicator CLI command completed successfully.

- *If you are replacing a drawer in a **controller** shelf **without** Drawer Loss Protection:*

- a. Turn off both power switches on the controller shelf.
- b. Wait for all LEDs on the controller shelf to go dark.

- *If you are replacing a drawer in an **expansion** drive shelf **without** Drawer Loss Protection:*

- a. Turn off both power switches on the controller shelf.
- b. Wait for all LEDs on the controller shelf to go dark.
- c. Turn off both power switches on the drive shelf.
- d. Wait two minutes for drive activity to stop.

Step 2: Remove cable chains

Remove both cable chains so you can remove and replace a failed drive drawer. The left and right cable chains allow the drawers to slide in and out.

About this task

Each drive drawer has left and right cable chains. The metal ends on the cable chains slide into corresponding vertical and horizontal guide rails inside the enclosure, as follows:

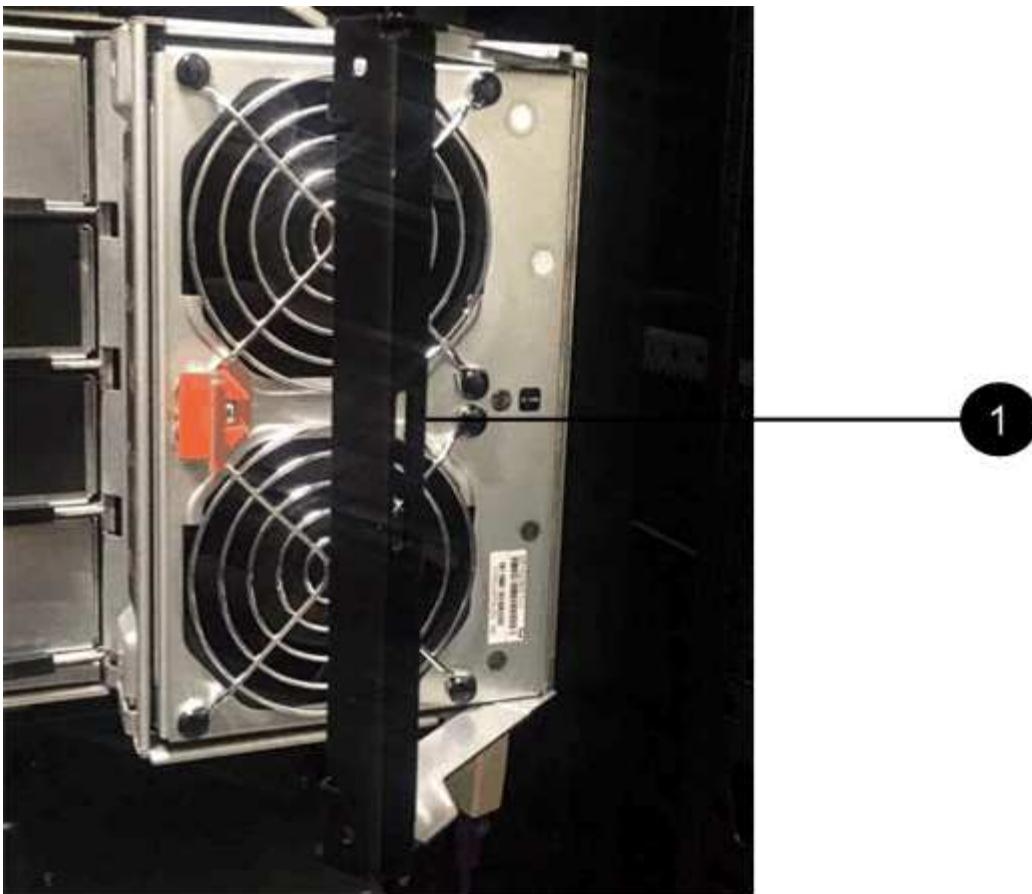
- The left and right vertical guide rails connect the cable chain to the enclosure's midplane.
- The left and right horizontal guide rails connect the cable chain to the individual drawer.

 **Possible hardware damage** — If the drive tray is powered on, the cable chain is energized until both ends are unplugged. To avoid shorting out the equipment, do not allow the unplugged cable chain connector to touch the metal chassis if the other end of the cable chain is still plugged in.

Steps

1. Make sure host I/O activity has stopped and the drive shelf or controller shelf is powered off, or issue the Set Drawer Attention Indicator CLI command.
2. From the rear of the drive shelf, remove the right fan canister:
 - a. Press the orange tab to release the fan canister handle.

The figure shows the handle for the fan canister extended and released from the orange tab on the left.



(1) Fan canister handle

- b. Using the handle, pull the fan canister out of the drive tray, and set it aside.
- c. If the tray is powered on, ensure that the left fan goes to its maximum speed.



Possible equipment damage due to overheating — If the tray is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

3. Determine which cable chain to disconnect:

- If the power is on, the amber Attention LED on the front of the drawer indicates the cable chain you need to disconnect.
- If the power is off, you must manually determine which of the five cable chains to disconnect.
The figure shows the right side of the drive shelf with the fan canister removed. With the fan canister removed, you can see the five cable chains and the vertical and horizontal connectors for each drawer.

The top cable chain is attached to drive drawer 1. The bottom cable chain is attached to drive drawer 5. The callouts for drive drawer 1 are provided.



(1) Vertical connector (connected to midplane)

(2) Cable chain

(3) Horizontal connector (connected to drawer)

4. For easy access, use your finger to move the cable chain on the right side to the left.
5. Disconnect any of the right cable chains from their corresponding vertical guide rail.
 - a. Using a flashlight, locate the orange ring on the end of the cable chain that is connected to the vertical guide rail in the enclosure.



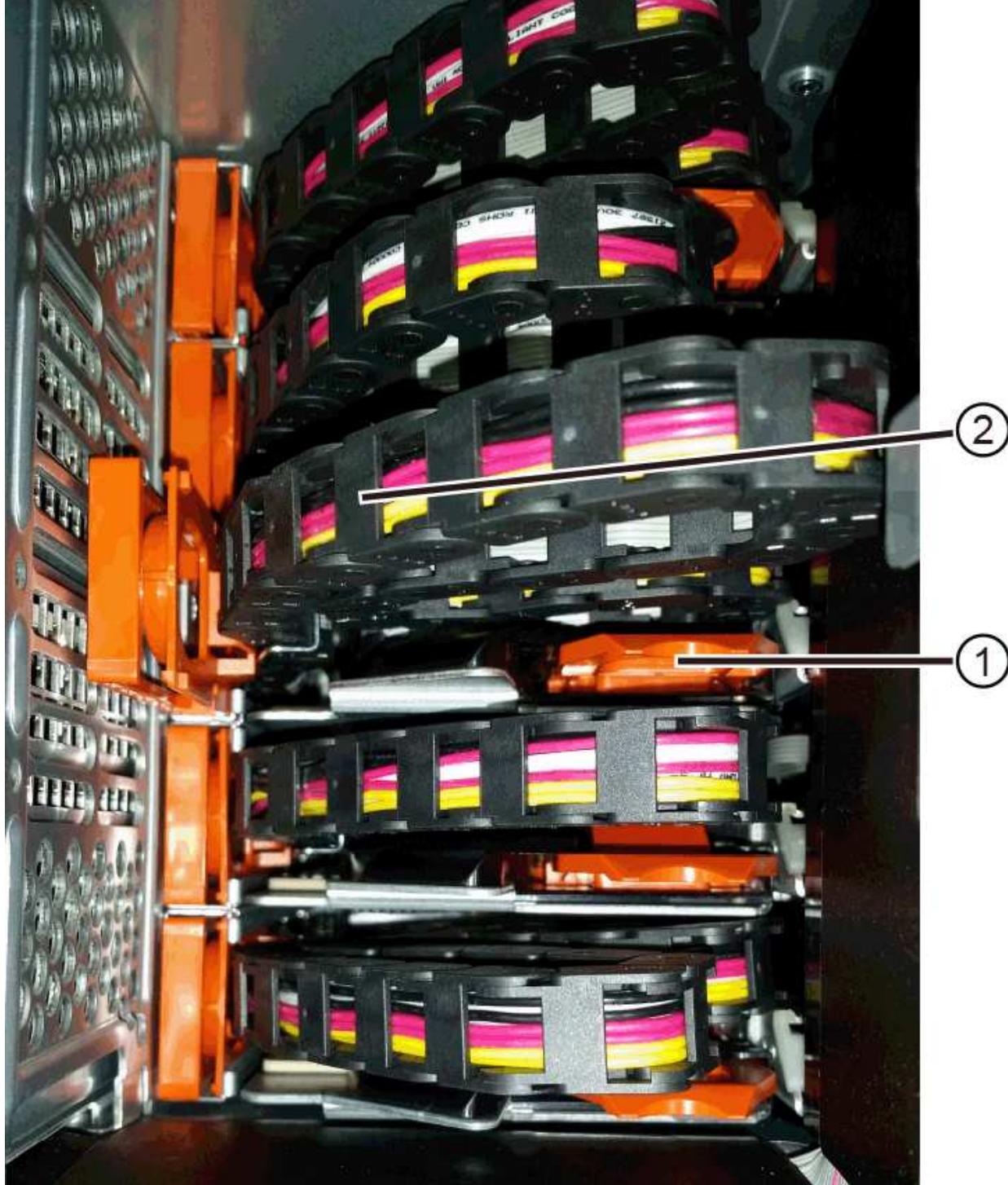
(1) Orange ring on vertical guide rail

(2) Cable chain, partially removed

- b. To unlatch the cable chain, insert your finger into the orange ring and press towards the middle of the system.

- c. To unplug the cable chain, carefully pull your finger toward you approximately 1 inch (2.5 cm). Leave the cable chain connector within the vertical guide rail. (If the drive tray is powered on, do not allow the cable chain connector to touch the metal chassis.)
6. Disconnect the other end of the cable chain:
 - a. Using a flashlight, locate the orange ring on the end of the cable chain that is attached to the horizontal guide rail in the enclosure.

The figure shows the horizontal connector on the right and the cable chain disconnected and partially pulled out on the left side.



(1) Orange ring on horizontal guide rail

(2) Cable chain, partially removed

- b. To unlatch the cable chain, gently insert your finger into the orange ring and push down.

The figure shows the orange ring on the horizontal guide rail (see item 1 in the figure above), as it is pushed down so that the rest of the cable chain can be pulled out of the enclosure.

- c. Pull your finger toward you to unplug the cable chain.

7. Carefully pull the entire cable chain out of the drive shelf.

8. Replace the right fan canister:

- a. Slide the fan canister all the way into the shelf.

- b. Move the fan canister handle until it latches with the orange tab.

- c. If the drive shelf is receiving power, confirm that the amber Attention LED on the back of the fan is not illuminated and that air is coming out the back of the fan.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the correct speed.

If the power is off, the fans do not run and the LED is not on.

9. From the back of the drive shelf, remove the left fan canister.

10. If the drive shelf is receiving power, ensure that the right fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

11. Disconnect the left cable chain from its vertical guide rail:

- a. Using a flashlight, locate the orange ring on the end of the cable chain attached to the vertical guide rail.
- b. To unlatch the cable chain, insert your finger into the orange ring.
- c. To unplug the cable chain, pull toward you approximately 1 inch (2.5 cm). Leave the cable chain connector within the vertical guide rail.



Possible hardware damage — If the drive tray is powered on, the cable chain is energized until both ends are unplugged. To avoid shorting out the equipment, do not allow the unplugged cable chain connector to touch the metal chassis if the other end of the cable chain is still plugged in.

12. Disconnect the left cable chain from the horizontal guide rail, and pull the entire cable chain out of the drive shelf.

If you are performing this procedure with the power on, all LEDs turn off when you disconnect the last cable chain connector, including the amber Attention LED.

13. Replace the left fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is not illuminated and that air is coming out the back of the fan.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the

correct speed.

Step 3: Remove failed drive drawer (60-drive)

Remove a failed drive drawer to replace it with a new one.



Possible loss of data access — Magnetic fields can destroy all data on the drive and cause irreparable damage to the drive circuitry. To avoid loss of data access and damage to the drives, always keep drives away from magnetic devices.

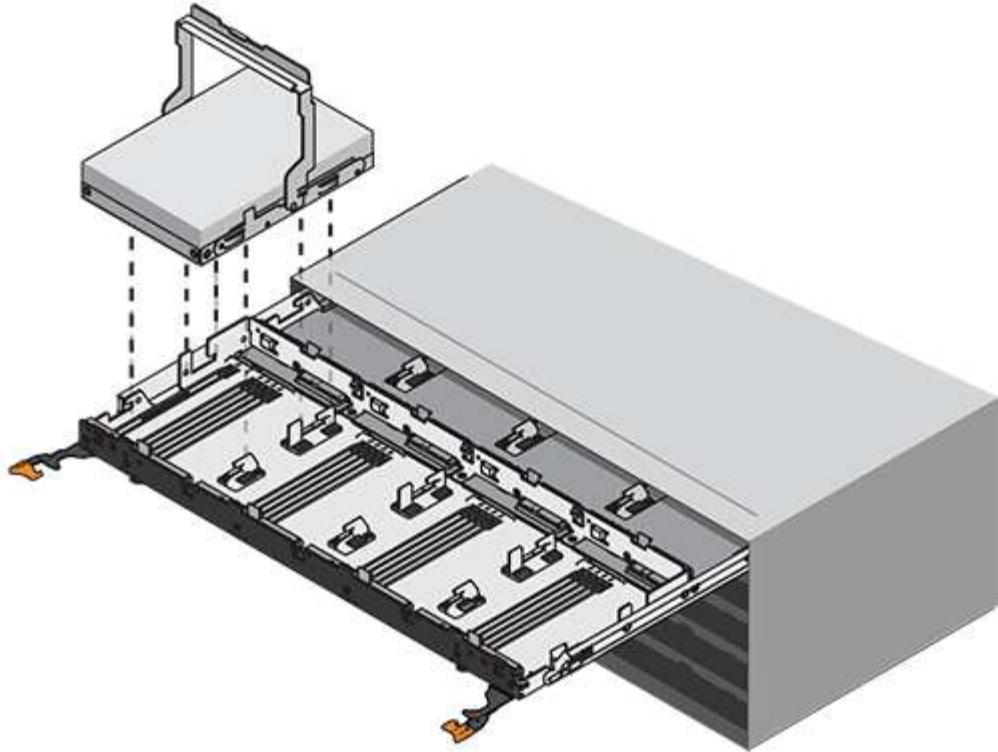
Steps

1. Make sure that:
 - The right and left cable chains are removed from the drive drawer.
 - The right and left fan canisters are replaced.
2. Remove the bezel from the front of the drive shelf.
3. Unlatch the drive drawer by pulling out on both levers.
4. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
5. If volumes have already been created and assigned, use a permanent marker to note the exact location of each drive. For example, using the following drawing as a reference, write the appropriate slot number on the top of each drive.

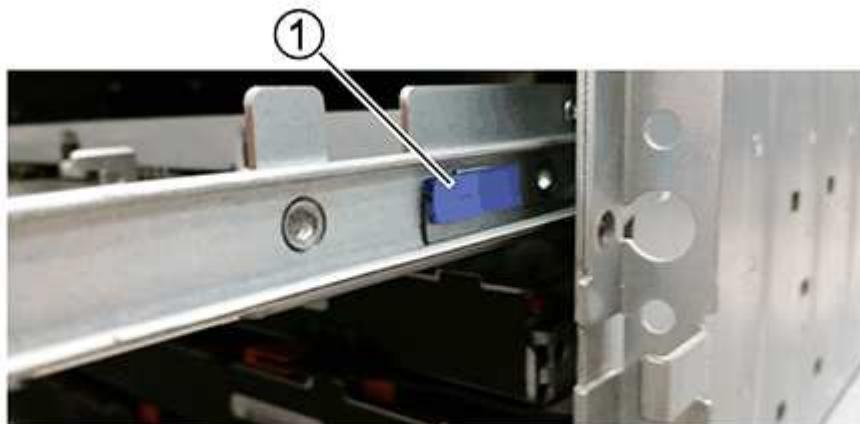


Possible loss of data access — Make sure to record the exact location of each drive before removing it.

6. Remove the drives from the drive drawer:
 - a. Gently pull back the orange release latch that is visible on the center front of each drive.
 - b. Raise the drive handle to vertical.
 - c. Use the handle to lift the drive from the drive drawer.



- d. Place the drive on a flat, static-free surface and away from magnetic devices.
- 7. Remove the drive drawer:
 - a. Locate the plastic release lever on each side of the drive drawer.



(1) Drive drawer release lever

- b. Disengage both release levers by pulling the latches toward you.
- c. While holding both release levers, pull the drive drawer toward you.
- d. Remove the drive drawer from the drive shelf.

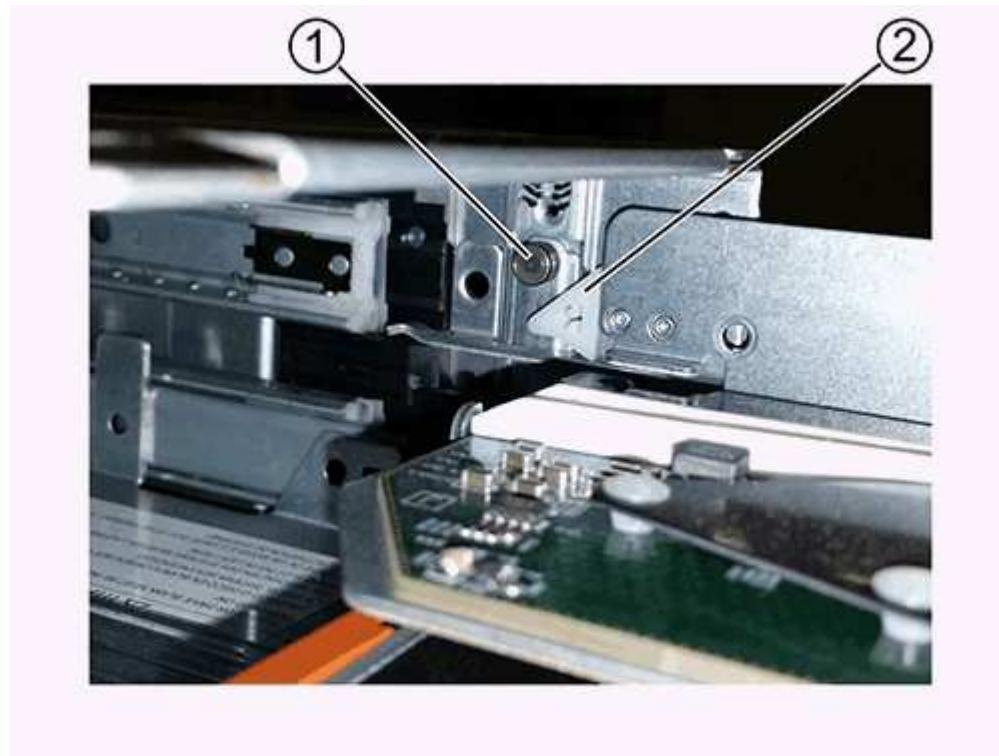
Step 4: Install new drive drawer (60-drive)

Install a new drive drawer to replace the failed one.

Steps

1. Determine a location to install each drive.
2. From the front of the drive shelf, shine a flashlight into the empty drawer slot, and locate the lock-out tumbler for that slot.

The lock-out tumbler assembly is a safety feature that prevents you from being able to open more than one drive drawer at one time.



(1) Lock-out tumbler

(2) Drawer guide

3. Position the replacement drive drawer in front of the empty slot and slightly to the right of center.

Positioning the drawer slightly to the right of center helps to ensure that the lock-out tumbler and the drawer guide are correctly engaged.

4. Slide the drive drawer into the slot, and ensure that the drawer guide slides under the lock-out tumbler.



Risk of equipment damage — Damage occurs if the drawer guide does not slide under the lock-out tumbler.

5. Carefully push the drive drawer all the way in until the latch fully engages.

Experiencing a higher level of resistance is normal when pushing the drawer closed for the first time.



Risk of equipment damage — Stop pushing the drive drawer if you feel binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, reinsert the drawer into the slot, ensure the tumbler is above the rail, and the rails are aligned correctly.

Step 5: Attach cable chains

Attach the cable chains so you can safely re-install the drives in the drive drawer.

When attaching a cable chain, reverse the order you used when disconnecting the cable chain. You must insert the chain's horizontal connector into the horizontal guide rail in the enclosure before inserting the chain's vertical connector into the vertical guide rail in the enclosure.

Steps

1. Make sure that:

- You completed the step to install the new drive drawer.
- You have two replacement cable chains, marked as LEFT and RIGHT (on the horizontal connector next to the drive drawer).

2. From the back of the drive shelf, remove the fan canister on the right side, and set it aside.

3. If the shelf is powered on, ensure that the left fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

4. Attach the right cable chain:

- a. Locate the horizontal and vertical connectors on the right cable chain and the corresponding horizontal guide rail and vertical guide rail inside the enclosure.
- b. Align both cable chain connectors with their corresponding guide rails.
- c. Slide the cable chain's horizontal connector onto the horizontal guide rail, and push it in as far as it can go.



Risk of equipment malfunction — Make sure to slide the connector into the guide rail. If the connector rests on the top of the guide rail, problems might occur when the system runs.

The figure shows the horizontal and vertical guide rails for the second drive drawer in the enclosure.



(1) Horizontal guide rail

(2) Vertical guide rail

- d. Slide the vertical connector on the right cable chain into the vertical guide rail.
- e. After you have reconnected both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.



Risk of equipment malfunction — If the connectors are not latched, the cable chain might come loose during drawer operation.

5. Reinstall the right fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is now off and that air is now coming out of the back.

The LED could remain on for as long as a minute after you reinstall the fan while the fan settles into the correct speed.

6. From the back of the drive shelf, remove the fan canister on the left side of the shelf.
7. If the shelf is powered on, ensure that the right fan goes to its maximum speed.



Possible equipment damage due to overheating — If the shelf is powered on, do not remove both fans at the same time. Otherwise, the equipment might overheat.

8. Reattach the left cable chain:

- a. Locate the horizontal and vertical connectors on the cable chain and their corresponding horizontal and vertical guide rails inside the enclosure.
- b. Align both cable chain connectors with their corresponding guide rails.
- c. Slide the cable chain's horizontal connector into the horizontal guide rail and push it in as far as it will go.



Risk of equipment malfunction — Make sure to slide the connector within the guide rail. If the connector rests on the top of the guide rail, problems might occur when the system runs.

- d. Slide the vertical connector on the left cable chain into the vertical guide rail.
- e. After you reconnect both ends of the cable chain, carefully pull on the cable chain to verify that both connectors are latched.



Risk of equipment malfunction — If the connectors are not latched, the cable chain might come loose during drawer operation.

9. Reinstall the left fan canister. If the drive shelf is receiving power, confirm that the amber LED on the back of the fan is now off and that air is now coming out of the back.

The LED could remain on for as long as a minute after you reinstall the fan while both fans settle into the correct speed.

Step 6: Complete drive drawer replacement (60-drive)

Complete the drive drawer replacement by reinserting the drives and replacing the front bezel in the correct order.



Possible loss of data access — You must install each drive in its original location in the drive drawer.

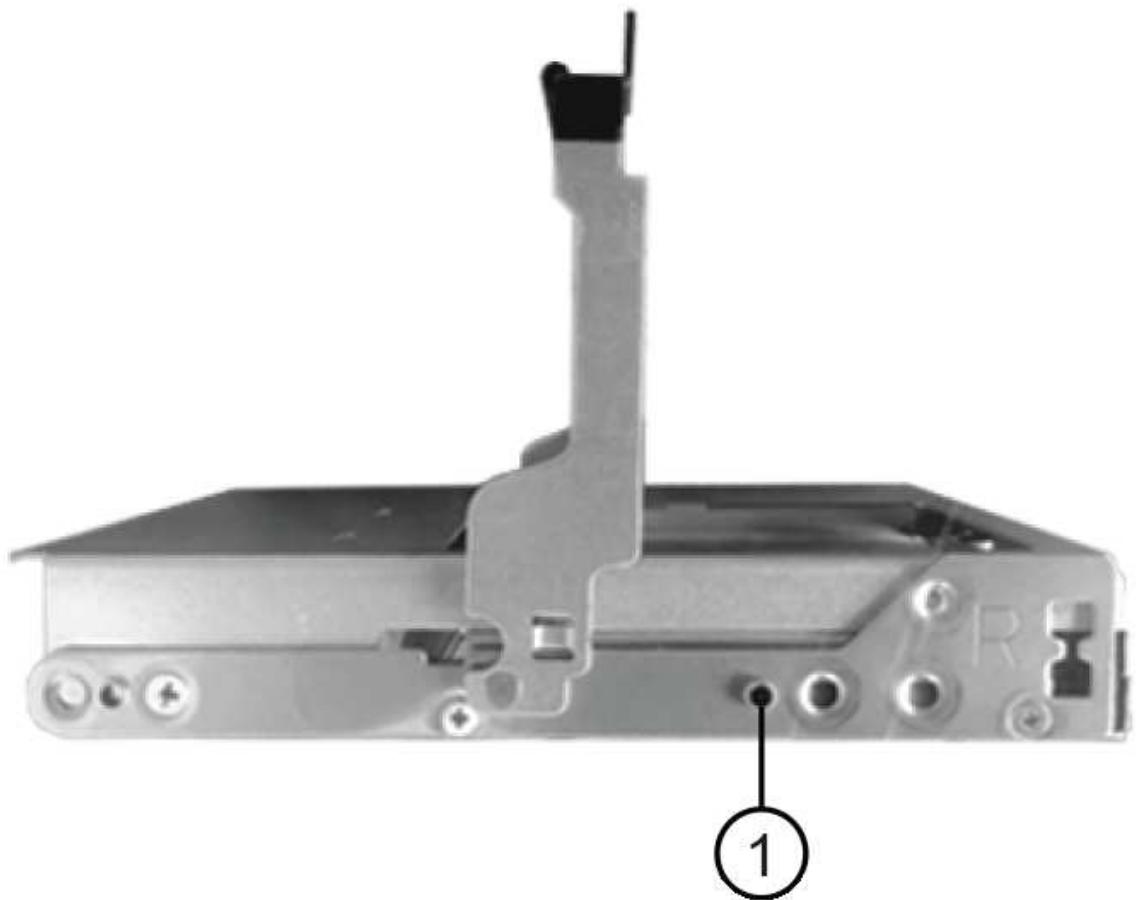
Steps

1. Reinstall the drives in the drive drawer:
 - a. Unlatch the drive drawer by pulling out on both levers at the front of the drawer.
 - b. Using the extended levers, carefully pull the drive drawer out until it stops. Do not completely remove the drive drawer from the drive shelf.
 - c. Determine which drive to install in each slot by using the notes you made when removing the drives.



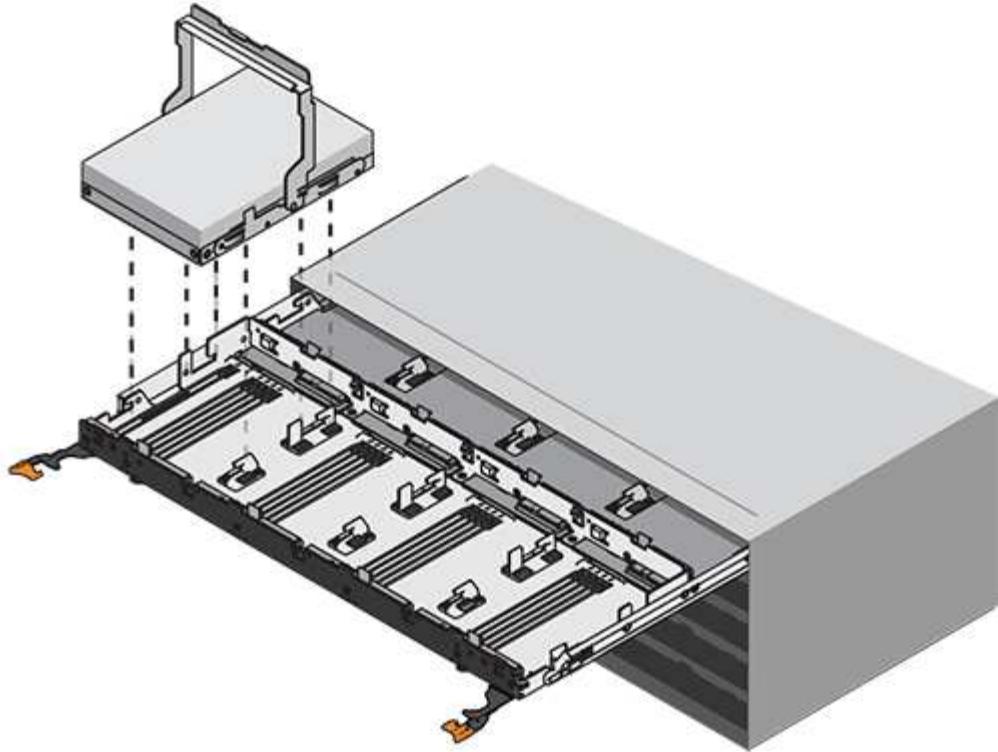
- d. Raise the handle on the drive to vertical.
- e. Align the two raised buttons on each side of the drive with the notches on the drawer.

The figure shows the right-side view of a drive, showing the location of the raised buttons.



(1) Raised button on the right side of the drive

- f. Lower the drive straight down, making sure the drive is pressed all the way down into the bay, and then rotate the drive handle down until the drive snaps into place.



- g. Repeat these steps to install all the drives.
2. Slide the drawer back into the drive shelf by pushing it from the center and closing both levers.



Risk of equipment malfunction — Make sure to completely close the drive drawer by pushing both levers. You must completely close the drive drawer to allow proper airflow and prevent overheating.

3. Attach the bezel to the front of the drive shelf.
4. If you have powered down one or more shelves, reapply power:
 - **If you replaced a drive drawer in a controller shelf without Drawer Loss Protection:**
 - a. Turn on both power switches on the controller shelf.
 - b. Wait 10 minutes for the power-on process to complete.
 - c. Confirm that both fans come on and that the amber LED on the back of the fans is off.
 - **If you replaced a drive drawer in an expansion drive shelf without Drawer Loss Protection:**
 - a. Turn on both power switches on the drive shelf.
 - b. Confirm that both fans come on and that the amber LED on the back of the fans is off.
 - c. Wait two minutes before applying power to the controller shelf.
 - d. Turn on both power switches on the controller shelf.
 - e. Wait 10 minutes for the power-on process to complete.
 - f. Confirm that both fans come on and that the amber LED on the back of the fans is off.

What's next?

Your drive drawer replacement is complete. You can resume normal operations.

Host interface cards

Requirements for E5700 HIC replacement

Before you add, upgrade, or replace a host interface card (HIC) in an E5700, review the requirements and considerations.

Procedure overview

You can add, upgrade, or replace a HIC in the E5724 controller shelf and the E5760 controller shelf.

The following is an overview of the steps to replace a HIC in an E5700 controllers (E5724 or E5760):

1. Take the controller offline
2. Remove the controller canister
3. Replace the battery
4. Replace the controller canister
5. Bring the controller online

Requirements for adding, upgrading or replacing a HIC

If you plan to add, upgrade, or replace a host interface card (HIC), keep the following requirements in mind.

- You must schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)
- You must have two HICs that are compatible with your controllers.

For duplex configurations (two controllers), the HICs installed in the two controller canisters must be identical. The presence of mismatched HICs causes the controller with the replacement HIC to lock down when you bring it online.

- You have all cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- You have an ESD wristband, or you have taken other antistatic precautions.
- You have a #1 Phillips screwdriver.
- You have labels to identify each cable that is connected to the controller canister.
- You have a management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Add E5700 host interface card (HIC)

You can add a host interface card (HIC) to E5700 controller canisters with baseboard host ports. This addition increases the number of host ports in your storage array and

provides additional host protocols.

About this task

When you add HICs, you must power off the storage array, install the HIC, and reapply power.

Before you begin

- Review [Requirements for E5700 HIC replacement](#).
- Schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, both controllers must have the same HIC configuration when they are powered on.)

What you'll need

- One or two HICs, based on whether you have one or two controllers in your storage array. The HICs must be compatible with your controllers.
- New host hardware installed for the new host ports, such as switches or host bus adapters (HBAs).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) and the [NetApp Hardware Universe](#).

- Labels to identify each cable that is connected to the controller canister.
- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to add HIC

Prepare to add a HIC by backing up the storage array's configuration database, collecting support data, and stopping host I/O operations. Then, you can power down the controller shelf.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-**

<arrayName>-<dateTime>.7z

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- Select **Support > Support Center > Diagnostics**.
- Select **Collect Support Data**.
- Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. 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.



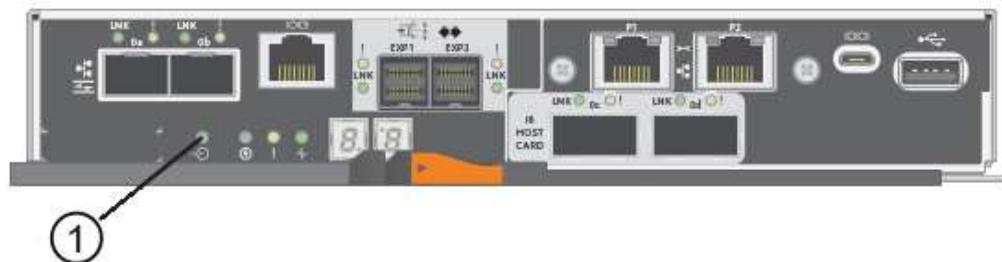
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose access to the data because the storage is not accessible.

- If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
- Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
8. Power down the controller shelf.
 - a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can add the new HIC.

Steps

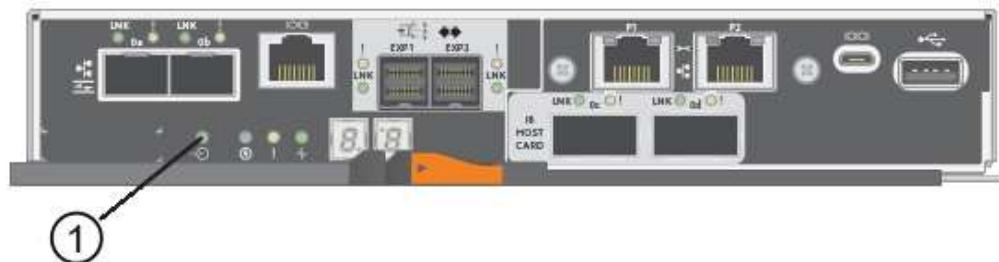
1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



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

3. Confirm that the Cache Active LED on the back of the controller is off.

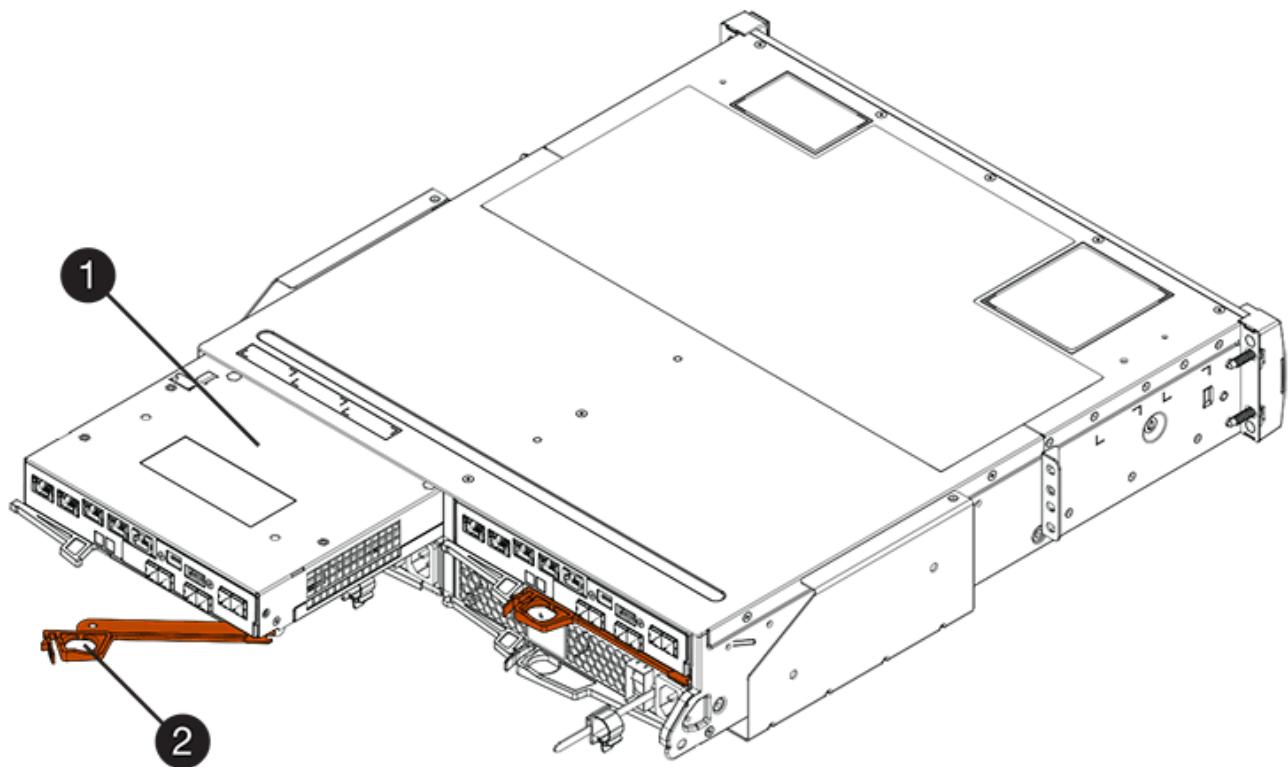
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

4. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

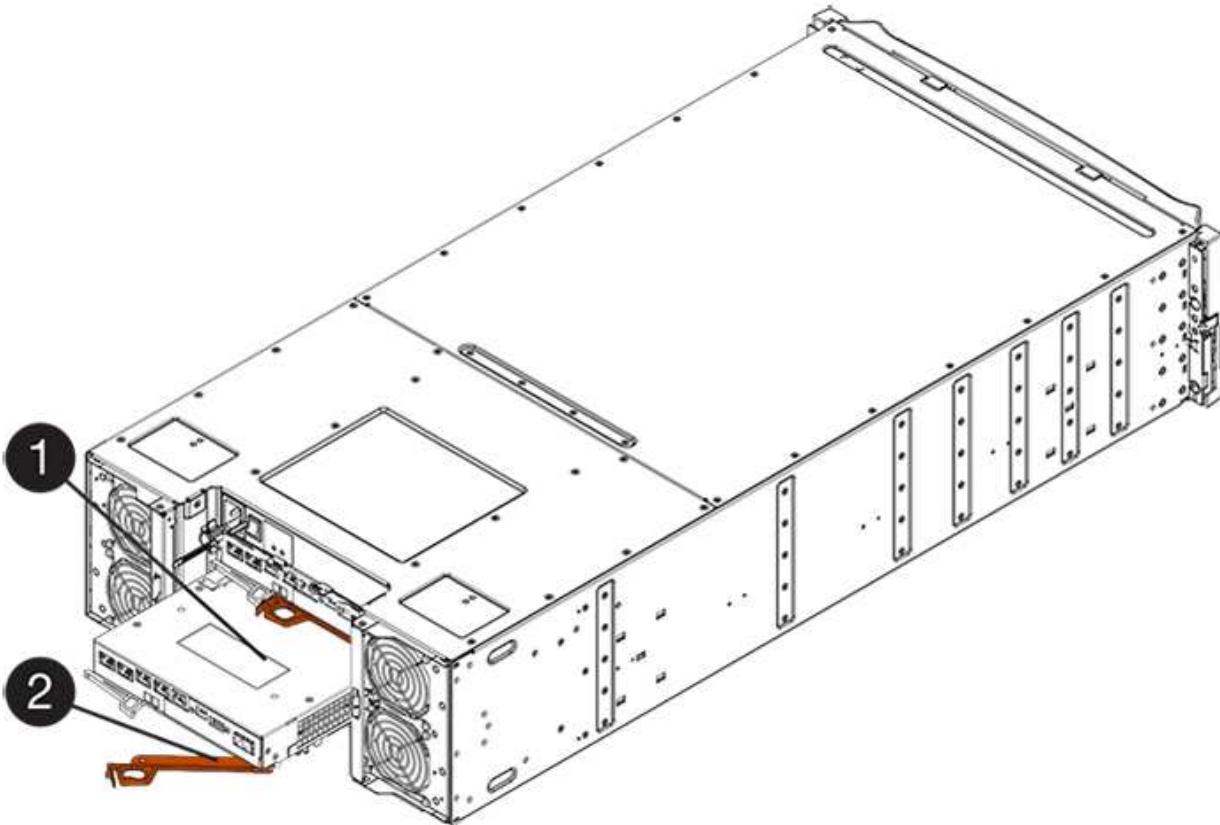
The following figure is an example of an E5724 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

The following figure is an example of an E5760 controller shelf:



(1) Controller canister

(2) Cam handle

5. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E5724 controller shelf, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

6. Turn the controller canister over, so that the removable cover faces up.
7. Place the controller canister on a flat, static-free surface.

Step 3: Install a HIC

Install the host interface card (HIC) to increase the number of host ports in your storage array.



Possible loss of data access — Never install a HIC in an E5700 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs will cause the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Press the button on the cover of the controller canister, and slide the cover off.
3. Confirm that the green LED inside the controller (by the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active

(2) Battery

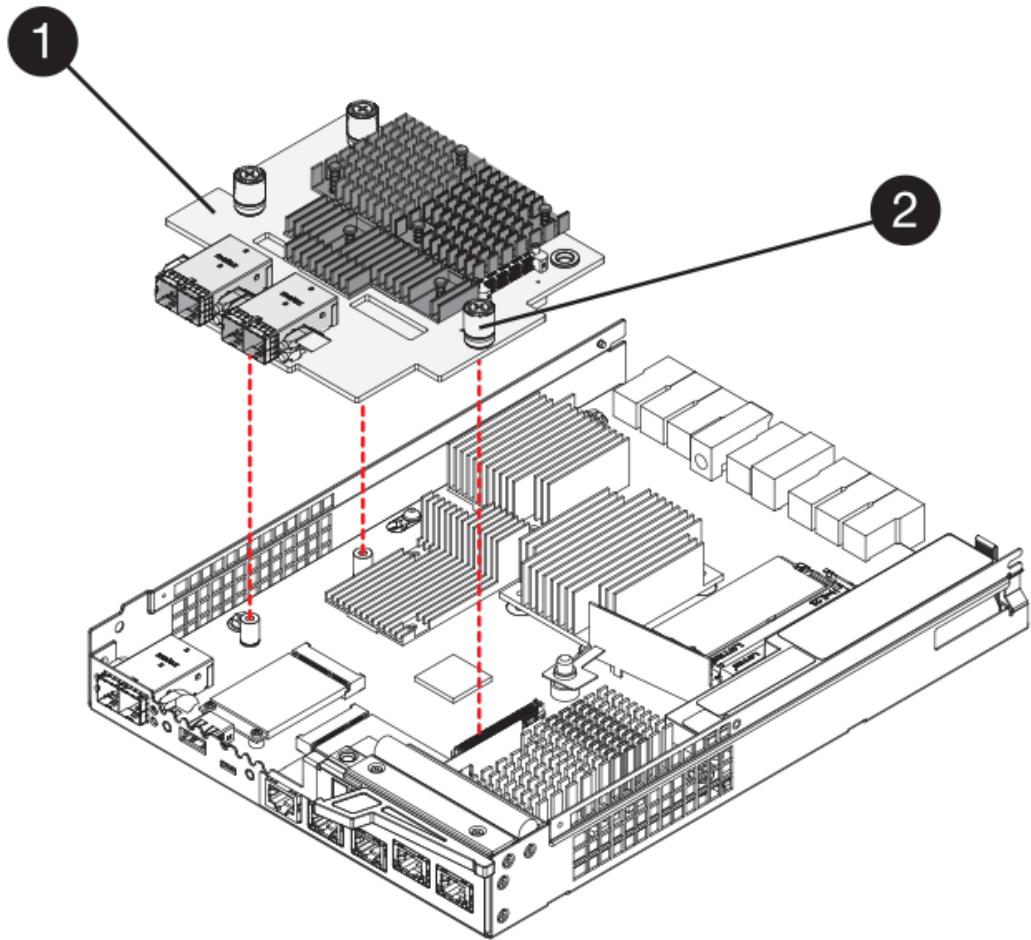
4. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the controller canister, and remove the faceplate.
5. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

6. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



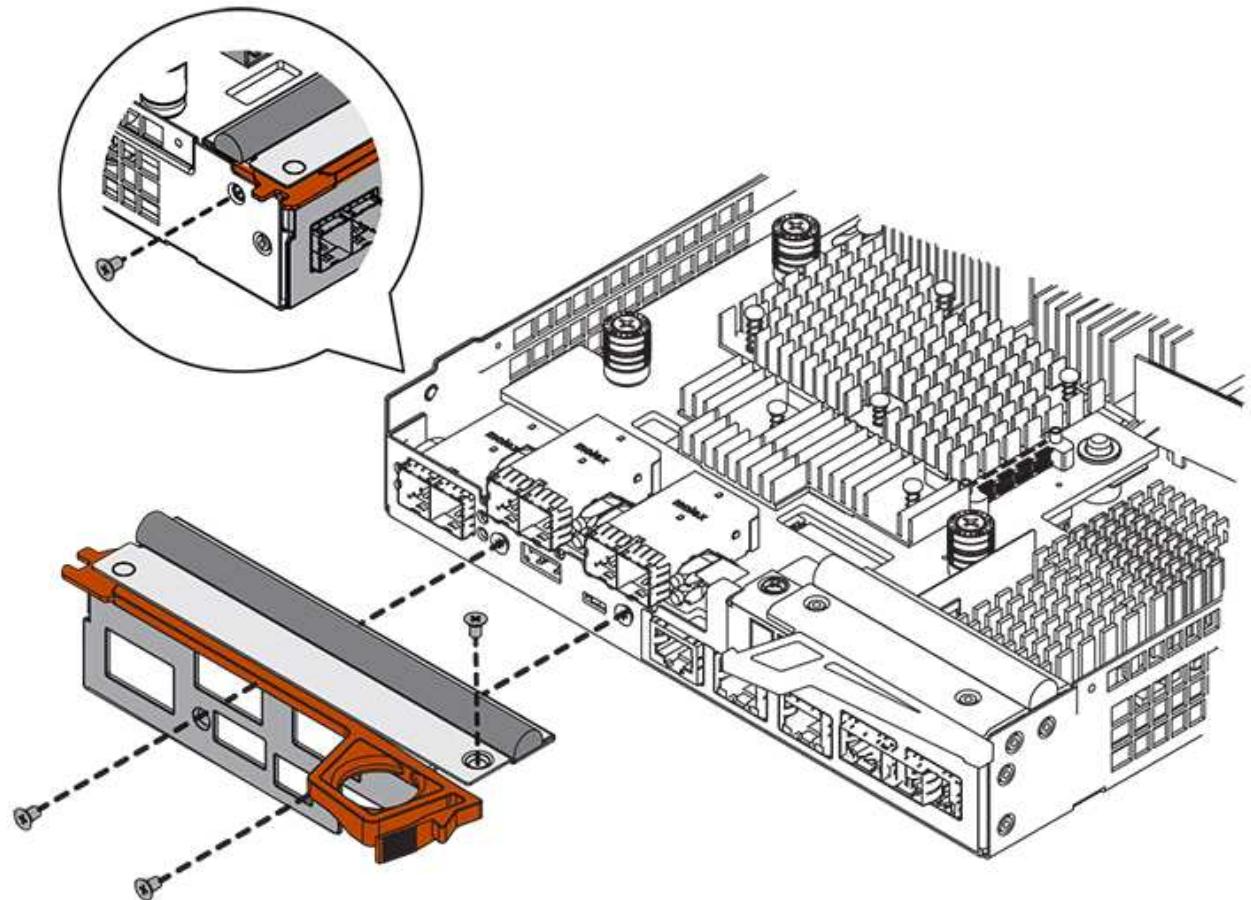
(1) Host interface card (HIC)

(2) Thumbscrews

7. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over tighten the screws.

8. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.



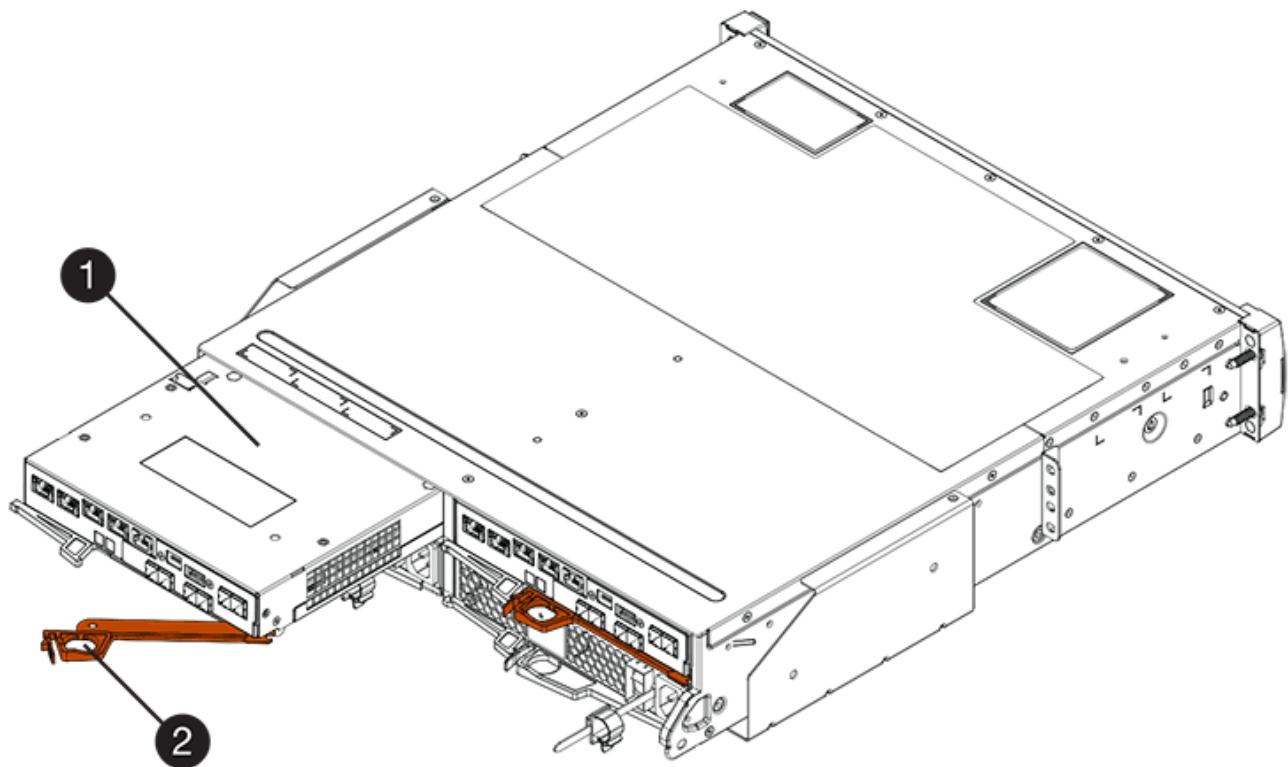
Step 4: Reinstall controller canister

Reinstall the controller canister into the controller shelf after installing the new HIC.

Steps

1. Turn the controller canister over, so that the removable cover faces down.
2. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

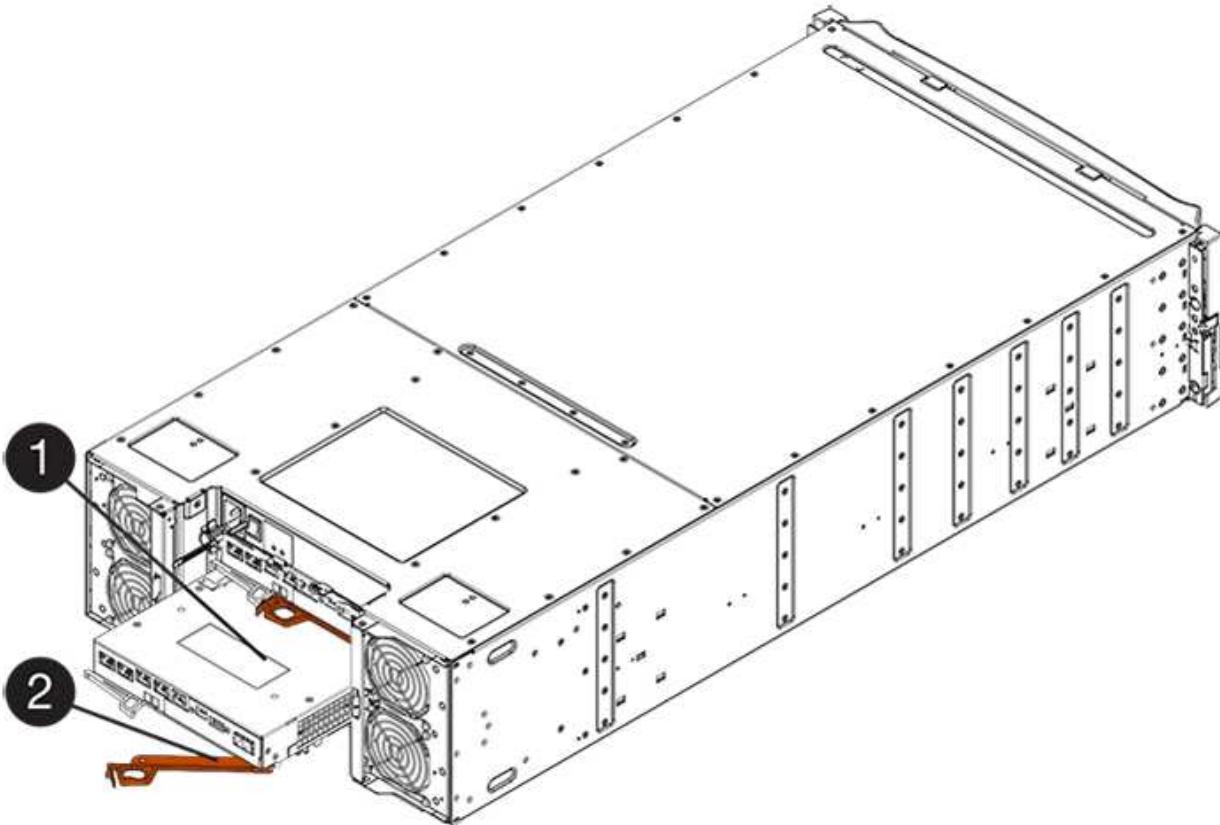
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) Controller canister

(2) Cam handle

3. Move the cam handle to the left to lock the controller canister in place.
4. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

5. (Optional) If you are adding HICs to a duplex configuration, repeat all steps to remove the second controller canister, install the second HIC, and reinstall the second controller canister.

Step 5: Complete HIC addition

Check the controller LEDs and seven-segment display, and then confirm that the controller's status is Optimal.

Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS, Sd, blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
 - The amber Attention LED on the controller turns on and then turns off, unless there is an error.

- The green Host Link LEDs remain off until you connect the host cables.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Host Link LEDs

(2) Attention LED (Amber)

(3) Seven-segment display

- From SANtricity System Manager, confirm that the controller's status is Optimal.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

- If the new HIC ports require SFP+ transceivers, install these SFPs.
- If you installed a HIC with SFP+ (optical) ports, confirm the new ports have the host protocol you expect.
 - From SANtricity System Manager, select **Hardware**.
 - If the graphic shows the drives, click **Show back of shelf**.
 - Select the graphic for either Controller A or Controller B.
 - Select **View settings** from the context menu.
 - Select the **Host Interfaces** tab.
 - Click **Show more settings**.
- Review the details shown for the HIC ports (the ports labelled **e0x** or **0x** in HIC Location **slot 1**) to determine if you are ready to connect the host ports to the data hosts:
 - If the new HIC ports have the protocol you expect:*

You are ready to connect the new HIC ports to the data hosts; go to the next step.

- If the new HIC ports do **not** have the protocol you expect:*

You must apply a software feature pack before you can connect the new HIC ports to the data hosts. See [Change E5700 host protocol](#). Then, connect the host ports to the data hosts and

resume operations.

6. Connect the cables from the controller's host ports to the data hosts.

If you need instructions for configuring and using a new host protocol, refer to the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#).

What's next?

The process of adding a host interface card to your storage array is complete. You can resume normal operations.

Upgrade E5700 host interface card (HIC)

You can upgrade a host interface card (HIC) in an E5700 array to increase the number of host ports or to change host protocols.

About this task

When you upgrade the HICs, you must power off the storage array, remove the existing HIC from each controller, install a new HIC, and reapply power.

Before you begin

- Review [Requirements for E5700 HIC replacement](#).
- Schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, this is because both controllers must have the same HIC configuration when they are powered on.)

What you'll need

- One or two HICs, based on whether you have one or two controllers in your storage array. The HICs must be compatible with your controllers.
- New host hardware installed for the new host ports, such as switches or host bus adapters (HBAs).
- All cables, transceivers, switches, and host bus adapters (HBAs) needed to connect the new host ports.

For information about compatible hardware, refer to the [NetApp Interoperability Matrix](#) or the [NetApp Hardware Universe](#).

- Labels to identify each cable that is connected to the controller canister.
- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Prepare to upgrade HICs

Prepare to upgrade a HIC by backing up the storage array's configuration database, collecting support data, and stopping host I/O operations. Then, you can power down the controller shelf.

Steps

1. From the Home page of SANtricity System Manager, ensure that the storage array has Optimal status.

If the status is not Optimal, use the Recovery Guru or contact technical support to resolve the problem. Do not continue with this procedure.

2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. 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.



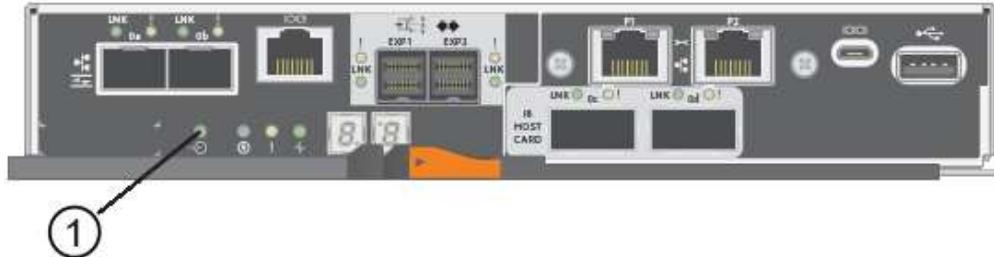
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose access to the data because the storage is not accessible.

5. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
6. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



(1) Cache Active LED

7. From the Home page of SANtricity System Manager, select **View Operations in Progress**. Wait for all operations to complete before continuing with the next step.
8. Power down the controller shelf.
 - a. Turn off both power switches on the controller shelf.
 - b. Wait for all LEDs on the controller shelf to turn off.

Step 2: Remove controller canister

Remove the controller canister so you can upgrade the new HIC.

Steps

1. Label each cable that is attached to the controller canister.
2. Disconnect all the cables from the controller canister.



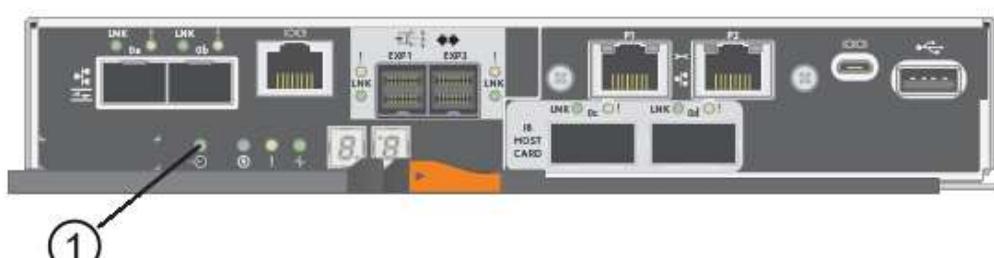
To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

3. If the HIC ports use SFP+ transceivers, remove them.

Depending on what type of HIC you are upgrading to, you might be able to reuse these SFPs.

4. Confirm that the Cache Active LED on the back of the controller is off.

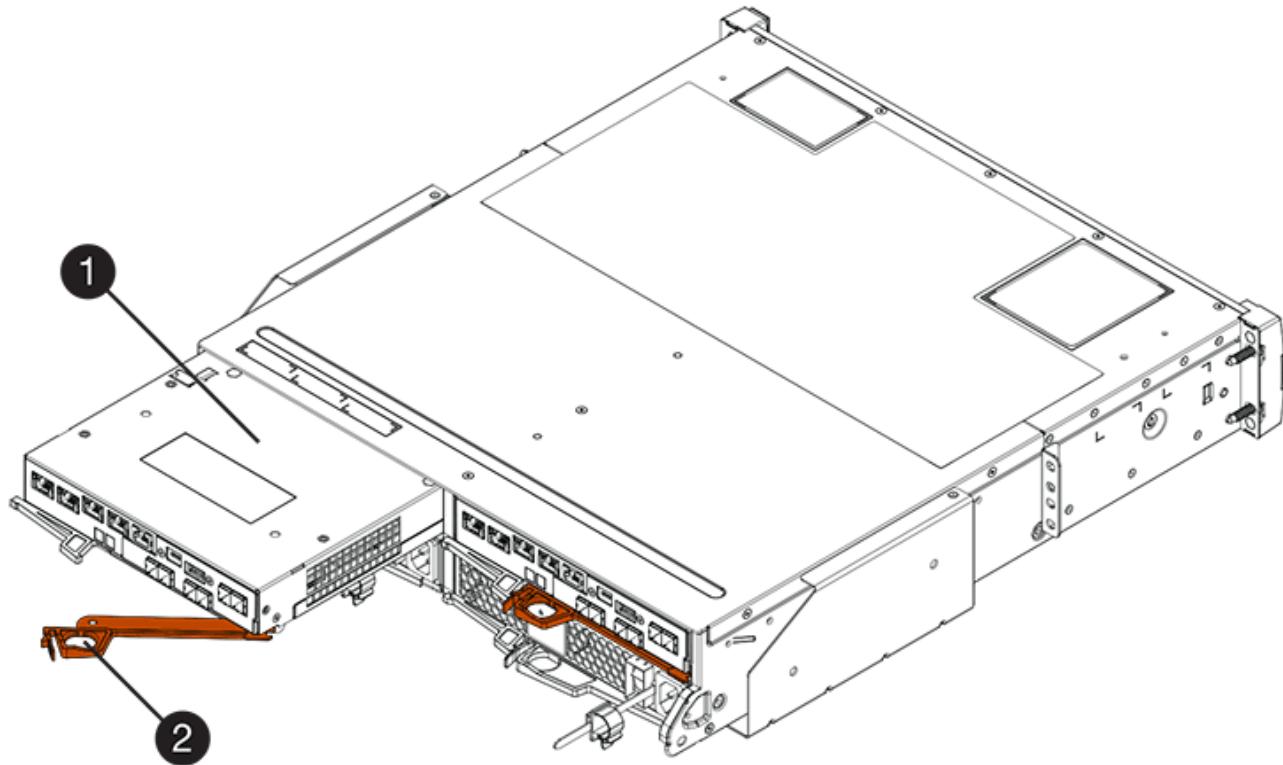
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

5. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

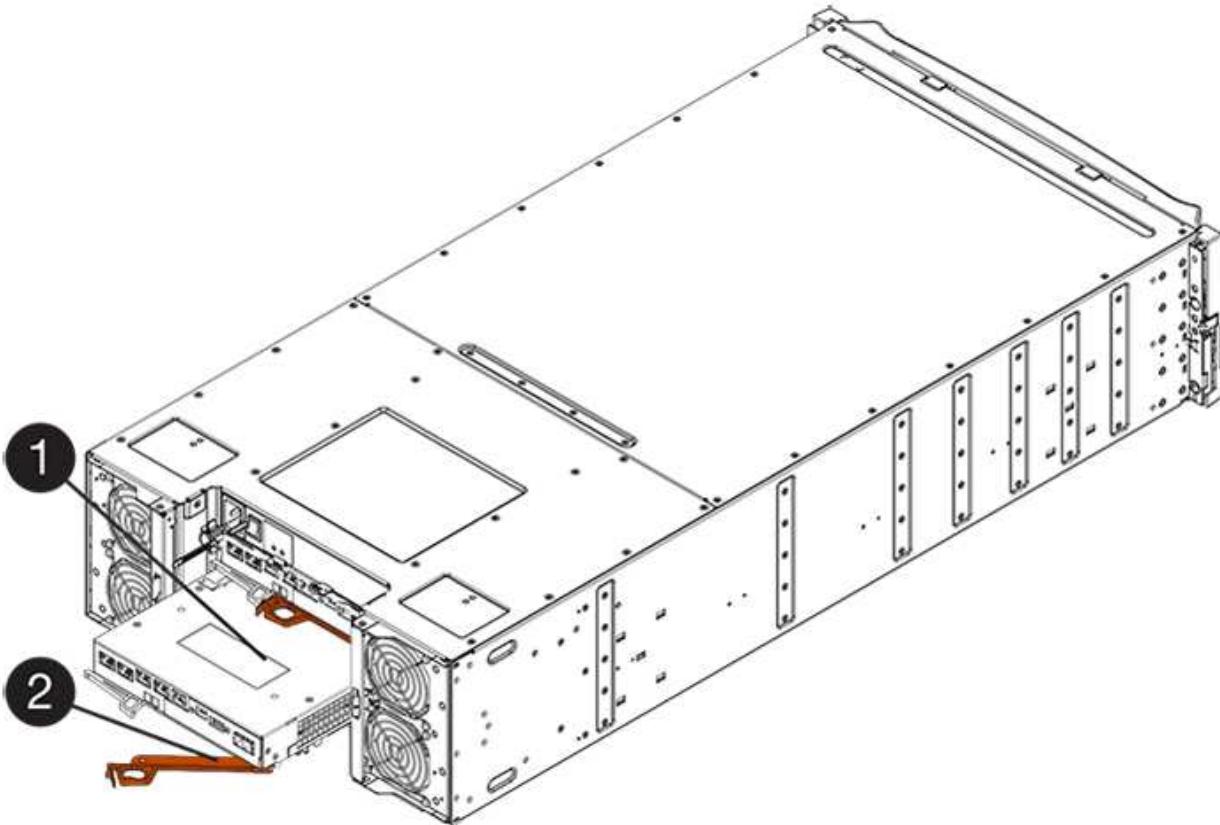
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

6. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E5724 controller shelf, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

7. Turn the controller canister over, so that the removable cover faces up.
8. Place the controller canister on a flat, static-free surface.

Step 3: Remove a HIC

Remove the original HIC so you can replace it with an upgraded one.

Steps

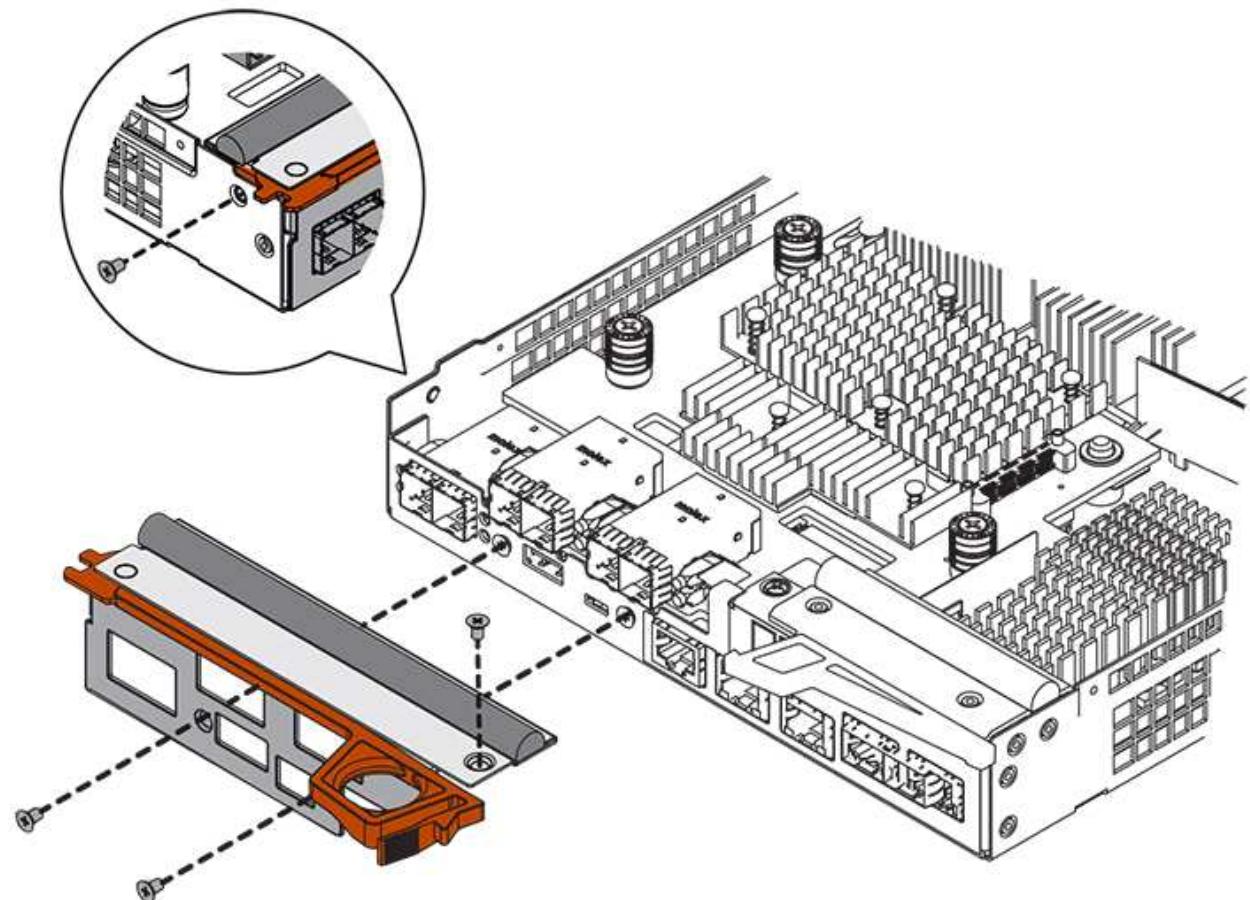
1. Remove the controller canister's cover by pressing down on the button and sliding the cover off.
2. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



3. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller canister.

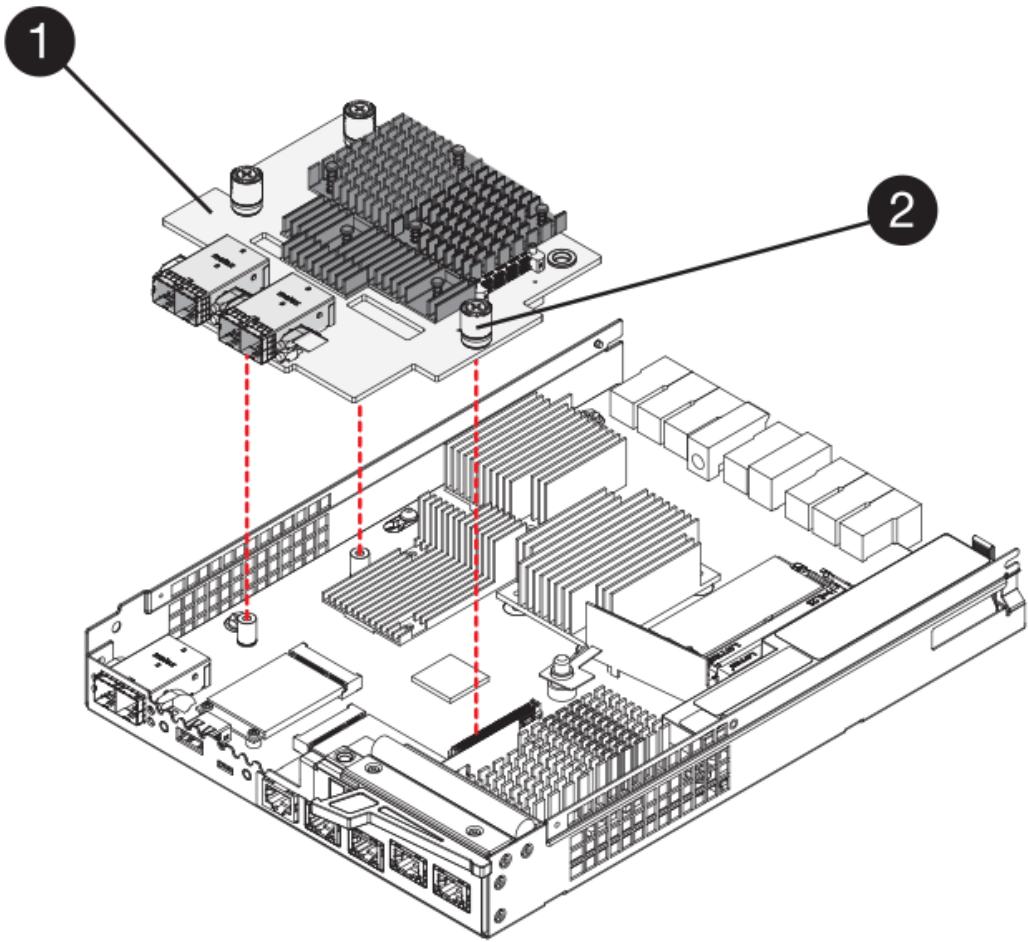
There are four screws: one on the top, one on the side, and two on the front.



4. Remove the HIC faceplate.
5. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
6. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



(1) Host interface card (HIC)

(2) Thumbscrews

7. Place the HIC on a static-free surface.

Step 4: Install the new HIC

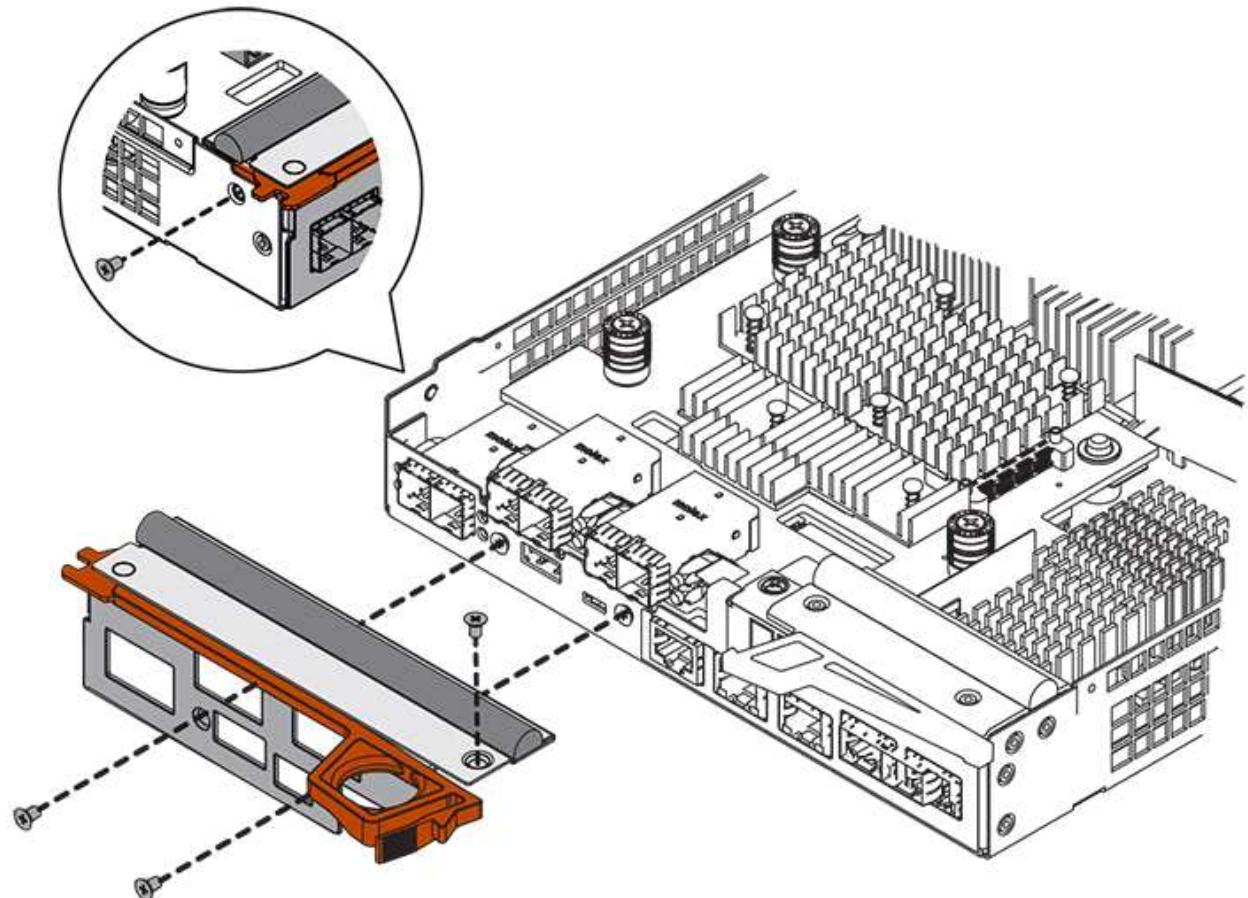
Install the new host HIC.



Possible loss of data access — Never install a HIC in an E5700 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs will cause the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Using a #1 Phillips screwdriver, remove the four screws that attach the HIC faceplate to the controller canister, and remove the faceplate.



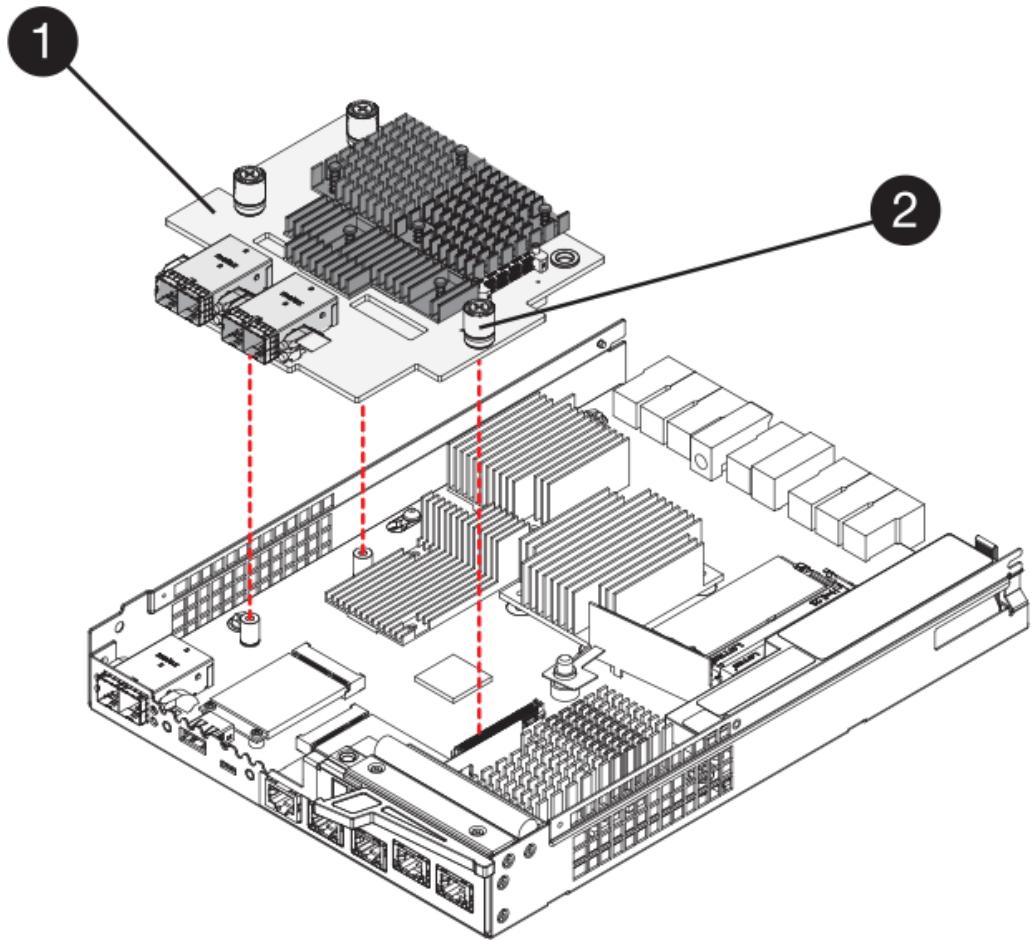
3. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

4. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



(1) Host interface card (HIC)

(2) Thumbscrews

5. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over-tighten the screws.

6. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.

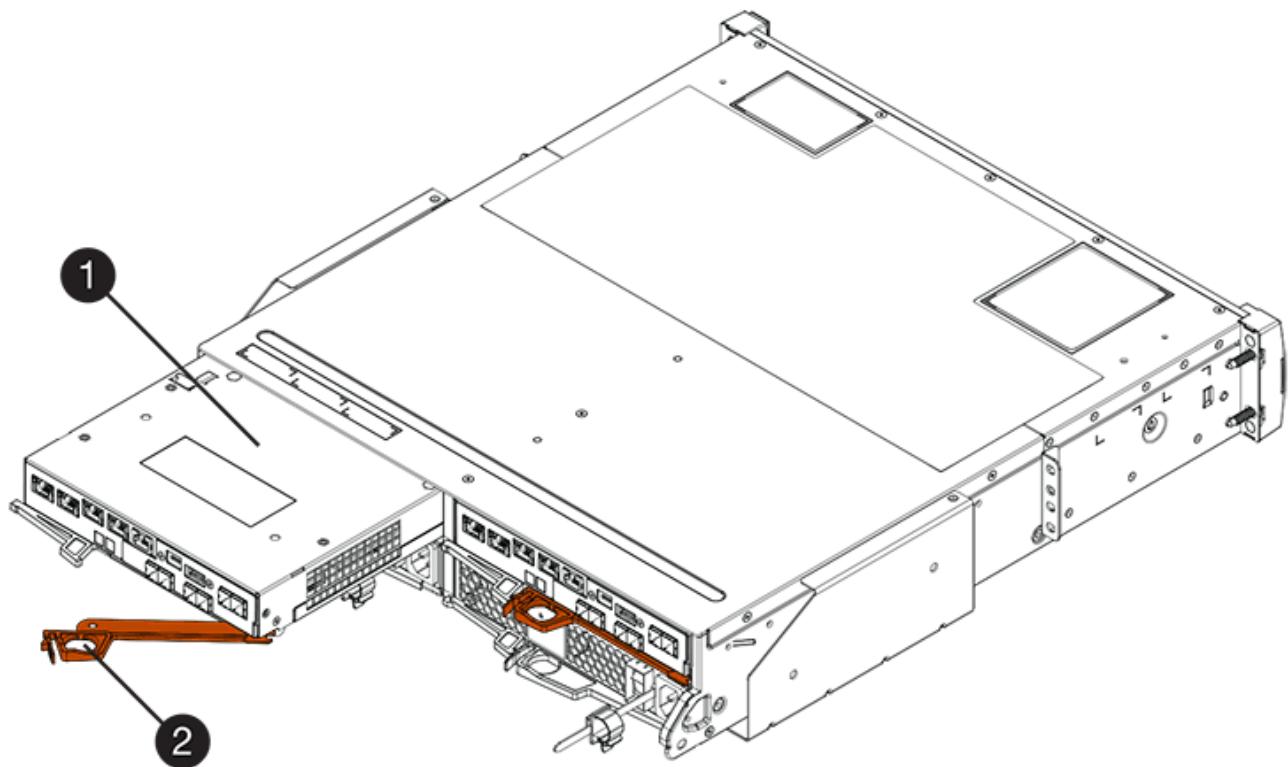
Step 5: Reinstall controller canister

After installing the new HIC, reinstall the controller canister into the controller shelf.

Steps

1. Reinstall the cover on the controller canister by sliding the cover from back to front until the button clicks.
2. Turn the controller canister over, so that the removable cover faces down.
3. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

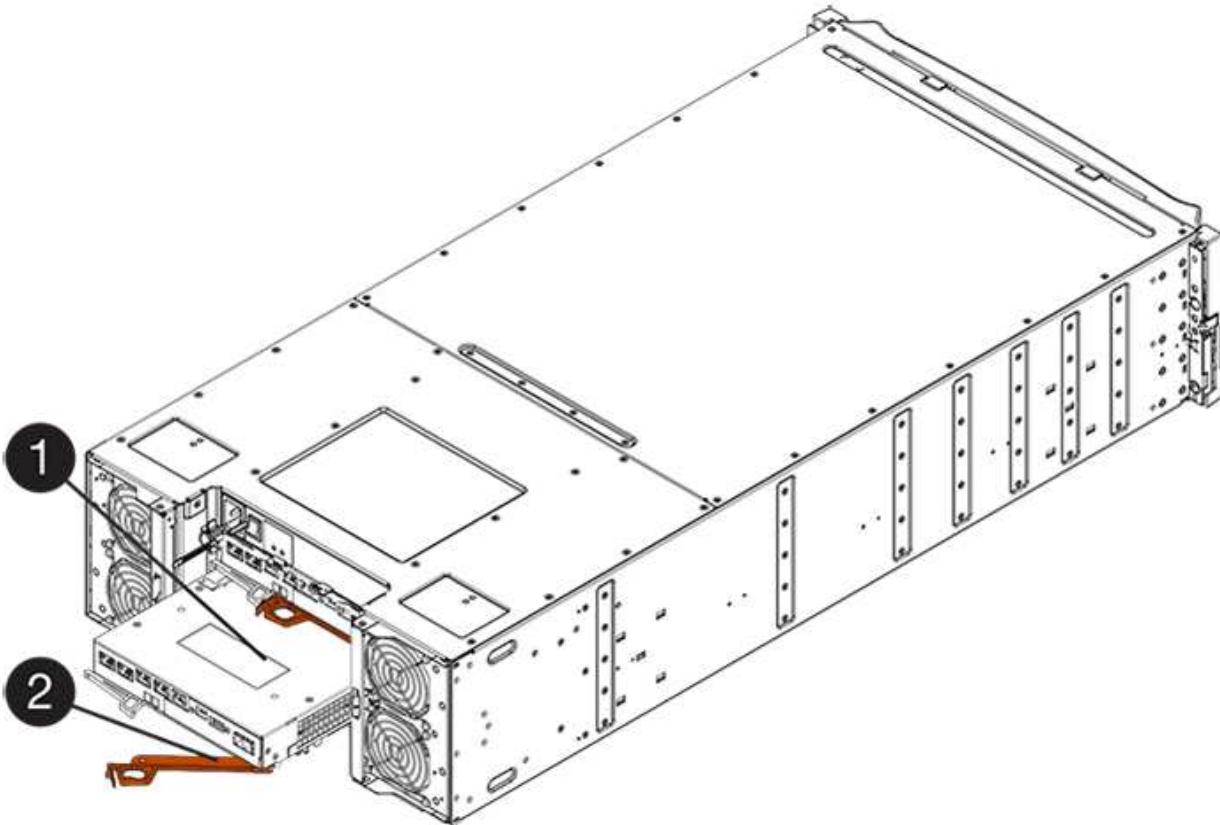
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

4. Move the cam handle to the left to lock the controller canister in place.
5. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

6. (Optional) If you are upgrading HICs in a duplex configuration, repeat all steps to remove the other controller canister, remove the HIC, install the new HIC, and replace the second controller canister.

Step 6: Complete the HIC upgrade

Check the controller LEDs and seven-segment display and confirm that the controller's status is Optimal.

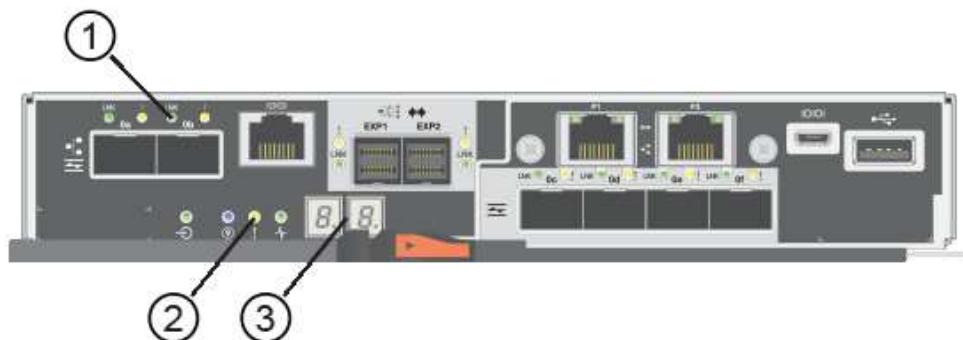
Steps

1. Turn on the two power switches at the back of the controller shelf.
 - Do not turn off the power switches during the power-on process, which typically takes 90 seconds or less to complete.
 - The fans in each shelf are very loud when they first start up. The loud noise during start-up is normal.
2. As the controller boots, check the controller LEDs and seven-segment display.
 - The seven-segment display shows the repeating sequence **OS, Sd, blank** to indicate that the controller is performing Start-of-day (SOD) processing. After a controller has successfully booted up, its seven-segment display should show the tray ID.
 - The amber Attention LED on the controller turns on and then turns off, unless there is an error.

- The green Host Link LEDs remain off until you connect the host cables.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.



(1) Host Link LED (amber)

(2) Attention LED (amber)

(3) Seven-segment display

3. From SANtricity System Manager, confirm that the controller's status is Optimal.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

4. If the new HIC ports require SFP+ transceivers, install these SFPs.

5. Connect the cables from the controller's host ports to the data hosts.

What's next?

The process of upgrading a host interface card in your storage array is complete. You can resume normal operations.

Replace E5700 host interface card (HIC)

You can replace a host interface card (HIC) that has failed.

About this task

When you replace a HIC, you place the controller offline (for duplex configurations), remove the controller canister, install the new HIC, and then replace the controller canister.

Before you begin

- Review [Requirements for E5700 HIC replacement](#).
- Schedule a downtime maintenance window for this procedure. The power must be off when you install HICs, so you cannot access data on the storage array until you have successfully completed this procedure. (In a duplex configuration, both controllers must have the same HIC configuration when they

are powered on.)

- Verify that no volumes are in use or that you have a multipath driver installed on all hosts using these volumes.
- From SANtricity System Manager, verify the details in the Recovery Guru to confirm that you have a failed HIC and to ensure no other items must be addressed before you can remove and replace the HIC.

What you'll need

- Two HICs that are compatible with your controllers.

For duplex configurations (two controllers), the HICs installed in the two controller canisters must be identical. The presence of mismatched HICs causes the controller with the replacement HIC to lock down when you bring it online.

- An ESD wristband, or you have taken other antistatic precautions.
- A #1 Phillips screwdriver.
- Labels to identify each cable that is connected to the controller canister.
- A management station with a browser that can access SANtricity System Manager for the controller. (To open the System Manager interface, point the browser to the controller's domain name or IP address.)

Step 1: Place controller offline (duplex)

If you have a duplex configuration, you must place the affected controller offline so you can safely remove the failed HIC.

Steps

1. From the Details area of the Recovery Guru, determine which of the controller canisters has the failed HIC.
2. Back up the storage array's configuration database using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to restore your configuration. The system will save the current state of the RAID configuration database, which includes all data for volume groups and disk pools on the controller.

- From System Manager:
 - a. Select **Support > Support Center > Diagnostics**.
 - b. Select **Collect Configuration Data**.
 - c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **configurationData-<arrayName>-<dateTime>.7z**.

- Alternatively, you can back up the configuration database by using the following CLI command:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all  
file="filename";
```

3. Collect support data for your storage array using SANtricity System Manager.

If a problem occurs during this procedure, you can use the saved file to troubleshoot the issue. The system will save inventory, status, and performance data about your storage array in a single file.

a. Select **Support > Support Center > Diagnostics**.

b. Select **Collect Support Data**.

c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

4. If the controller is not already offline, take it offline now using SANtricity System Manager.

◦ From SANtricity System Manager:

a. Select **Hardware**.

b. If the graphic shows the drives, select **Show back of shelf** to show the controllers.

c. Select the controller that you want to place offline.

d. From the context menu, select **Place offline**, and confirm that you want to perform the operation.



If you are accessing SANtricity System Manager using the controller you are attempting to take offline, a SANtricity System Manager Unavailable message is displayed. Select **Connect to an alternate network connection** to automatically access SANtricity System Manager using the other controller.

◦ Alternatively, you can take the controllers offline by using the following CLI commands:

For controller A: set controller [a] availability=offline

For controller B: set controller [b] availability=offline

5. Wait for SANtricity System Manager to update the controller's status to offline.



Do not begin any other operations until after the status has been updated.

Step 2: Remove controller canister

Remove the controller canister so you can add the new HIC.

Steps

1. Label each cable that is attached to the controller canister.

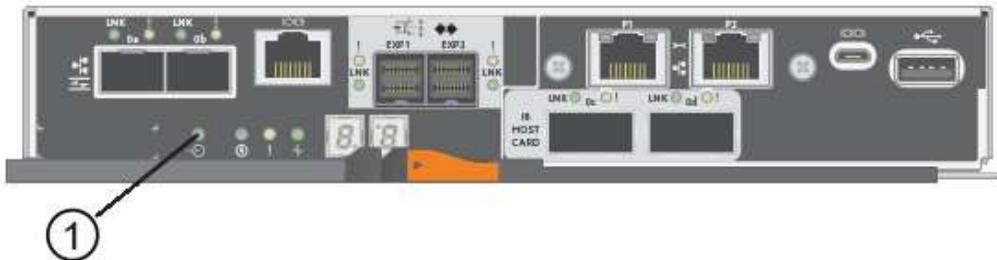
2. Disconnect all the cables from the controller canister.



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

3. Confirm that the Cache Active LED on the back of the controller is off.

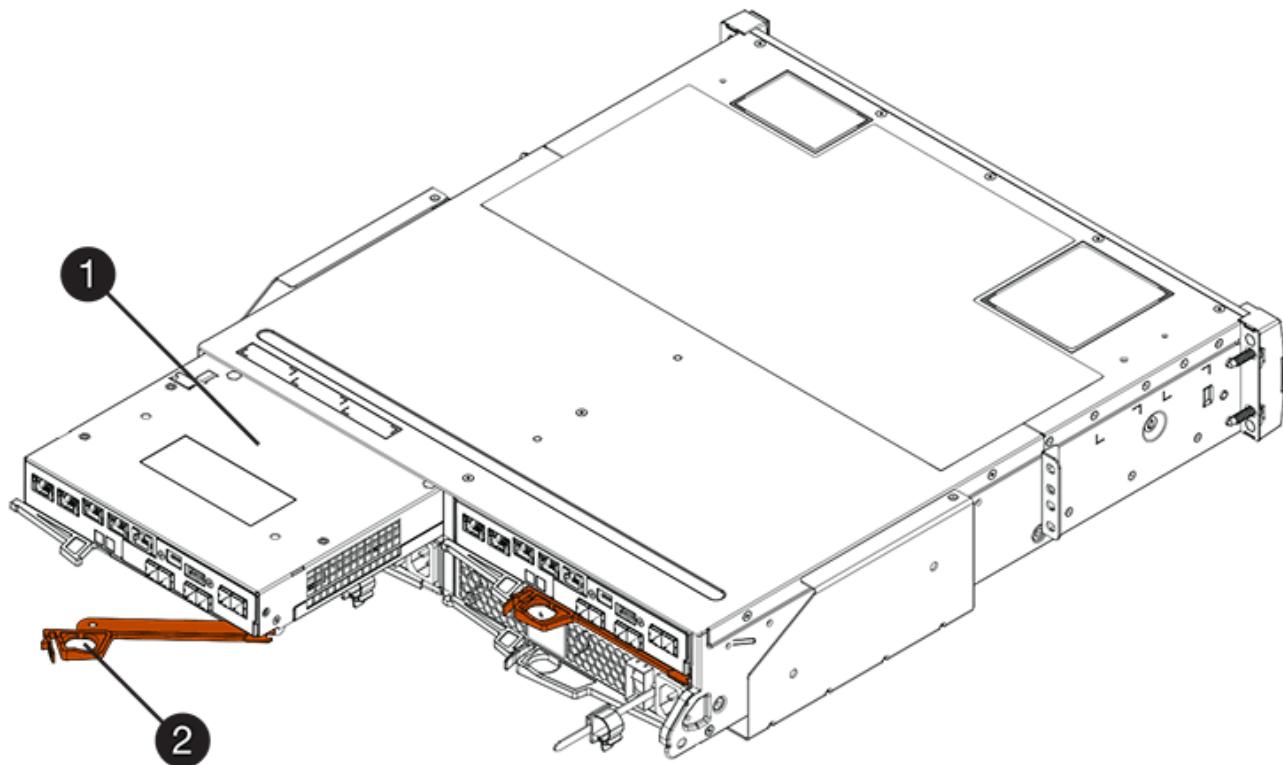
The green Cache Active LED on the back of the controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off before removing the controller canister.



(1) Cache Active LED

4. Squeeze the latch on the cam handle until it releases, and then open the cam handle to the right to release the controller canister from the shelf.

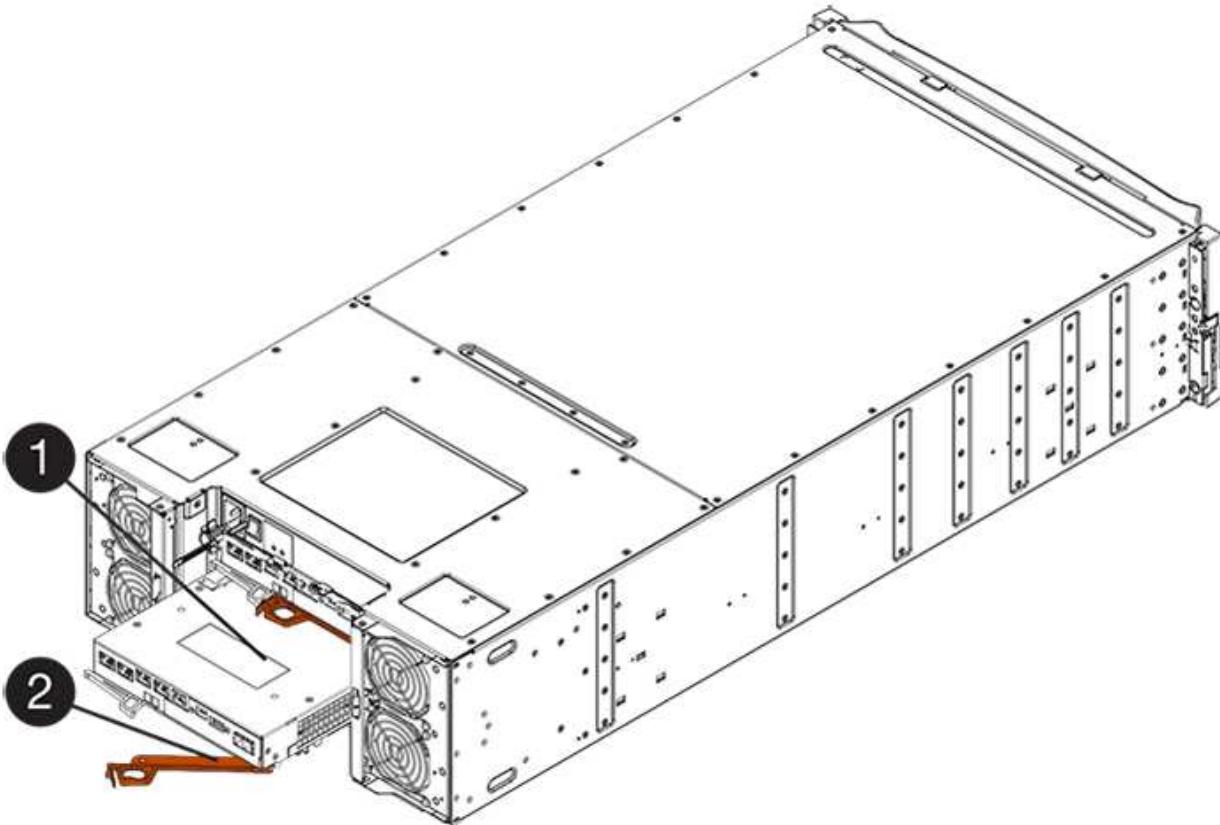
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) *Controller canister*

(2) *Cam handle*

5. Using two hands and the cam handle, slide the controller canister out of the shelf.



Always use two hands to support the weight of a controller canister.

If you are removing the controller canister from an E5724 controller shelf, a flap swings into place to block the empty bay, helping to maintain air flow and cooling.

6. Turn the controller canister over, so that the removable cover faces up.
7. Place the controller canister on a flat, static-free surface.

Step 3: Install a HIC

Install a new HIC to replace the failed one.



Possible loss of data access — Never install a HIC in an E5700 controller canister if that HIC was designed for another E-Series controller. In addition, if you have a duplex configuration, both controllers and both HICs must be identical. The presence of incompatible or mismatched HICs causes the controllers to lock down when you apply power.

Steps

1. Unpack the new HIC and the new HIC faceplate.
2. Press the button on the cover of the controller canister, and slide the cover off.
3. Confirm that the green LED inside the controller (by the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



(1) Internal Cache Active LED

(2) Battery

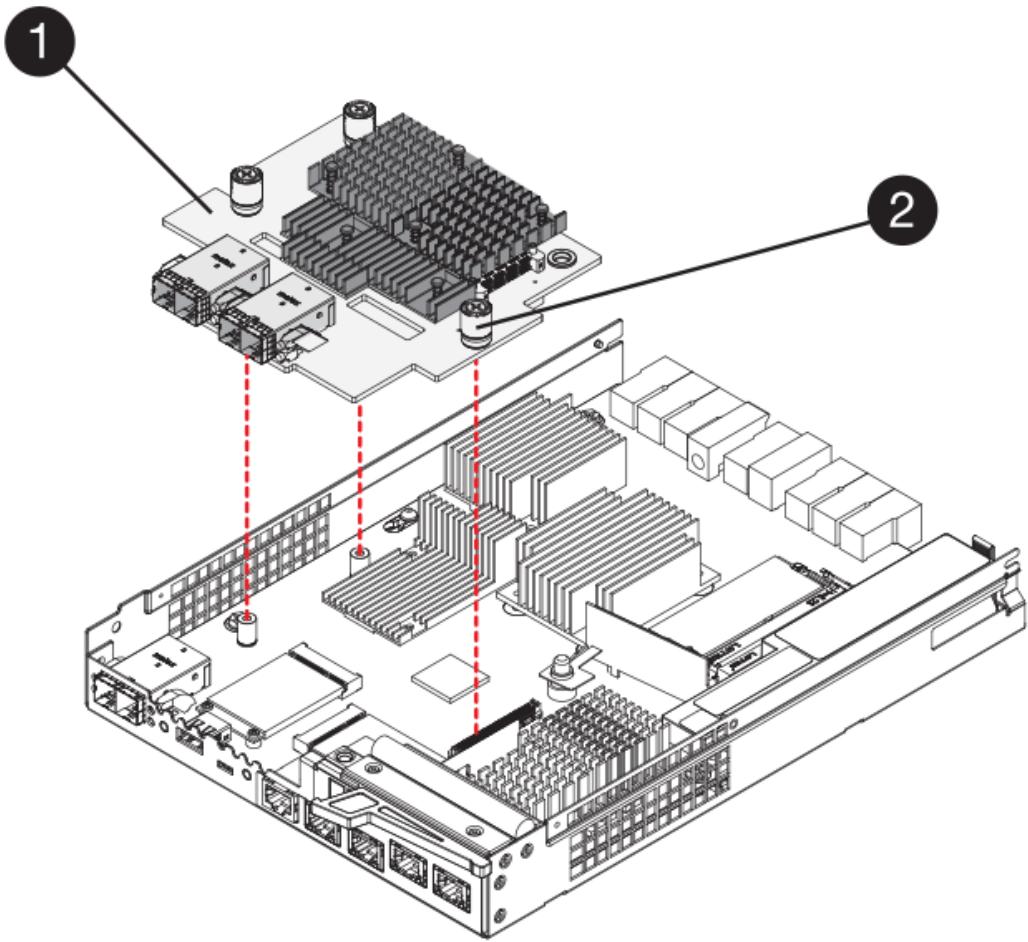
4. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the controller canister, and remove the faceplate.
5. Align the three thumbscrews on the HIC with the corresponding holes on the controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

6. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



Possible equipment damage — Be very careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



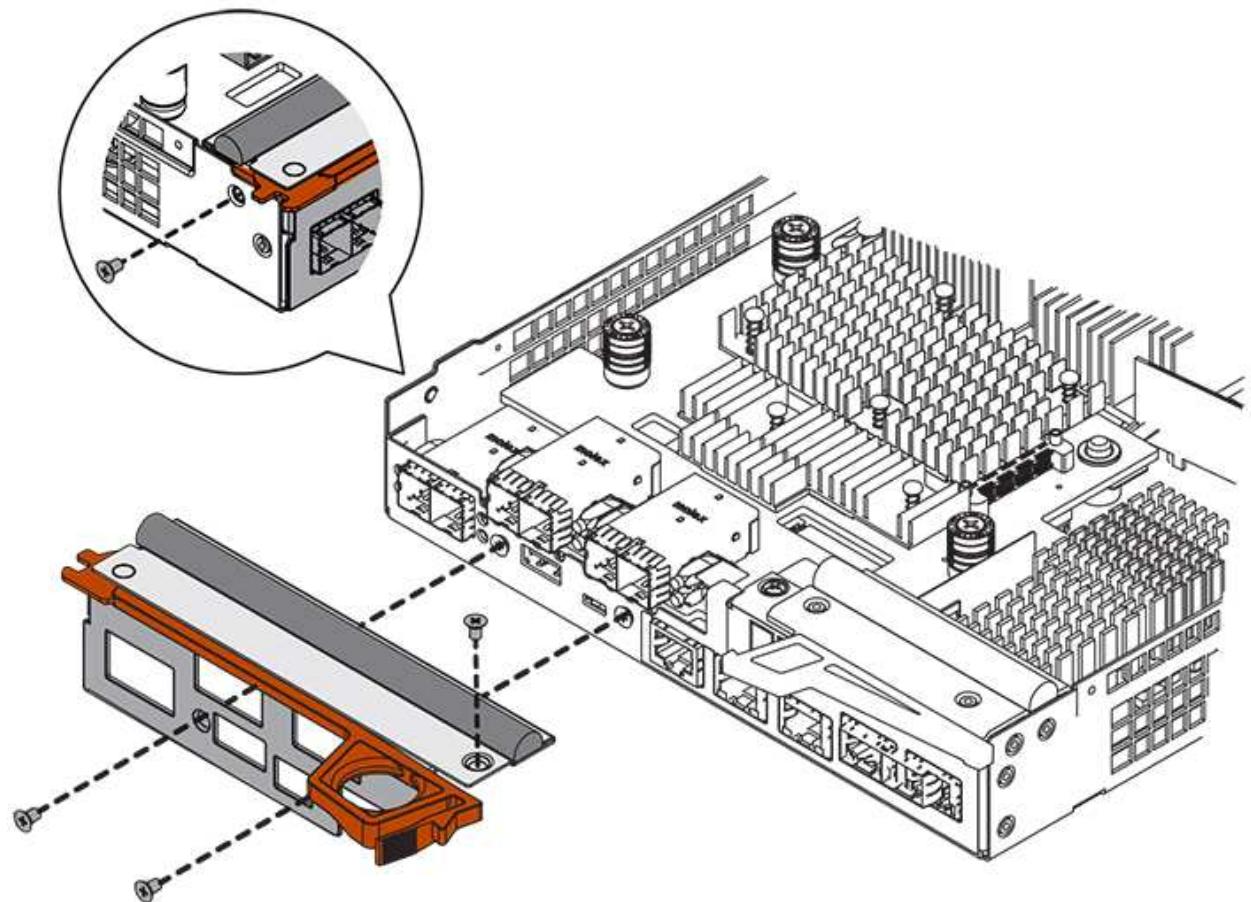
(1) Host interface card

(2) Thumbscrews

7. Hand-tighten the HIC thumbscrews.

Do not use a screwdriver, or you might over-tighten the screws.

8. Using a #1 Phillips screwdriver, attach the new HIC faceplate to the controller canister with the four screws you removed previously.



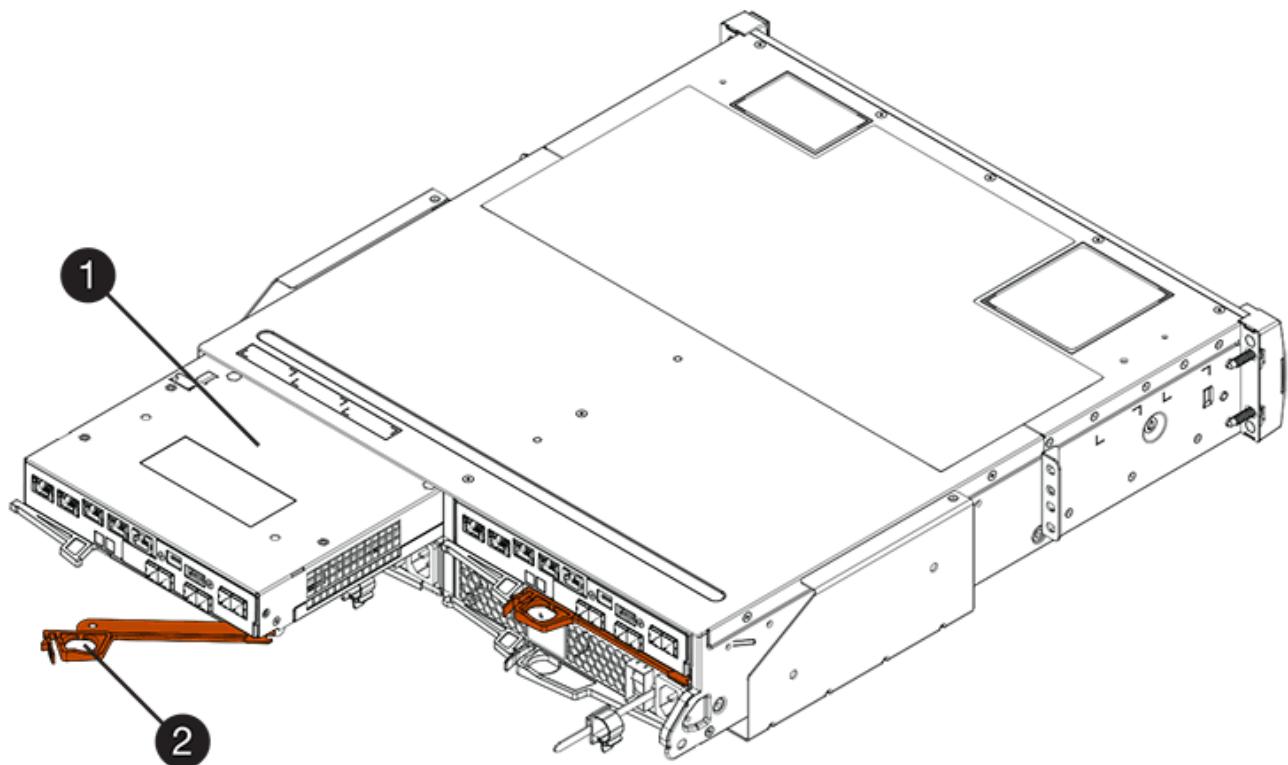
Step 4: Reinstall controller canister

After installing the HIC, reinstall the controller canister into the controller shelf.

Steps

1. Turn the controller canister over, so that the removable cover faces down.
2. With the cam handle in the open position, slide the controller canister all the way into the controller shelf.

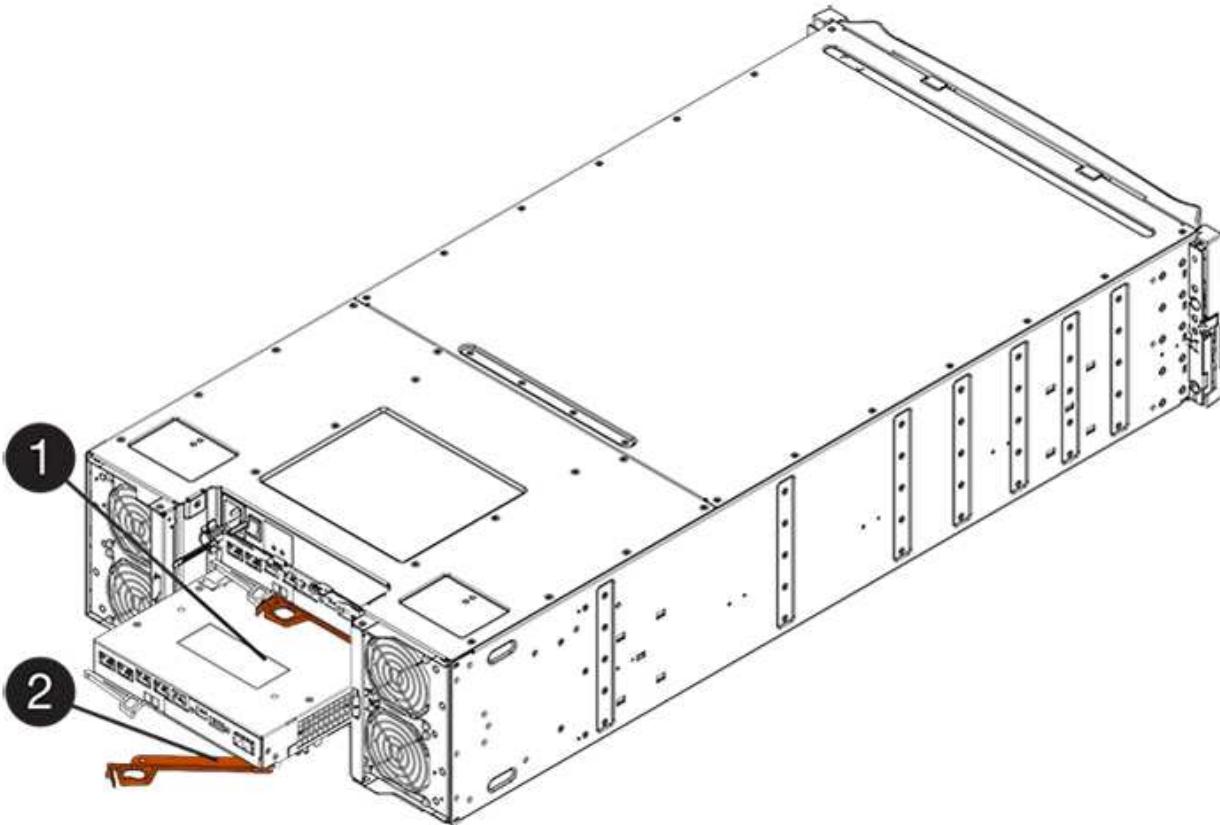
The following figure is an example of an E5724 controller shelf:



(1) Controller canister

(2) Cam handle

The following figure is an example of an E5760 controller shelf:



(1) Controller canister

(2) Cam handle

3. Move the cam handle to the left to lock the controller canister in place.
4. Reconnect all the cables you removed.



Do not connect data cables to the new HIC ports at this time.

5. (Optional) If you are adding HICs to a duplex configuration, repeat all steps to remove the second controller canister, install the second HIC, and reinstall the second controller canister.

Step 5: Place controller online (duplex)

If you have a duplex configuration, bring the controller online to confirm the storage array is working correctly, collect support data, and resume operations.



Perform this task only if your storage array has two controllers.

Steps

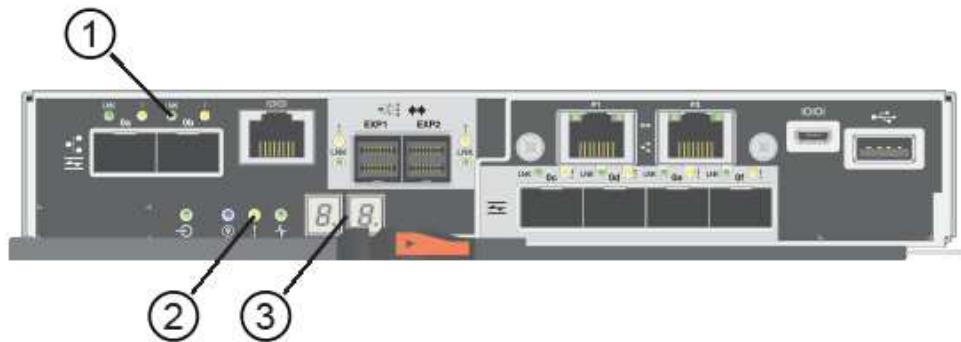
1. As the controller boots, check the controller LEDs and the seven-segment display.



The figure shows an example controller canister. Your controller might have a different number and a different type of host ports.

When communication with the other controller is reestablished:

- The seven-segment display shows the repeating sequence **OS**, **OL**, **blank** to indicate that the controller is offline.
- The amber Attention LED remains lit.
- The Host Link LEDs might be on, blinking, or off, depending on the host interface.



(1) Host Link LED

(2) Attention LED (amber)

(3) Seven-segment display

2. Bring the controller online using SANtricity System Manager.

- From SANtricity System Manager:
 - Select **Hardware**.
 - If the graphic shows the drives, select **Show back of shelf**.
 - Select the controller you want to place online.
 - Select **Place Online** from the context menu, and confirm that you want to perform the operation.

The system places the controller online.

- Alternatively, you can use the following CLI commands:

For controller A: set controller [a] availability=online;

For controller B: set controller [b] availability=online;

3. Check the codes on the controller's seven-segment display as it comes back online. If the display shows one of the following repeating sequences, immediately remove the controller.

- **OE, L0, blank** (mismatched controllers)

- **OE, L6, blank** (unsupported HIC)

Attention: Possible loss of data access — If the controller you just installed shows one of these codes, and the other controller is reset for any reason, the second controller could also lock down.

4. When the controller is back online, confirm that its status is Optimal, and check the controller shelf's Attention LEDs.

If the status is not Optimal or if any of the Attention LEDs are on, confirm that all cables are correctly seated, and check that the HIC and the controller canister are installed correctly. If necessary, remove and reinstall the controller canister and the HIC.



If you cannot resolve the problem, contact technical support.

5. Collect support data for your storage array using SANtricity System Manager.

- a. Select **Support > Support Center > Diagnostics**.
- b. Select **Collect Support Data**.
- c. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name, **support-data.7z**.

6. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Contact technical support at [NetApp Support](#), 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number.

What's next?

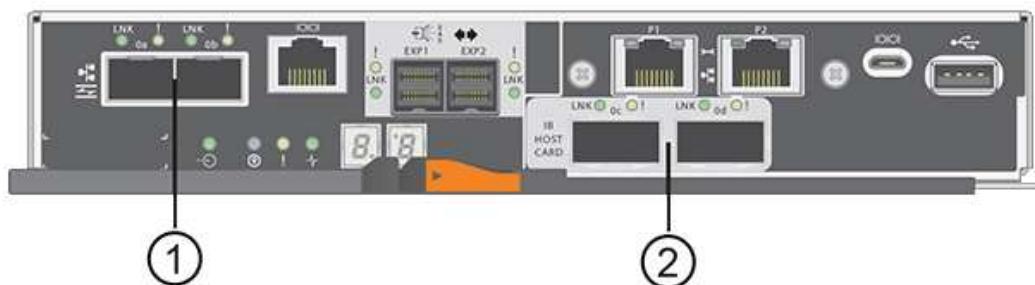
Your HIC replacement is complete. You can resume normal operations.

Host port protocol

Requirements for changing the E5700 host port protocol

Before converting the host port protocol in the E5700, review the requirements.

The following figure shows the E5700 with its SFP+ (optical) baseboard host ports (**1**) and the optional two IB HIC ports (**2**).



Requirements

- You must schedule a downtime maintenance window for this procedure.
- You must stop host I/O operations when you perform the conversion, and you will not be able to access data on the storage array until you have successfully completed the conversion.
- You must use out-of-band management. (You cannot use in-band management to complete this procedure.)
- You have obtained the necessary hardware for the conversion. Your NetApp Sales Representative can help you determine what hardware you need and help you order the correct parts.
- If you are attempting to change the baseboard host ports of your storage array, and it currently uses dual-

protocol (also referred to as *unified*) SFP transceivers that you purchased from NetApp, you do not need to change your SFP transceivers.

- Make sure that the dual-protocol SFP transceivers support both FC (at 4 Gbps, or 16 Gbps) and iSCSI (at 10 Gbps), but they do not support 1 Gbps iSCSI. See [Step 1: Determine whether you have dual-protocol SFPs](#) to determine what type of SFP transceivers are installed.

Considerations for changing the host protocol

The considerations for changing the host protocol depend on the starting and ending protocols of the baseboard host ports and the HIC ports.

If you use a Mirroring feature or the Data Assurance (DA) feature, you must understand what happens to these features when you change the host port protocol.



The following considerations apply only if you are converting a storage array that has already been in use. These considerations do not apply if you are converting a new storage array that does not yet have hosts and volumes defined.

Converting from FC to iSCSI

- Asynchronous Mirroring requires both the local storage array and the remote storage array to use the same protocol.
 - If you are currently using Asynchronous Mirroring through the baseboard, you must deactivate Asynchronous Mirroring relationships using those ports before applying the feature pack.
 - Refer to the online help for SANtricity System Manager to delete all mirror consistency groups and remove all mirrored pairs from the local and remote storage arrays. In addition, follow the instructions in the online help to deactivate Asynchronous Mirroring.



If your configuration contains SAN Boot hosts connected to the FC baseboard ports, check the [NetApp Interoperability Matrix](#) tool to ensure that the configuration is supported on iSCSI. If it is not, you cannot convert the host protocol to iSCSI.

- The Synchronous Mirroring feature is not supported for iSCSI.

- If you are currently using Synchronous Mirroring relationships via the baseboard ports, you must deactivate those Synchronous Mirroring relationships.
 - Refer to the online help for SANtricity System Manager to remove all synchronous mirrored pairs, which removes mirror relationships on the local storage array and on the remote storage array. In addition, follow the instructions in the online help to deactivate Synchronous Mirroring.



If you do not deactivate Synchronous Mirroring relationships before converting to iSCSI, your system will lose data access and data loss might occur.

Converting from iSCSI to FC

- Asynchronous Mirroring requires both the local storage array and the remote storage array to use the same protocol. If you are currently using Asynchronous Mirroring with the baseboard ports, you must deactivate Asynchronous Mirroring before changing the protocol.
- Refer to the online help for SANtricity System Manager to delete all mirror consistency groups and remove all mirrored pairs from the local and remote storage arrays. In addition, follow the instructions in the online help to deactivate Asynchronous Mirroring.

Converting IB-iSER to/from IB-SRP

- You do not have to make any changes to your hardware when you convert from/to iSER to SRP.
- The Data Assurance (DA) feature is not supported for SRP.
- The DA feature is not supported for IB-SRP. If you are currently using this feature via the IB-HIC and you want to convert those ports from iSER to SRP, you must permanently disable DA on all volumes. Refer to the online help for SANtricity System Manager to change the settings for a volume to permanently disable the data assurance setting.



After it has been disabled, DA cannot be re-enabled on the volume.

- Confirm the following:
 - SANtricity System Manager is accessible via a web browser.
 - The storage system is running SANtricity OS (controller firmware) version 08.40.11.00 or later.

Mirroring operations need same host protocol

Mirroring operations are not affected if the host ports being used for mirroring keep the same protocol after you apply the feature pack. Even so, before applying the feature pack, you should confirm that all mirror consistency groups are synchronized. After applying the feature pack, you should test the communication between the local storage array and the remote storage array. Refer to the online help for SANtricity System Manager if you have questions on how to do this.



Asynchronous and synchronous mirroring are not supported for NVMe over Fabrics. To disable Asynchronous and Synchronous mirroring, you can use the `disable storageArray feature=asyncMirror` or `disable storageArray feature=syncMirror` commands through the command line interface. Refer to the [Disable storage array feature](#) mirroring commands under the CLI Command Reference Online Help for more information on how to disable mirroring.

Change E5700 host protocol

For an E5700 storage array, you can convert baseboard host ports as follows:

- Fibre Channel (FC) to iSCSI
- iSCSI to FC
- iSER to InfiniBand (IB)
- SRP to IB
- NVMe to IB
- NVMe to RoCE

Step 1: Determine whether you have dual-protocol SFPs

Use SANtricity System Manager to determine what type of SFP transceivers you have. Because these SFPs can be used with both FC and iSCSI protocols, they are referred to as *dual-protocol* or *unified* SFPs.

If your current SFPs support data rates of 16 Gbps and 10 Gbps, you can continue to use them after converting the host port protocol.

Steps

1. From SANtricity System Manager, select **Support**.
2. Select the **Support Center** tile.
3. On the Support Resources tab, locate and select the **Storage Array Profile** link.
4. Type **SFP** in the text box, and click **Find**.
5. For each SFP listed in the Storage Array Profile, locate the entry for **Supported data rate(s)**.

| | |
|-------------------------|----------------------------------|
| SFP status: | Optimal |
| Attached to: | Host-side of controller B |
| Location: | Unknown |
| Supported data rate(s): | 16 Gbps, 10 Gbps, 8 Gbps, 4 Gbps |
| Link length: | Short |
| Connector: | LC |
| Transmitter type: | Shortwave Laser w/o OFC |
| Transmission media: | TM Multi-mode 62.5m (M6) |
| IEEE company ID: | 00 17 6a |
| Revision: | Not Available |
| Part number: | AFBR-57F5UMZ |
| Serial number: | AA1317J14X7 |
| Vendor: | AVAGO |
| Date of manufacture: | 4/28/13 |

6. Refer to the table to determine whether you can reuse the SFPs, as follows:

| Supported data rate(s) | SFP type | Supported protocol |
|--------------------------|---------------|--|
| 16 Gbps, 10 Gbps, 4 Gbps | Dual-protocol | <ul style="list-style-type: none">• FC: 16 Gbps, 4 Gbps• iSCSI: 10 Gbps |
| 10 Gbps | 10 Gbps | iSCSI only |
| 16 Gbps, 8 Gbps, 4 Gbps | 16 Gbps | FC only |

- If you have dual-protocol SFPs, you can continue using them after you convert the protocol.



The dual-protocol SFPs do not support 1 Gb iSCSI. If you are converting host ports to iSCSI, be aware that the dual-protocol SFPs support only a 10 Gb link to the connected port.

- If you have 16 Gbps SFPs, and you are converting host ports to iSCSI, you must remove the SFPs and replace them with dual-protocol or 10 Gbps SFPs after converting the protocol. As needed, you can also use 10 Gbps iSCSI copper by using a special Twin-Ax cable with SFPs.



8Gbps FC SFPs are NOT supported in the E28xx or E57xx controllers. ONLY 16Gbps and 32 Gbps FC SFPs are supported.

- If you have 10 Gbps SFPs, and you are converting host ports to FC, you must remove the SFPs from these ports and replace them with dual-protocol or 16 Gbps SFPs after converting the protocol.

Step 2: Obtain the feature pack

To obtain the feature pack, you need the serial number from the controller shelf, a Feature Activation Code, and the Feature Enable Identifier for the storage array.

Steps

1. Locate the serial number.
 - a. From SANtricity System Manager, select **Support > Support Center**.
 - b. With the **Support Resources** tab selected, scroll to the **View top storage array properties** section.
 - c. Locate the **Chassis Serial Number**, and copy this value to a text file.

View top storage array properties

| | |
|--|----------------------------------|
| Storage array world-wide identifier (ID): | 600A0980006CEF9B00000000574DB18C |
| Chassis serial number: | 1142FG00061 |
| Number of shelves: | 2 |
| Number of drives: | 41 |
| Drive media types: | HDD |
| Number of controllers: | 2 |
| Controller board ID: | 2806 |

2. Locate the **feature pack submodel ID**.
 - a. From the SANtricity System Manager, select **Support**.
 - b. Select the **Support Center** tile.
 - c. On the Support Resources tab, locate and select the **Storage Array Profile** link.
 - d. Type **feature pack submodel ID** in the text box, and click **Find**.
 - e. Locate the feature pack submodel ID for the starting configuration.

Storage Array Profile



Feature pack submodel ID

Find

Results: 1 of 1

Feature pack submodel ID: 318

Additional feature information

Snapshot groups allowed per base volume (see note below): 4
Volume assignments per host or host cluster: 256

Note: If a volume is a member of a snapshot consistency group, that membership (member volume) counts against both the snapshot groups allowed per base volume and the volume assignments per host or host cluster.

FIRMWARE INVENTORY

Storage Array

| | |
|---|--------------------------|
| Report Date: | 2/13/17 4:56:33 PM UTC |
| Storage Array Name: | LDAPandCLI-Cfg04-Arapaho |
| Current SANtricity OS Software Version: | 88.40.39.74.001 |
| Management Software Version: | 11.40.0010.0051 |
| Controller Firmware Version: | 88.40.39.74 |
| Supervisor Software Version: | 88.40.39.74 |
| IOM (ESM) Version: | 81.40.0G00.0006 |
| Current NVSRAM Version: | N280X-840834-402 |
| Staged SANtricity OS Software Version: | None |
| Staged NVSRAM Version: | None |

3. Using the feature pack submodel ID, locate the corresponding Controller submodel ID for the starting configuration and find the Feature Activation Code for the desired ending configuration within the table below. Then, copy that Feature Activation Code to a text file.



Baseboard ports are disabled when running an NVMe protocol on the HIC.



If you are not using the IB HIC, you can ignore the *HIC Ports* column in the following tables:

Encryption Capable Feature Activation Codes (Baseboard Port Only Conversions)

| Starting Configuration | | Ending Configuration | | |
|------------------------|-----------------------|------------------------|-----------------------|-------------------------|
| Controller submodel ID | Ports to Convert | Controller Submodel ID | Ports Converted To | Feature Activation Code |
| 360 | FC baseboard ports | 362 | iSCSI baseboard ports | SGL-2SB-ZEX13 |
| 362 | iSCSI baseboard ports | 360 | FC baseboard ports | 5GI-4TB-ZW3HL |

Encryption Capable Feature Activation Codes

| Starting configuration | | | Ending configuration | | | |
|------------------------|-----------------|-----------|------------------------|-----------------|-----------|-------------------------|
| Controller Submodel ID | Baseboard Ports | HIC Ports | Controller Submodel ID | Baseboard Ports | HIC Ports | Feature Activation Code |

| Encryption Capable Feature Activation Codes | | | | | | |
|---|-------|------|-----|---------------|----------------------|---------------|
| 360 | FC | iSER | 361 | FC | SRP | UGG-XSB-ZCZKU |
| | | | 362 | iSCSI | iSER | SGL-2SB-ZEX13 |
| | | | 363 | iSCSI | SRP | VGN-LTB-ZGFCT |
| | | | 382 | Not Available | NVMe/IB | KGI-ISB-ZDHQF |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | YGH-BHK-Z8EKB |
| 361 | FC | SRP | 360 | FC | iSER | JGS-0TB-ZID1V |
| | | | 362 | iSCSI | iSER | UGX-RTB-ZLBPV |
| | | | 363 | iSCSI | SRP | 2G1-BTB-ZMRYN |
| | | | 382 | Not Available | NVMe/IB | TGV-8TB-ZKTH6 |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | JGM-EIK-ZAC6Q |
| 362 | iSCSI | iSER | 360 | FC | iSER | 5GI-4TB-ZW3HL |
| | | | 361 | FC | SRP | EGL-NTB-ZXKQ4 |
| | | | 363 | iSCSI | SRP | HGP-QUB-Z1ICJ |
| | | | 383 | Not Available | NVMe/IB | BGS-AUB-Z2YNG |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | 1GW-LIK-ZG9HN |

| Encryption Capable Feature Activation Codes | | | | | | |
|---|---------------|---------|-----|---------------|----------------------|---------------|
| | iSCSI | SRP | 360 | FC | iSER | SGU-TUB-Z3G2U |
| 363 | | | 361 | FC | SRP | FGX-DUB-Z5WF7 |
| | | | 362 | iSCSI | SRP | LG3-GUB-Z7V17 |
| | | | 383 | Not Available | NVMe/IB | NG5-ZUB-Z8C8J |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | WG2-0IK-ZI75U |
| | | | 360 | FC | iSER | QG6-ETB-ZPPPT |
| 382 | Not Available | NVMe/IB | 361 | FC | SRP | XG8-XTB-ZQ7XS |
| | | | 362 | iSCSI | iSER | SGB-HTB-ZS0AH |
| | | | 363 | iSCSI | SRP | TGD-1TB-ZT5TL |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | IGR-IIK-ZDBRB |
| | | | 360 | FC | iSER | LG8-JUB-ZATLD |
| 383 | Not Available | NVMe/IB | 361 | FC | SRP | LGA-3UB-ZBAX1 |
| | | | 362 | iSCSI | iSER | NGF-7UB-ZE8KX |
| | | | 363 | iSCSI | SRP | 3GI-QUB-ZFP1Y |
| | | | 403 | Not Available | NVMe/RoCE or NVMe/FC | 5G7-RIK-ZL5PE |

| Encryption Capable Feature Activation Codes | | | | | | |
|---|---------------|----------------------|-----|---------------|---------|---------------|
| 403 | Not Available | NVMe/RoCE or NVMe/FC | 360 | FC | iSER | BGC-UIK-Z03GR |
| | | | 361 | FC | SRP | LGF-EIK-ZPJRX |
| | | | 362 | iSCSI | iSER | PGJ-HIK-ZSIDZ |
| | | | 363 | iSCSI | SRP | 1GM-1JK-ZTYQX |
| | | | 382 | Not Available | NVMe/IB | JGH-XIK-ZQ142 |

| Non-Encryption Feature Activation Codes (Baseboard Port Only Conversions) | | | | | |
|---|-----------------------|------------------------|-----------------------|--|-------------------------|
| Starting configuration | | Ending Configuration | | | |
| Controller submodel ID | Ports to Convert | Controller Submodel ID | Ports Converted To | | Feature Activation Code |
| 365 | FC baseboard ports | 367 | iSCSI baseboard ports | | BGU-GVB-ZM3KW |
| 367 | iSCSI baseboard ports | 366 | FC baseboard ports | | 9GU-2WB-Z503D |

| Non-Encryption Feature Activation Codes | | | | | | |
|---|-----------------|-----------|------------------------|-----------------|-----------|-------------------------|
| Starting configuration | | | Ending configuration | | | |
| Controller submodel ID | Baseboard ports | HIC ports | Controller submodel ID | Baseboard ports | HIC ports | Feature Activation Code |
| | | | | | | |

| Non-Encryption Feature Activation Codes | | | | | | |
|---|-------|------|-----|---------------|----------------------|---------------|
| 365 | FC | iSER | 366 | FC | SRP | BGP-DVB-ZJ4YC |
| | | | 367 | iSCSI | iSER | BGU-GVB-ZM3KW |
| | | | 368 | iSCSI | SRP | 4GX-ZVB-ZNJVD |
| | | | 384 | Not Available | NVMe/IB | TGS-WVB-ZKL9T |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | WGC-GJK-Z7PU2 |
| 366 | FC | SRP | 365 | FC | iSER | WG2-3VB-ZQHLF |
| | | | 367 | iSCSI | iSER | QG7-6VB-ZSF8M |
| | | | 368 | iSCSI | SRP | PGA-PVB-ZUWMX |
| | | | 384 | Not Available | NVMe/IB | CG5-MVB-ZRYW1 |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | 3GH-JJK-ZANJQ |
| 367 | iSCSI | iSER | 365 | FC | iSER | PGR-IWB-Z48PC |
| | | | 366 | FC | SRP | 9GU-2WB-Z503D |
| | | | 368 | iSCSI | SRP | SGJ-IWB-ZJFE4 |
| | | | 385 | Not Available | NVMe/IB | UGM-2XB-ZKV0B |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | 8GR-QKK-ZFJTP |

| Non-Encryption Feature Activation Codes | | | | | | |
|---|---------------|---------|-----|---------------|----------------------|---------------|
| 368 | iSCSI | SRP | 365 | FC | iSER | YG0-LXB-ZLD26 |
| | | | 366 | FC | SRP | SGR-5XB-ZNTFB |
| | | | 367 | iSCSI | SRP | PGZ-5WB-Z8M0N |
| | | | 385 | Not Available | NVMe/IB | KG2-0WB-Z9477 |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | 2GV-TKK-ZIHI6 |
| 384 | Not Available | NVMe/IB | 365 | FC | iSER | SGF-SVB-ZWU9M |
| | | | 366 | FC | SRP | 7GH-CVB-ZYBGV |
| | | | 367 | iSCSI | iSER | 6GK-VVB-ZZSRN |
| | | | 368 | iSCSI | SRP | RGM-FWB-Z195H |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | VGM-NKK-ZDLDK |
| 385 | Not Available | NVMe/IB | 365 | FC | iSER | GG5-8WB-ZBKEM |
| | | | 366 | FC | SRP | KG7-RWB-ZC2RZ |
| | | | 367 | iSCSI | iSER | NGC-VWB-ZFZEN |
| | | | 368 | iSCSI | SRP | 4GE-FWB-ZGGQJ |
| | | | 405 | Not Available | NVMe/RoCE or NVMe/FC | NG1-WKK-ZLFAI |

Non-Encryption Feature Activation Codes

| | | | | | | |
|-----|---------------|----------------------|-----|---------------|---------|---------------|
| 405 | Not Available | NVMe/RoCE or NVMe/FC | 365 | FC | iSER | MG6-ZKK-ZNDVC |
| | | | 366 | FC | SRP | WG9-JKK-ZPUAR |
| | | | 367 | iSCSI | iSER | NGE-MKK-ZRSW9 |
| | | | 368 | iSCSI | SRP | TGG-6KK-ZT9BU |
| | | | 384 | Not Available | NVMe/IB | AGB-3KK-ZQBLR |



If your controller submodel ID is not listed, contact [NetApp Support](#).

4. In System Manager, locate the Feature Enable Identifier.

- Go to **Settings > System**.
- Scroll down to **Add-ons**.
- Under **Change Feature Pack**, locate the **Feature Enable Identifier**.
- Copy and paste this 32-digit number to a text file.

Change Feature Pack

X

Ensure you have obtained a feature pack file from your Technical Support Engineer. After you have obtained the file, transfer it to the storage array to change your feature pack.

Feature Enable Identifier: **333030343238333030343439574DB18C**

Select the feature pack file:

Current feature pack: SMID 261

Important: Changing a feature pack is an offline operation. Verify that there are no hosts or applications accessing the storage array and back up all data before proceeding.

Type CHANGE to confirm that you want to perform this operation.

Cancel
Change

- Go to [NetApp License Activation: Storage Array Premium Feature Activation](#), and enter the information

required to obtain the feature pack.

- Chassis serial number
- Feature Activation Code
- Feature Enable Identifier



The Premium Feature Activation web site includes a link to “Premium Feature Activation Instructions.” Do not attempt to use those instructions for this procedure.

6. Choose whether to receive the key file for the feature pack in an email or download it directly from the site.

Step 3: Stop host I/O

Stop all I/O operations from the host before converting the protocol of the host ports. You cannot access data on the storage array until you successfully complete the conversion.

This task applies only if you are converting a storage array that has already been in use.

Steps

1. 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.



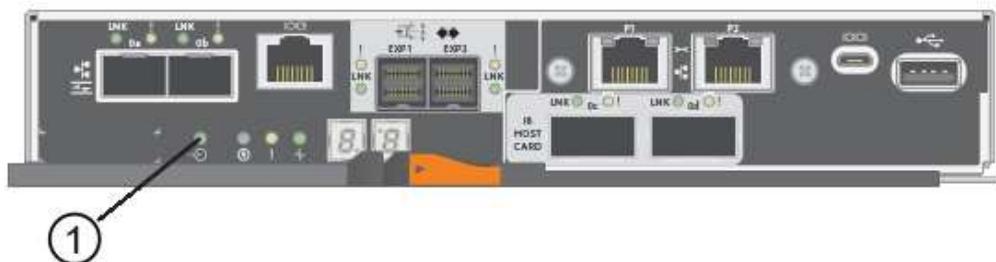
The exact steps to stop host I/O operations depend on the host operating system and the configuration, which are beyond the scope of these instructions. If you are not sure how to stop host I/O operations in your environment, consider shutting down the host.



Possible data loss — If you continue this procedure while I/O operations are occurring, the host application might lose data because the storage array will not be accessible.

2. If the storage array participates in a mirroring relationship, stop all host I/O operations on the secondary storage array.
3. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED (1) on the back of each controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.



4. From the Home page of SANtricity System Manager, select **View Operations in Progress**.

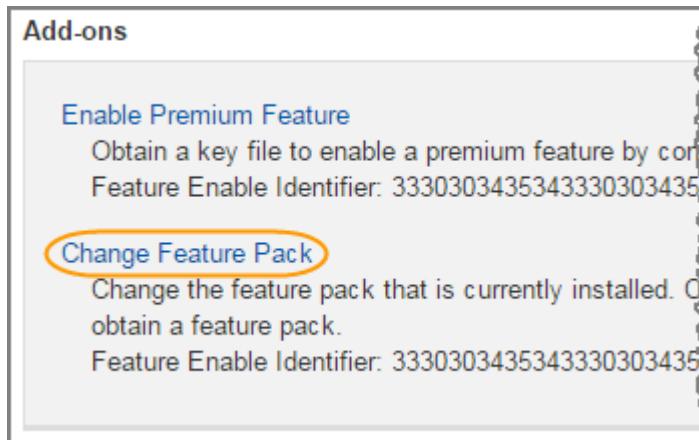
5. Wait for all operations to complete before continuing with the next step.

Step 4: Change the feature pack

Change the feature pack to convert the host protocol of the baseboard host ports, the IB HIC ports, or both types of ports.

Steps

1. From SANtricity System Manager, select **Settings > System**.
2. Under **Add-ons**, select **Change Feature Pack**.



3. Click **Browse**, and then select the feature pack you want to apply.
4. Type **CHANGE** in the field.
5. Click **Change**.

The feature pack migration begins. Both controllers automatically reboot twice to allow the new feature pack to take effect. The storage array returns to a responsive state after the reboot is complete.

6. Confirm the host ports have the protocol you expect.
 - a. From SANtricity System Manager, select **Hardware**.
 - b. Click **Show back of shelf**.
 - c. Select the graphic for either Controller A or Controller B.
 - d. Select **View settings** from the context menu.
 - e. Select the **Host Interfaces** tab.
 - f. Click **Show more settings**.
- g. Review the details shown for the baseboard ports and the HIC ports (labeled "slot 1"), and confirm that each type of port has the protocol you expect.

What's next?

Go to [Complete host protocol conversion](#).

Complete E5700 host protocol conversion

After converting the protocol of the host ports, perform additional steps to use the new protocol.

The steps you might need to complete depend on the starting and ending protocols of the baseboard host ports and the HIC ports.

Complete FC to iSCSI conversion

If you previously had FC host ports and you converted to iSCSI, you might need to modify your existing configuration to support iSCSI. The following procedure is only applicable if there is no iSCSI HIC present.

About this task

This task applies only if you are converting a storage array that has already been in use.

This task does not apply if you are converting a new storage array that does not yet have hosts and volumes defined. If you converted the host-port protocol of a new storage array, see the [Cabling procedures](#) to install cables and SFPs. Then, follow the instructions in the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#) to complete the setup for each protocol.

Steps

1. Configure the switches.

You should configure the switches used to transport iSCSI traffic according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as code updates.

2. From SANtricity System Manager, select **Hardware > Configure iSCSI ports**.

3. Select the port settings.

You can set up your iSCSI network in many ways. Consult your network administrator for tips on selecting the best configuration for your environment.

4. Update the host definitions in SANtricity System Manager.

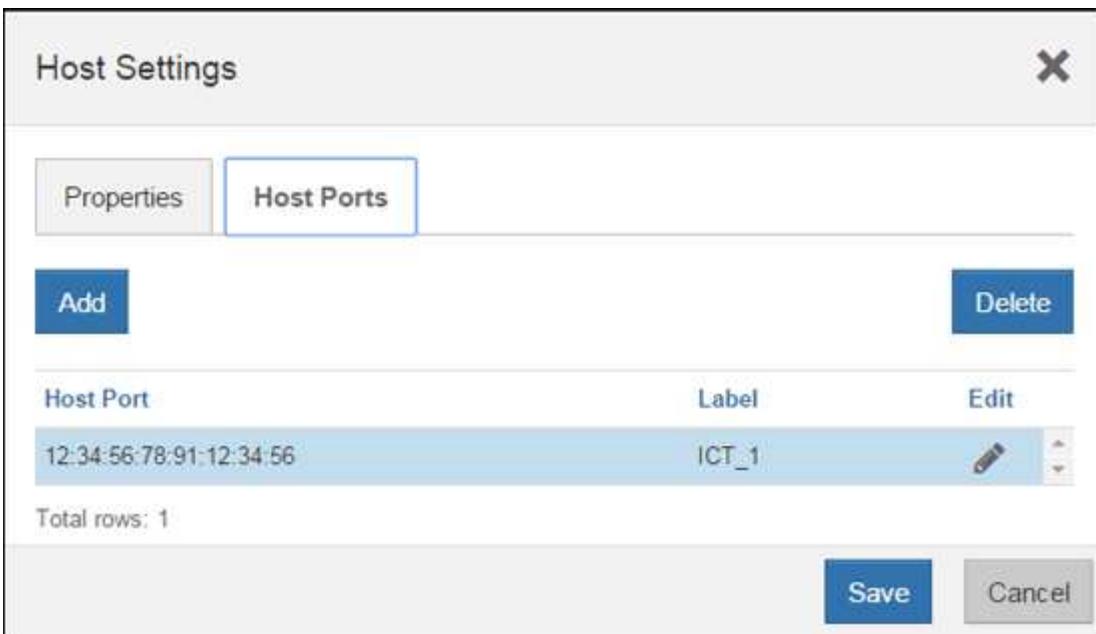


If you need instructions to add hosts or host clusters, refer to the online help for SANtricity System Manager.

- a. Select **Storage > Hosts**.
- b. Select the host to which the port will be associated, and click **View/Edit Settings**.

The Host Settings dialog box appears.

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



- d. Click **Add**, and use the **Add Host Port** dialog box to associate a new host port identifier to the host.

The length of the host port identifier name is determined by the host interface technology. FC host port identifier names must have 16 characters. iSCSI host port identifier names have a maximum of 223 characters. The port must be unique. A port number that has already been configured is not allowed.

- e. Click **Delete**, and use the **Delete Host Port** dialog box to remove (unassociate) a host port identifier.

The **Delete** option does not physically remove the host port. This option removes the association between the host port and the host. Unless you remove the host bus adapter or the iSCSI initiator, the host port is still recognized by the controller.

- f. Click **Save** to apply your changes to the host port identifier settings.

- g. Repeat these steps to add and remove any additional host port identifiers.
5. Reboot the host or perform a rescan so that the host properly discovers the LUNs.
 6. Remount volumes or start using block volume.

What's next?

Your host protocol conversion is complete. You can resume normal operations.

Complete iSCSI to FC conversion

If you previously had iSCSI host ports and you converted to FC, you might need to modify your existing configuration to support FC. The following procedure is only applicable if no FC HIC is present.

This task applies only if you are converting a storage array that has already been in use.

This task does not apply if you are converting a new storage array that does not yet have hosts and volumes defined. If you converted the host-port protocol of a new storage array, see the [Cabling procedures](#) to install cables and SFPs. Then, follow the instructions in the [Linux express configuration](#), [Windows express configuration](#), or [VMware express configuration](#) to complete the setup for each protocol.

Steps

1. Install the HBA utility and determine initiator WWPNs.

2. Zone the switches.

Zoning the switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

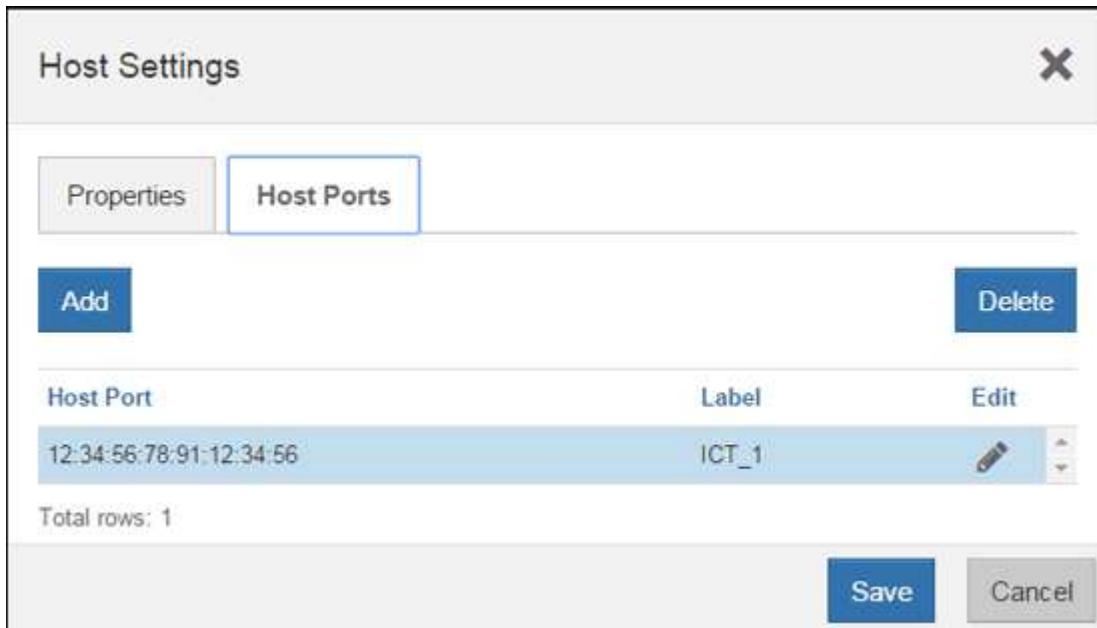
3. Update the host definitions in SANtricity System Manager.

- Select **Storage > Hosts**.

- Select the host to which the port will be associated, and click **View/Edit Settings**.

The Host Settings dialog box appears.

- Click the **Host Ports** tab.



- Click **Add**, and use the **Add Host Port** dialog box to associate a new host port identifier to the host.

The length of the host port identifier name is determined by the host interface technology. FC host port identifier names must have 16 characters. iSCSI host port identifier names have a maximum of 223 characters. The port must be unique. A port number that has already been configured is not allowed.

- Click **Delete**, and use the **Delete Host Port** dialog box to remove (unassociate) a host port identifier.

The **Delete** option does not physically remove the host port. This option removes the association between the host port and the host. Unless you remove the host bus adapter or the iSCSI initiator, the host port is still recognized by the controller.

- Click **Save** to apply your changes to the host port identifier settings.

- Repeat these steps to add and remove any additional host port identifiers.

4. Reboot the host or perform a rescan so that the host properly discovers mapped storage.

5. Remount volumes or start using block volume.

What's next?

Your host protocol conversion is complete. You can resume normal operations.

Complete conversion for IB-iSER to/from IB-SRP, NVMe over IB, NVMe over RoCE, or NVMe over FC

After you apply the feature pack key to convert the protocol used by your InfiniBand iSER HIC port to/from SRP, NVMe over InfiniBand, NVMe over RoCE, or NVMe over Fibre Channel, you need to configure the host to use the appropriate protocol.

Steps

1. Configure the host to use the SRP, iSER, or NVMe protocol.

For step-by-step instructions on how to configure the host to use SRP, iSER, or NVMe, see the [Linux express configuration](#).

2. To connect the host to the storage array for an SRP configuration, you must enable the InfiniBand driver stack with the appropriate options.

Specific settings might vary between Linux distributions. Check the [NetApp Interoperability Matrix](#) for specific instructions and additional recommended settings for your solution.

What's next?

Your host protocol conversion is complete. You can resume normal operations.

Manage storage

Use the links below to access documentation that describes how to configure, manage, and monitor storage objects and E-Series storage systems. The links take you to a different documentation site.

Online help for System Manager 11.7

Access the [SANtricity System Manager 11.7 online help](#), where you can find information about how to plan, configure, manage, and troubleshoot your storage array.

Online help for Unified Manager 5

Access the [SANtricity Unified Manager 5 online help](#), where you can learn how to execute storage management commands on multiple network storage arrays.

Command reference

Access the [Command reference](#), where you can learn how to configure and monitor your storage arrays using command line interface (CLI) commands.

Use SANtricity solutions

Web services proxy

SANtricity Web Services Proxy overview

The SANtricity Web Services Proxy is a RESTful API server installed separately on a host system to manage hundreds of new and legacy NetApp E-Series storage systems. The proxy includes SANtricity Unified Manager, which is a web-based interface that provides similar functions.

Installation overview

Installing and configuring the Web Services Proxy involves the following steps:

1. [Review installation and upgrade requirements](#).
2. [Download and install Web Services Proxy file](#).
3. [Log in to API and Unified Manager](#).
4. [Configure Web Services Proxy](#).

Find more information

- Unified Manager — The proxy installation includes SANtricity Unified Manager, a web-based interface that provides configuration access to newer E-Series and EF-Series storage systems. For more information, see the Unified Manager online help, which is available from its user interface or from the [Documentation Center](#).
- GitHub repository — GitHub contains a repository for the collection and organization of sample scripts illustrating the use of the NetApp SANtricity Web Services API. To access the repository, see [NetApp Webservices samples](#).
- Representational state transfer (REST) — Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities, so you should be familiar with REST concepts. For more information, see [Architectural Styles and the Design of Network-based Software Architectures](#).
- JavaScript Object Notation (JSON) — Because data within Web Services is encoded through JSON, you should be familiar with JSON programming concepts. For more information, see [Introducing JSON](#).

Learn about Web Services

Web Services and Unified Manager overview

Before you install and configure the Web Services proxy, read the overview of Web Services and SANtricity Unified Manager.

Web Services

Web Services is an Application Programming Interface (API) that allows you to configure, manage, and monitor NetApp E-Series and EF-Series storage systems. By issuing API requests, you can complete workflows such as configuration, provisioning, and performance monitoring for E-Series storage systems.

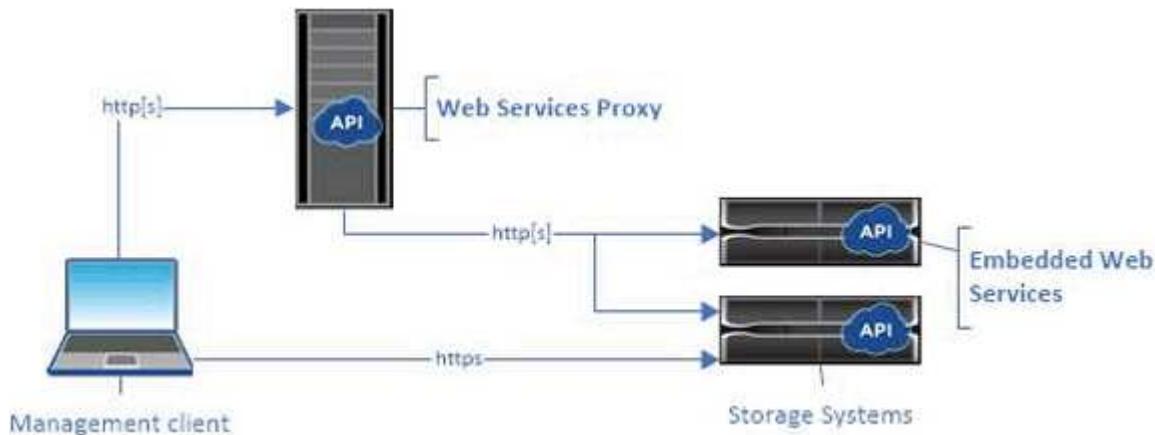
When using the Web Services API to manage storage systems, you should be familiar with the following:

- JavaScript Object Notation (JSON) – Because data within Web Services is encoded through JSON, you should be familiar with JSON programming concepts. For more information, see [Introducing JSON](#).
- Representational state transfer (REST) – Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities, so you should be familiar with REST concepts. For more information, see [Architectural Styles and the Design of Network-based Software Architectures](#).
- Programming language concepts – Java and Python are the most common programming languages used with the Web Services API, but any programming language that can make HTTP requests is sufficient for API interaction.

Web Services is available in two implementations:

- **Embedded** — A RESTful API server is embedded on each controller of an E2800/EF280 storage system running NetApp SANtricity 11.30 or later versions, an E5700/EF570 running SANtricity 11.40 or later versions, and an EF300 or EF600 running SANtricity 11.60 or later versions. No installation is required.
- **Proxy** — The SANtricity Web Services Proxy is a RESTful API server installed separately on a Windows or Linux server. This host-based application can manage hundreds of new and legacy NetApp E-Series storage systems. In general, you should use the proxy for networks with more than 10 storage systems. The proxy can handle numerous requests more efficiently than the embedded API.

The core of the API is available in both implementations.



The following table provides a comparison of the proxy and the embedded version.

| Consideration | Proxy | Embedded |
|---------------|---|---|
| Installation | Requires a host system (Linux or Windows). The proxy is available for download at the NetApp Support Site or on DockerHub . | No installation or enablement required. |

| Consideration | Proxy | Embedded |
|--------------------|---|---|
| Security | <p>Minimal security settings by default.</p> <p>Security settings are low so that developers can get started with the API quickly and easily. If desired, you can configure the proxy with the same security profile as the embedded version.</p> | <p>High security settings by default.</p> <p>Security settings are high because the API runs directly on the controllers. For example, it does not allow HTTP access, and it disables all SSL and older TLS encryption protocols for HTTPS.</p> |
| Central management | Manages all storage systems from one server. | Manages only the controller on which it is embedded. |

Unified Manager

The proxy installation package includes Unified Manager, a web-based interface that provides configuration access to newer E-Series and EF-Series storage systems, such as the E2800, E5700, EF300, and EF600.

From Unified Manager, you can perform the following batch operations:

- View the status of multiple storage systems from a central view
- Discover multiple storage systems in your network
- Import settings from one storage system to multiple systems
- Upgrade firmware for multiple storage systems

Compatibility and restrictions

The following compatibility and restrictions apply to using the Web Services Proxy.

| Consideration | Compatibility or restriction |
|------------------------------|--|
| HTTP support | The Web Services Proxy allows use of HTTP or HTTPS. (The embedded version of Web Services requires HTTPS for security reasons.) |
| Storage systems and firmware | The Web Services Proxy can manage all E-Series storage systems, including a mixture of older systems and the latest E2800, EF280, E5700, EF570, EF300, and EF600 series systems. |

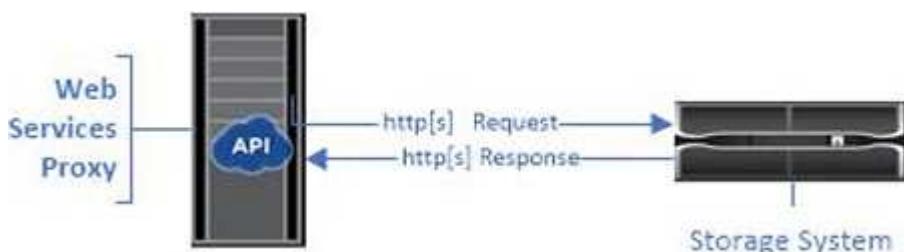
| Consideration | Compatibility or restriction |
|------------------------------|--|
| IP Support | <p>The Web Services Proxy supports either the IPv4 protocol or IPv6 protocol.</p> <p>(i) The IPv6 protocol might fail when the Web Services Proxy tries to automatically discover the management address from the controller configuration. Possible causes for the failure include problems during IP address forwarding or IPv6 being enabled on the storage systems but not on the server.</p> |
| NVSRAM file name constraints | <p>The Web Services Proxy uses NVSRAM file names to identify version information accurately. Therefore, you cannot change NVSRAM filenames when they are used with the Web Services Proxy. The Web Services Proxy might not recognize a renamed NVSRAM file as a valid firmware file.</p> |
| Symbol Web | <p>Symbol Web is a URL in the REST API. It provides access to almost all symbol calls. The symbol function is part of the following URL:</p> <pre data-bbox="817 1030 1449 1136">http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function</pre> <p>(i) Symbol-disabled storage systems are supported through the Web Services Proxy.</p> |

API basics

In the Web Services API, HTTP communications involve a request-response cycle.

URL elements in requests

Regardless of the programming language or tool used, each call to the Web Services API has a similar structure, with a URL, HTTP verb, and an Accept header.



All requests include a URL, as in the following example, and contain the elements described in the table.

`https://webservices.name.com:8443/devmgr/v2/storage-systems`

| Area | Description |
|---|---|
| HTTP transport <code>https://</code> | <p>The Web Services Proxy enables the use of HTTP or HTTPS.</p> <p>The embedded Web Services requires HTTPS for security reasons.</p> |
| Base URL and port <code>webservices.name.com:8443</code> | <p>Each request must be correctly routed to an active instance of Web Services. The FQDN (fully qualified domain name) or the IP address of the instance is required, along with the listening port. By default, Web Services communicates over port 8080 (for HTTP) and port 8443 (for HTTPS).</p> <p>For the Web Services Proxy, both ports can be changed during the proxy installation or in the <code>wsconfig.xml</code> file. Port contention is common on data center hosts running various management applications.</p> <p>For the embedded Web Services, the port on the controller cannot be changed; it defaults to port 8443 for secure connections.</p> |
| API path <code>devmgr/v2/storage-systems</code> | <p>A request is made to a specific REST resource or endpoint within the Web Services API. Most endpoints are in the form of:</p> <p><code>devmgr/v2/<resource>/[id]</code></p> <p>The API path consists of three parts:</p> <ul style="list-style-type: none">• <code>devmgr</code> (Device Manager) is the namespace of the Web Services API.• <code>v2</code> denotes the version of the API that you are accessing. You can also use <code>utils</code> to access login endpoints.• <code>storage-systems</code> is a category within the documentation. |

Supported HTTP verbs

Supported HTTP verbs include GET, POST, and DELETE:

- GET requests are used for read-only requests.
- POST requests are used to create and update objects, and also for read requests that might have security implications.

- DELETE requests are typically used to remove an object from management, remove an object entirely, or to reset the state of the object.



Currently, the Web Services API does not support PUT or PATCH. Instead, you can use POST to provide the typical functionality for these verbs.

Accept headers

When returning a request body, Web Services returns the data in JSON format (unless otherwise specified). Certain clients default to requesting “text/html” or something similar. In these cases, the API responds with an HTTP code 406, denoting that it cannot provide data in this format. As a best practice, you should define the Accept header as “application/json” for any cases in which you expect JSON as the response type. In other cases where a response body is not returned (for example, DELETE), providing the Accept header does not cause any unintended effects.

Responses

When a request is made to the API, a response returns two critical pieces of information:

- HTTP status code — Indicates whether the request was successful.
- Optional response body — Usually provides a JSON body representing the state of the resource or a body providing more details on the nature of a failure.

You must check the status code and the content-type header to determine what the resulting response body looks like. For HTTP status codes 200-203 and 422, Web Services returns a JSON body with the response. For other HTTP status codes, Web Services generally does not return an additional JSON body, either because the specification does not allow it (204) or because the status is self-explanatory. The table lists common HTTP status codes and definitions. It also indicates whether information associated with each HTTP code is returned in a JSON body.

| HTTP status code | Description | JSON body |
|-----------------------------------|---|-----------|
| 200 OK | Denotes a successful response. | Yes |
| 201 Created | Indicates that an object was created. This code is used in a few rare cases instead of a 200 status. | Yes |
| 202 Accepted | Indicates that the request is accepted for processing as an asynchronous request, but you must make a subsequent request to get the actual result. | Yes |
| 203 Non-Authoritative Information | Similar to a 200 response, but Web Services cannot guarantee that the data is up-to-date (for example, only cached data is available at this time). | Yes |

| HTTP status code | Description | JSON body |
|--------------------------|---|-----------|
| 204 No Content | Indicates a successful operation, but there is no response body. | No |
| 400 Bad Request | Indicates that the JSON body provided in the request is not valid. | No |
| 401 Unauthorized | Indicates that an authentication failure has occurred. Either no credentials were provided, or the username or password was invalid. | No |
| 403 Forbidden | An authorization failure, which indicates that the authenticated user does not have permission to access the requested endpoint. | No |
| 404 Not Found | Indicates that the requested resource could not be located. This code is valid for nonexistent APIs or nonexistent resources requested by the identifier. | No |
| 422 Unprocessable Entity | Indicates the request is generally well-formed, but either the input parameters are invalid, or the state of the storage system does not allow Web Services to satisfy the request. | Yes |
| 424 Failed Dependency | Used in the Web Services Proxy to indicate that the requested storage system is currently inaccessible. Therefore, Web Services cannot satisfy the request. | No |
| 429 Too Many Requests | Indicates that a request limit was exceeded and should be retried at a later time. | No |

Sample scripts

GitHub contains a repository for the collection and organization of sample scripts illustrating the use of the NetApp SANtricity Web Services API. To access the repository, see [NetApp Webservices samples](#).

Terms and concepts

The following terms apply to the Web Services Proxy.

| Term | Definition |
|----------------|--|
| API | An Application Programming Interface (API) is a set of protocols and methods that enables developers to communicate with devices. The Web Services API is used to communicate with E-Series storage systems. |
| ASUP | The AutoSupport (ASUP) feature collects data in a customer support bundle and automatically sends the message file to technical support for remote troubleshooting and problem analysis. |
| Endpoint | Endpoints are functions that are available through the API. An endpoint includes an HTTP verb, plus the URI path. In Web Services, endpoints can execute such tasks as discovering storage systems and creating volumes. |
| HTTP Verb | An HTTP verb is a corresponding action for an endpoint, such as retrieving and creating data. In Web Services, HTTP verbs include POST, GET, and DELETE. |
| JSON | JavaScript Object Notation (JSON) is a structured data format much like XML, which uses a minimal, readable format. Data within Web Services is encoded through JSON. |
| REST / RESTful | <p>Representational state transfer (REST) is a loose specification that defines an architectural style for an API. Because most REST APIs do not fully adhere to the specification, they are described as “RESTful” or “REST-like.” Generally, a “RESTful” API is agnostic to programming languages and has the following characteristics:</p> <ul data-bbox="845 1396 1493 1628" style="list-style-type: none"> • HTTP-based, which follows the general semantics of the protocol • Producer and consumer of structured data (JSON, XML, etc.) • Object-oriented (as opposed to operation-oriented) <p>Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities.</p> |
| storage system | A storage system is an E-Series array, which includes shelves, controllers, drives, software, and firmware. |

| Term | Definition |
|--------------|--|
| SYMbol API | SYMbol is a legacy API for managing E-Series storage systems. The underlying implementation of the Web Services API uses SYMbol. |
| Web Services | Web Services is an API that NetApp designed for developers to manage E-Series storage systems. There are two implementations of Web Services: embedded on the controller and a separate proxy that can be installed on Linux or Windows. |

Install and configure

Review installation and upgrade requirements

Before installing the Web Services Proxy, review the installation requirements and upgrade considerations.

Installation requirements

You can install and configure the Web Services Proxy on a Windows or Linux host system.

Proxy installation includes the following requirements.

| Requirement | Description |
|----------------------|---|
| Hostname limitations | Be sure that the hostname of the server where you plan to install the Web Services Proxy contains only ASCII letters, numerical digits, and hyphens (-). This requirement is due to a limitation of Java Keytool, which is used in generating a self-signed certificate for the server. If the hostname of your server contains any other characters, such as an underscore (_), the Webserver will fail to start after installation. |
| Operating systems | <p>You can install the proxy on the following operating systems:</p> <ul style="list-style-type: none"> • Linux • Windows <p>For a complete list of operating systems and firmware compatibility, see the NetApp Interoperability Matrix Tool.</p> |

| Requirement | Description |
|----------------------------------|---|
| Linux: Additional Considerations | Linux Standard Base libraries (init-functions) are required for the Webserver to function properly. You must install the lsb/insserv packages for your operating system. For more information, refer to the "Additional packages required" section of the Readme file. |
| Multiple instances | You can install only one instance of Web Services Proxy on a server; however, you can install the proxy on multiple servers within your network. |
| Capacity planning | <p>Web Services Proxy requires adequate space for logging. Make sure that your system meets the following available disk space requirements:</p> <ul style="list-style-type: none"> • Required installation space — 275 MB • Minimum logging space — 200 MB • System memory — 2 GB; heap space is 1 Gb by default <p>You can use a disk-space monitoring tool to verify available disk drive space for persistent storage and logging.</p> |
| License | The Web Services Proxy is a free, standalone product that does not require a license key. However, applicable copyrights and terms of service apply. If you are installing the proxy in either Graphical or Console mode, you must accept the End User License Agreement (EULA). |

Upgrade considerations

If you are upgrading from a previous version, be aware that some items are preserved or removed.

- For the Web Services Proxy, previous configuration settings are preserved. These settings include user passwords, all discovered storage systems, server certificates, trusted certificates, and server runtime configuration.
- For Unified Manager, all SANtricity OS files previously loaded in the repository are removed during the upgrade.

Download and install Web Services Proxy file

Installation involves downloading the file and then installing the proxy package on a Linux or Windows server.

Download Web Services Proxy files

You can download the installation file and the readme file from the Software download page of the NetApp Support site.

The download package includes the Web Services Proxy and the Unified Manager interface.

Steps

1. Go to [NetApp Support - Downloads](#).
2. Select **E-Series SANtricity Web Services Proxy**.
3. Follow the instructions to download the file. Make sure you select the correct download package for your server (for example, EXE for Windows; BIN or RPM for Linux).
4. Download the installation file to the server where you want to install the proxy and Unified Manager.

Install on Windows or Linux server

You can install the Web Services Proxy and Unified Manager using one of three modes (Graphical, Console, or Silent), or by using an RPM file (Linux only).

Before you begin

- [Review installation requirements](#).
- Make sure you have downloaded the correct installation file (EXE for Windows; BIN for Linux) to the server where you want to install the proxy and Unified Manager.

Graphical mode install

You can run the installation in Graphical mode for either Windows or Linux. In Graphical mode, the prompts appear in a Windows-style interface.

Steps

1. Access the folder where you downloaded the installation file.
2. Launch the installation for either Windows or Linux, as follows:

- Windows — Double-click the installation file:

```
santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe
```

- Linux — Run the following command:

```
santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin
```

In the above filenames, nn.nn.nn.nnnn represents the version number.

The installation process starts and the NetApp SANtricity Web Services Proxy + Unified Manager splash screen appears.

3. Follow the on-screen prompts.

During the installation, you are prompted to enable several features and enter some configuration parameters. If necessary, you can change any of these selections later in the configuration files.

4. When the Webserver Started message appears, click **OK** to complete the installation.

The Install Complete dialog box appears.

5. Click the check boxes if you want to launch Unified Manager or the interactive API documentation, and then click **Done**.

Console mode install

You can run the installation in Console mode for either Windows or Linux. In Console mode, the prompts appear in the terminal window.

Steps

1. Run the following command: <install filename> -i console

In the above command, <install filename> represents the name of the proxy installation file you downloaded (for example: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).



To cancel the installation at any time during the installation process, type **QUIT** at the command prompt.

The installation process starts and the Launching Installer — Introduction message appears.

2. Follow the on-screen prompts.

During the installation, you are prompted to enable several features and enter some configuration parameters. If necessary, you can change any of these selections later in the configuration files.

3. When the installation is complete, press **Enter** to exit the installer.

Silent mode install

You can run the installation in Silent mode for either Windows or Linux. In Silent mode, no return messages or scripts appear in the terminal window.

Steps

1. Run the following command: <install filename> -i silent

In the above command, <install filename> represents the name of the proxy installation file you downloaded (for example: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Press **Enter**.

The installation process can take several minutes to complete. After successful installation, a command prompt appears in the terminal window.

RPM command install (Linux only)

For Linux systems that are compatible with the RPM package management system, you can install the Web Services Proxy using an optional RPM file.

Steps

1. Download the RPM file to the server where you want to install the proxy and Unified Manager.
2. Open a terminal window.

3. Enter the following command:

```
rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
```



In the above command, `nn.nn.nn.nnnn` represents the version number.

The installation process can take several minutes to complete. After successful installation, a command prompt appears in the terminal window.

Log in to API and Unified Manager

Web Services includes API documentation, which enables you to directly interact with the REST API. It also includes Unified Manager, a browser-based interface for managing multiple E-Series storage systems.

Log in to Web Services API

After you install the Web Services Proxy, you can access the interactive API documentation in a browser.

The API documentation runs with each instance of Web Services, and is also available in a static PDF format from the NetApp Support site. To access the interactive version, you open a browser and enter the URL pointing to where Web Services resides (either a controller for the embedded version or a server for the proxy).



The Web Services API implements the OpenAPI specification (originally called the Swagger specification).

For initial login, you use the "admin" credentials. "Admin" is considered a super administrator with access to all functions and roles.

Steps

1. Open a browser.
2. Enter the URL for the embedded or proxy implementation:

- ° Embedded: `https://<controller>:<port>/devmgr/docs/`

In this URL, `<controller>` is the IP address or FQDN of the controller, and `<port>` is the management port number of the controller (defaults to 8443).

- ° Proxy: `http[s]://<server>:<port>/devmgr/docs/`

In this URL, `<server>` is the IP address or FQDN of the server where the proxy is installed, and `<port>` is the listening port number (defaults to 8080 for HTTP or 8443 for HTTPS).



If the listening port is already in use, the proxy detects the conflict and prompts you to choose a different listening port.

The API documentation opens in the browser.

3. When the interactive API documentation opens, go to the drop-down menu in the upper right of the page and select **utils**.

4. Click the **Login** category to see the available endpoints.
5. Click the **POST: /login** endpoint, and then click **Try it out**.
6. For first-time login, enter admin for the username and password.
7. Click **Execute**.
8. To access the endpoints for storage management, go to the drop-down menu in the upper right and select **v2**.

The high-level categories for endpoints are displayed. You can navigate the API documentation as described in the table.

| Area | Description |
|----------------|---|
| Drop-down menu | <p>At the upper right of the page, a drop-down menu provides options for switching between version 2 of the API documentation (V2), the SYMbolic interface (SYMbolic V2), and API utilities (utils) for logging in.</p> <p> Because version 1 of the API documentation was a prerelease and not generally available, V1 is not included in the drop-down menu.</p> |
| Categories | <p>The API documentation is organized by high-level categories (for example: Administration, Configuration). Click on a category to see the related endpoints.</p> |
| Endpoints | <p>Select an endpoint to see its URL paths, required parameters, response bodies, and status codes that the URLs are likely to return.</p> |
| Try It Out | <p>Interact with the endpoint directly by clicking Try It Out. This button is provided in each of the expanded views for endpoints.</p> <p>When you click the button, fields appear for entering parameters (if applicable). You can then enter values and click Execute.</p> <p>The interactive documentation uses JavaScript to make the request directly to the API; it is not a test request.</p> |

Log in to Unified Manager

After you install the Web Services Proxy, you can access Unified Manager to manage multiple storage systems in a web-based interface.

To access Unified Manager, you open a browser and enter the URL pointing to where the proxy is installed. The following browsers and versions are supported.

| Browser | Minimum version |
|-----------------------------|-----------------|
| Google Chrome | 79 |
| Microsoft Internet Explorer | 11 |
| Microsoft Edge | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |

Steps

1. Open a browser and enter the following URL:

```
http[s]://<server>:<port>/um
```

In this URL, <server> represents the IP address or FQDN of the server where the Web Services Proxy is installed, and <port> represents the listening port number (defaults to 8080 for HTTP or 8443 for HTTPS).

The Unified Manager login page opens.

2. For first-time login, enter `admin` for the user name, and then set and confirm a password for the admin user.

The password can include up to 30 characters. For further information about users and passwords, see the Access Management section of the Unified Manager online help.

Configure Web Services Proxy

You can modify the Web Services Proxy settings to meet the unique operating and performance requirements for your environment.

Stop or restart the Webserver

The Webserver service is started during installation and runs in the background. During some configuration tasks, you might need to stop or restart the Webserver service.

Steps

1. Do one of the following:

- For Windows, go to the **Start** menu, select **Administrative Tools > Services**, locate **NetApp SANtricity Web Services** and then select either **Stop** or **Restart**.
- For Linux, choose the method of stopping and restarting the Webserver for your operating system version. During the installation, a popup dialog indicated what daemon started. For example:

```
web_services_proxy webserver installed and started. You can interact with it
using systemctl start|stop|restart|status web_services_proxy.service
```

The most common method for interacting with the service is by using `systemctl` commands.

Resolve port conflicts

If the Web Services Proxy is running while another application is available at the defined address or port, you can resolve the port conflict in the wsconfig.xml file.

Steps

1. Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Add the following line to the wsconfig.xml file, in which *n* is the port number:

```
<sslport clientauth="request">*n*</sslport>
<port>n</port>
```

The following table shows the attributes that control HTTP ports and HTTPS ports.

| Name | Description | Parent Node | Attributes | Required |
|---------|--|-------------|--|----------|
| config | The root node for the config | Null | Version - The version of the config schema is currently 1.0. | Yes |
| sslport | The TCP port to listen for SSL requests. Defaults to 8443. | config | Clientauth | No |
| port | The TCP port to listen for HTTP request, defaults to 8080. | config | - | No |

3. Save and close the file.
4. Restart the Webserver service so the change takes effect.

Configure load-balancing and/or high-availability

To use the Web Services Proxy in a highly-available (HA) configuration, you can configure load balancing. In an HA configuration, typically either a single node receives all requests while the others are on stand-by, or requests are load-balanced across all nodes.

The Web Services Proxy can exist in a highly-available (HA) environment, with most APIs operating correctly regardless of the recipient of the request. Metadata tags and folders are two exceptions, because tags and folders are stored in a local database and are not shared between Web Services Proxy instances.

However, there are some known timing issues that occur in a small percentage of requests. Specifically, one instance of the proxy can have newer data faster than a second instance for a small window. The Web Services Proxy includes a special configuration that removes this timing issue. This option is not enabled by

default, because it increases the amount of time it takes to service requests (for data consistency). To enable this option, you must add a property to an .INI file (for Windows) or an .SH file (for Linux).

Steps

1. Do one of the following:

- Windows: Open the appserver64.ini file, and then add the `Dload-balance.enabled=true` property.

For example: `vmarg -Dload-balance.enabled=true`

- Linux: Open the webserver.sh file, and then add the `Dload-balance.enabled=true` property.

For example: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Save your changes.

3. Restart the Webserver service so the change takes effect.

Disable SYMbol HTTPS

You can disable SYMbol commands (default setting) and send commands over a remote procedure call (RPC). This setting can be changed in the wsconfig.xml file.

By default, the Web Services Proxy sends SYMbol commands over HTTPS for all E2800 series and E5700 series storage systems running SANtricity OS versions 08.40 or later. SYMbol commands sent over HTTPS are authenticated to the storage system. If needed, you can disable HTTPS SYMbol support and send commands over RPC. Whenever SYMbol over RPC is configured, all passive commands to the storage system are enabled without authentication.



When SYMbol over RPC is used, the Web Services Proxy cannot connect to systems with the SYMbol management port disabled.

Steps

1. Open the wsconfig.xml file, located at:

- (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy`
- (Linux) — `/opt/netapp/santricity_web_services_proxy`

2. In the `devicemgt.symbolclientstrategy` entry, replace the `httpsPreferred` value with `rpcOnly`.

For example:

```
<env key="devicemgt.symbolclientstrategy">rpcOnly</env>
```

3. Save the file.

Configure cross-origin resource sharing

You can configure cross-origin resource sharing (CORS), which is a mechanism that uses additional HTTP headers to provide a web application running at one origin to have permission to access selected resources from a server at a different origin.

CORS is handled by the cors.cfg file located in the working directory. The CORS configuration is open by default, so cross domain access is not restricted.

If no configuration file is present, CORS is open. But if the cors.cfg file is present, then it is used. If the cors.cfg file is empty, you cannot make a CORS request.

Steps

1. Open the cors.cfg file, which is located in the working directory.
2. Add the desired lines to the file.

Each line in the CORS configuration file is a regular expression pattern to match. The origin header must match a line in the cors.cfg file. If any line pattern matches the origin header, the request is allowed. The complete origin is compared, not just the host element.

3. Save the file.

Requests are matched on the host and according to protocol, such as the following:

- Match localhost with any protocol — *localhost*
- Match localhost for HTTPS only — https://localhost*

Uninstall Web Services Proxy

To remove the Web Services Proxy and Unified Manager, you can use any mode (Graphical, Console, Silent, or RPM file), regardless of what method you used to install the proxy.

Graphical mode uninstall

You can run the uninstall in Graphical mode for either Windows or Linux. In Graphical mode, the prompts appear in a Windows-style interface.

Steps

1. Launch the uninstall for either Windows or Linux, as follows:

- Windows — Go to the directory that contains the `uninstall_web_services_proxy` uninstall file. The default directory is at the following location: `C:/Program Files/NetApp/SANtricity Web Services Proxy/`. Double-click `uninstall_web_services_proxy.exe`.



Alternatively, you can go to **Control Panel > Programs > Uninstall a program**, and then select "NetApp SANtricity Web Services Proxy."

- Linux — Go to the directory that contains the Web Services Proxy uninstall file. The default directory is at the following location:

```
/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy
```

2. Run the following command:

```
uninstall_web_services_proxy -i gui
```

The SANtricity Web Services Proxy splash screen appears.

3. From the Uninstall dialog box, click **Uninstall**.

The Uninstaller progress bar appears and shows the progress.

4. When the Uninstall Complete message appears, click **Done**.

Console mode uninstall

You can run the uninstall in Console mode for either Windows or Linux. In Console mode, the prompts appear in the terminal window.

Steps

1. Go to the `uninstall_web_services_proxy` directory.
2. Run the following command:

```
uninstall_web_services_proxy -i console
```

The uninstall process starts.

3. When the uninstall is complete, press **Enter** to exit the installer.

Silent mode uninstall

You can run the uninstall in Silent mode for either Windows or Linux. In Silent mode, no return messages or scripts appear in the terminal window.

Steps

1. Go to the `uninstall_web_services_proxy` directory.
2. Run the following command:

```
uninstall_web_services_proxy -i silent
```

The uninstall process runs, but no return messages or scripts appear in the terminal window. After Web Services Proxy is successfully uninstalled, a command prompt appears in the terminal window.

RPM command uninstall (Linux only)

You can use an RPM command to uninstall the Web Services Proxy from a Linux system.

Steps

1. Open a terminal window.
2. Enter the following command line:

```
rpm -e santricity_webservices
```



The uninstall process might leave files that were not part of the original installation. Manually delete these files to remove Web Services Proxy completely.

Manage user access in Web Services Proxy

You can manage user access to the Web Services API and Unified Manager for security purposes.

Overview of access management

Access management includes role-based logins, password encryption, basic authentication, and LDAP integration.

Role-based access

Role-based access control (RBAC) associates predefined users with roles. Each role grants permissions to a specific level of functionality.

The following table describes each role.

| Role | Description |
|-----------------|--|
| security.admin | SSL and certificate management. |
| storage.admin | Full read/write access to storage system configuration. |
| storage.monitor | Read-only access to view storage system data. |
| support.admin | Access to all hardware resources on storage systems and support operations such as AutoSupport (ASUP) retrieval. |

Default user accounts are defined in the users.properties file. You can change user accounts by directly modifying the users.properties file or by using the Access Management functions in Unified Manager.

The following table lists the user logins available for the Web Services Proxy.

| Predefined user login | Description |
|-----------------------|--|
| admin | A super administrator who has access to all functions and includes all roles. For Unified Manager, you must set the password on first-time login. |
| storage | The administrator responsible for all storage provisioning. This user includes the following roles: storage.admin, support.admin, and storage.monitor. This account is disabled until a password is set. |
| security | The user responsible for security configuration. This user includes the following roles: security.admin and storage.monitor. This account is disabled until a password is set. |
| support | The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: support.admin and storage.monitor. This account is disabled until a password is set. |

| Predefined user login | Description |
|-----------------------|---|
| monitor | A user with read-only access to the system. This user includes only the storage.monitor role. This account is disabled until a password is set. |
| rw | The rw (read/write) user includes the following roles: storage.admin, support.admin, and storage.monitor. This account is disabled until a password is set. |
| ro | The ro (read only) user includes only the storage.monitor role. This account is disabled until a password is set. |

Password encryption

For each password, you can apply an additional encryption process using the existing SHA256 password encoding. This additional encryption process applies a random set of bytes to each password (salt) for each SHA256 hash encryption. Salted SHA256 encryption is applied to all newly created passwords.



Prior to the Web Services Proxy 3.0 release, passwords were encrypted through SHA256 hashing only. Any existing SHA256 hash-only encrypted passwords retain this encoding and are still valid under the users.properties file. However, SHA256 hash-only encrypted passwords are not as secure as those passwords with salted SHA256 encryption.

Basic authentication

By default, basic authentication is enabled, which means the server returns a basic authentication challenge. This setting can be changed in the wsconfig.xml file.

LDAP

Lightweight Directory Access Protocol (LDAP), an application protocol for accessing and maintaining distributed directory information services, is enabled for the Web Services Proxy. LDAP integration allows for user authentication and mapping of roles to groups.

For information on configuring LDAP functionality, refer to configuration options in the Unified Manager interface or in the LDAP section of the interactive API documentation.

Configure user access

You can manage user access by applying additional encryption to passwords, setting basic authentication, and defining role-based access.

Apply additional encryption to passwords

For the highest level of security, you can apply additional encryption to passwords using the existing SHA256 password encoding.

This additional encryption process applies a random set of bytes to each password (salt) for each SHA256 hash encryption. Salted SHA256 encryption is applied to all newly created passwords.

Steps

1. Open the users.properties file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
 - (Linux) — /opt/netapp/santricity_web_services_proxy/data/config
2. Re-enter the encrypted password as plain text.
3. Run the securepasswds command line utility to re-encrypt the password or simply restart the Web Services Proxy. This utility is installed in the root install directory for the Web Services Proxy.



Alternatively, you can salt and hash local user passwords whenever password edits are performed through the Unified Manager.

Configure basic authentication

By default basic authentication is enabled, which means the server returns a basic authentication challenge. If desired, you can change that setting in the wsconfig.xml file.

1. Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Modify the following line in the file by specifying false (not enabled) or true (enabled).

For example: <env key="enable-basic-auth">true</env>

3. Save the file.
4. Restart the Webserver service so the change takes effect.

Configure role-based access

To limit user access to specific functions, you can modify which roles are specified for each user account.

The Web Services Proxy includes role-based access control (RBAC), in which roles are associated with predefined users. Each role grants permissions to a specific level of functionality. You can change the roles assigned to user accounts by directly modifying the users.properties file.



You can also change user accounts by using Access Management in Unified Manager. For more information, see the online help available with Unified Manager.

Steps

1. Open the users.properties file, located in:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
 - (Linux) — /opt/netapp/santricity_web_services_proxy/data/config
2. Locate the line for the user account you want to modify (storage, security, monitor, support, rw, or ro).



Do not modify the admin user. This is a super user with access to all functions.

3. Add or remove the specified roles, as desired.

Roles include:

- security.admin — SSL and certificate management.
- storage.admin — Full read/write access to storage system configuration.
- storage.monitor — Read-only access to view storage system data.
- support.admin — Access to all hardware resources on storage systems and support operations such as AutoSupport (ASUP) retrieval.



The storage.monitor role is required for all users, including the administrator.

4. Save the file.

Manage security and certificates in Web Services Proxy

For security in the Web Services Proxy, you can specify an SSL port designation and you can manage certificates. Certificates identify website owners for secure connections between clients and servers.

Enable SSL

The Web Services Proxy uses Secure Sockets Layer (SSL) for security, which is enabled during installation. You can change the SSL port designation in the wsconfig.xml file.

Steps

1. Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Add or change the SSL port number, similar to the following example:

```
<sslport clientauth="request">8443</sslport>
```

Result

When the server is started with SSL configured, the server looks for the keystore and truststore files.

- If the server does not find a keystore, the server uses the IP address of the first detected non-loopback IPv4 address to generate a keystore and then add a self-signed certificate to the keystore.
- If the server does not find a truststore, or the truststore is not specified, the server uses the keystore as the truststore.

Bypass certificate validation

To support secure connections, the Web Services Proxy validates the storage systems' certificates against its own trusted certificates. If needed, you can specify that the proxy bypass that validation before connecting to the storage systems.

Before you begin

- All storage system connections must be secure.

Steps

1. Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Enter true in the trust.all.arrays entry, as shown in the example:

```
<env key="trust.all.arrays">true</env>
```

3. Save the file.

Generate and import a host management certificate

Certificates identify website owners for secure connections between clients and servers. To generate and import Certificate Authority (CA) certificates for the host system where the Web Services Proxy is installed, you can use API endpoints.

To manage certificates for the host system, you perform the following tasks using the API:

- Create a certificate signing request (CSR) for the host system.
- Send the CSR file to a CA, and then wait for them to send you the certificate files.
- Import the signed certificates to the host system.



You can also manage certificates in the Unified Manager interface. For more information, see the online help available in Unified Manager.

Steps

1. Log in to the [interactive API documentation](#).
2. Go to the drop-down menu in the upper right and then select **v2**.
3. Expand the **Administration** link and scroll down to the **/certificates** endpoints.
4. Generate the CSR file:
 - a. Select **POST:/certificates**, and then select **Try it out**.

The web server regenerates a self-signed certificate. You can then enter information in the fields to define the common name, organization, organization unit, alternate ID, and other information used to generate the CSR.

- b. Add the required information in the **Example values** pane to generate a valid CA certificate, and then execute the commands.



Do not call **POST:/certificates** or **POST:/certificates/reset** again, or you must regenerate the CSR. When you call **POST:/certificates** or **POST:/certificates/reset**, you are generating a new self-signed certificate with a new private key. If you send a CSR that was generated before the last reset of the private key on the server, the new security certificate does not work. You must generate a new CSR and request a new CA certificate.

- c. Execute the **GET:/certificates/server** endpoint to confirm that the current certificate status is the self-signed certificate with the information added from the **POST:/certificates** command.

The server certificate (denoted by the alias `jetty`) is still self-signed at this point.

- d. Expand the **POST:/certificates/export** endpoint, select **Try it out**, enter a file name for the CSR file, and then click **Execute**.
5. Copy and paste the `fileUrl` into a new browser tab to download the CSR file, and then send the CSR file to a valid CA to request a new web server certificate chain.
6. When the CA issues a new certificate chain, use a certificate manager tool to break out the root, intermediate, and web server certificates, and then import them to the Web Services Proxy server:
 - a. Expand the **POST:/sslconfig/server** endpoint and select **Try it out**.
 - b. Enter a name for the CA root certificate in the **alias** field.
 - c. Select **false** in the **replaceMainServerCertificate** field.
 - d. Browse to and select the new CA root certificate.
 - e. Click **Execute**.
 - f. Confirm that the certificate upload was successful.
 - g. Repeat the CA certificate upload procedure for the CA intermediate certificate.
 - h. Repeat the certificate upload procedure for the new web server security certificate file, except in this step, select **true** on the **replaceMainServerCertificate** drop-down.
 - i. Confirm that the web server security certificate import was successful.
 - j. To confirm that the new root, intermediate, and web server certificates are available in the keystore, run **GET:/certificates/server**.
7. Select and expand the **POST:/certificates/reload** endpoint, and then select **Try it out**. When prompted, whether you want to restart both controllers or not, select **false**. ("True" applies only in the case of dual array controllers.) Click **Execute**.

The **/certificates/reload** endpoint usually returns a successful http 202 response. However, the reload of the web server truststore and keystore certificates does create a race condition between the API process and the web server certificate reload process. In rare cases, the web server certificate reload can beat the API processing. In this case, the reload appears to fail even though it completed successfully. If this occurs, continue to the next step anyway. If the reload actually failed, the next step also fails.

8. Close the current browser session to the Web Services Proxy, open a new browser session, and confirm that a new secure browser connection to the Web Services Proxy can be established.

By using an incognito or in-private browsing session, you can open a connection to the server without using any saved data from previous browsing sessions.

Manage storage systems using Web Services Proxy

To manage storage systems in the network, you must first discover them and then add them to the management list.

Discover storage systems

You can set automatic discovery or manually discover storage systems.

Automatically discover storage systems

You can specify that storage systems are automatically discovered in the network by modifying the settings in the wsconfig.xml file. By default, IPv6 automatic discovery is disabled and IPv4 is enabled.

You only need to provide one management IP or DNS address to add a storage system. The server automatically discovers all management paths when the paths are either not configured or the paths are configured and rotatable.

 If you attempt to use an IPv6 protocol to automatically discover storage systems from the controller configuration after an initial connection has been made, the process might fail. Possible causes for the failure include problems during IP address forwarding or IPv6 being enabled on the storage systems, but not being enabled on the server.

Before you begin

Before enabling IPv6 discovery settings, verify that your infrastructure supports IPv6 connectivity to the storage systems to mitigate any connection issues.

Steps

1. Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
2. In the autodiscover strings, change settings from `true` to `false`, as desired. See the following example.

```
<env key="autodiscover.ipv6.enable">true</env>
```



When the paths are configured, but not configured so that the server can route to the addresses, intermittent connection errors happen. If you cannot set the IP addresses to be routable from the host, turn off auto discovery (change the settings to `false`).

3. Save the file.

Discover and add storage systems using API endpoints

You can use API endpoints to discover and add storage systems to the managed list. This procedure creates a management connection between the storage system and the API.

 This task describes how to discover and add storage systems using the REST API, so you can manage these systems in the interactive API documentation. However, you might want to manage storage systems in the Unified Manager instead, which provides an easy-to-use interface. For more information, see the online help available with Unified Manager.

Before you begin

For storage systems with SANtricity versions 11.30 and later, the legacy management interface for SYMBOL must be enabled in the SANtricity System Manager interface. Otherwise, the Discovery endpoints fail. You can find this setting by opening System Manager, and then going to **Settings > System > Additional Settings > Change Management Interface**.

Steps

1. Log in to the [interactive API documentation](#).

2. Discover storage systems, as follows:

- a. From the API documentation, make sure **V2** is selected in the drop-down, and then expand the **Storage-Systems** category.
- b. Click the **POST: /discovery** endpoint, and then click **Try it out**.
- c. Enter the parameters as described in the table.

| | |
|-------------------|---|
| startIP | Replace string with the starting and ending IP address range for one or more storage systems in the network. |
| endIP | |
| useAgents | Set this value to either: <ul style="list-style-type: none">• true = Use in-band agents for the network scan.• false = Do not use in-band agents for the network scan. |
| connectionTimeout | Enter the seconds allowed for the scan before the connection times out. |
| maxPortsToUse | Enter a maximum number of ports used for the network scan. |

- d. Click **Execute**.



API actions execute without user prompts.

The discovery process runs in the background.

- e. Make sure the code returns a 202.
- f. Under **Response Body**, locate the value returned for the requestId. You need the Request ID to view the results in the next step.

3. View discovery results, as follows:

- a. Click the **GET: /discovery** endpoint, and then click **Try it out**.
- b. Enter the Request ID from the previous step. If you leave the **Request ID** blank, the endpoint defaults to the last request ID executed.
- c. Click **Execute**.
- d. Make sure the code returns 200.
- e. In the response body, locate your Request ID and the strings for storageSystems. The strings look similar to the following example:

```

"storageSystems": [
    {
        "serialNumber": "123456789",
        "wwn": "000A011000AF000000000001A0C000E",
        "label": "EF570_Array",
        "firmware": "08.41.10.01",
        "nvssram": "N5700-841834-001",
        "ipAddresses": [
            "10.xxx.xx.213",
            "10.xxx.xx.214"
        ],
    },
]

```

f. Write down the values for wwn, label, and ipAddresses. You need them for the next step.

4. Add storage systems, as follows:

- Click the **POST: /storage-system** endpoint, and then click **Try it out**.
- Enter the parameters as described in the table.

| | |
|----------------------------|--|
| id | Enter a unique name for this storage system. You can enter the label (displayed in the response for GET: /discovery), but the name can be any string you choose. If you do not provide a value for this field, Web Services automatically assigns a unique identifier. |
| controllerAddresses | Enter the IP addresses displayed in the response for GET: /discovery. For dual controllers, separate the IP addresses with a comma. For example: "IP address 1", "IP address 2" |
| validate | Enter true , so you can receive confirmation that Web Services can connect to the storage system. |
| password | Enter the administrative password for the storage system. |
| wwn | Enter the WWN of the storage system (displayed in the response for GET: /discovery). |

- Remove all strings after "enableTrace": true, so that the entire string set is similar to the following example:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP", "Controller-B-Mgmt_IP"
  ],
  "validate": true,
  "password": "array-admin-password",
  "wwn": "000A011000AF000000000001A0C000E",
  "enableTrace": true
}
```

d. Click **Execute**.

e. Make sure the code response is 201, which indicates that the endpoint executed successfully.

The **Post: /storage-systems** endpoint is queued. You can view the results using the **GET: /storage-systems** endpoint in the next step.

5. Confirm the list addition, as follows:

a. Click the **GET: /storage-system** endpoint.

No parameters are required.

b. Click **Execute**.

c. Make sure that the code response is 200, which indicates that the endpoint executed successfully.

d. In the response body, look for the storage system details. The returned values indicate that it was successfully added to the list of managed arrays, similar to the following example:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ]
  }
]
```

Scale up the number of managed storage systems

By default, the API can manage up to 100 storage systems. If you need to manage more, you must bump the memory requirements for the server.

The server is set to use 512 MB of memory. For every 100 extra storage systems in your network, add 250 MB to that number. Do not add more memory than what you physically have. Allow enough extra for your operating system and other applications.

 The default cache size is 8,192 events. The approximate data usage for the MEL events cache is 1MB for each 8,192 events. Therefore, by retaining the defaults, cache usage should be approximately 1MB for a storage system.

 In addition to memory, the proxy uses network ports for each storage system. Linux and Windows consider network ports as file handles. As a security measure, most operating systems limit the number of open file handles that a process or a user can have open at one time. Especially in Linux environments, where open TCP connections are considered to be file handles, the Web Services Proxy can easily exceed this limit. Because the fix is system dependent, you should refer to your operating system's documentation for how to raise this value.

Steps

1. Do one of the following:
 - On Windows, go to the appserver64.init file. Locate the line, `vmarg .3=-Xmx512M`
 - On Linux, go to the webserver.sh file. Locate the line, `JAVA_OPTIONS="-Xmx512M"`
2. To increase the memory, replace 512 with the desired memory in MB.
3. Save the file.

Manage automatic polling for Web Services Proxy statistics

You can configure automatic polling for all disk and volume statistics on discovered storage systems.

Overview of statistics

Statistics provide information about the data collection rates and performance of the storage systems.

The Web Services Proxy provides access to the following types of statistics:

- Raw statistics — Total counters for data points at the time of data collection. Raw statistics can be used for total read operations or total write operations.
- Analyzed statistics — Calculated information for an interval. Examples of analyzed statistics are read input/output operations (IOPs) per second or write throughput.

Raw statistics are linear, typically requiring at least two collected data points to derive usable data from them. The analyzed statistics are a derivation of the raw statistics, which provide important metrics. Many values that can be derived from the raw statistics are shown in a usable, point-in-time format in the analyzed statistics for your convenience.

You can retrieve raw statistics regardless of whether the automatic polling is enabled or not. You can add the

`usecache=true` query string to the end of the URL to retrieve cached statistics from the last poll. Using cached results greatly increases the performance of statistics retrieval. However, multiple calls at a rate equal to or less than the configured polling interval cache retrieves the same data.

Statistics functionality

The Web Services Proxy provides API endpoints that enable the retrieval of raw and analyzed controller and interface statistics from supported hardware models and software versions.

Raw Statistics APIs

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

Analyzed Statistics APIs

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

These URLs retrieve analyzed statistics from the last poll and are only available when polling is enabled. These URLs include the following input-output data:

- Operations per second
- Throughput in megabytes per second
- Response times in milliseconds

The calculations are based on the differences between statistical polling iterations, which are the most common measures of storage performance. These statistics are preferable to unanalyzed statistics.



When the system starts, there is no previous statistics collection to use to calculate the various metrics, so analyzed statistics require at least one polling cycle after startup to return data. In addition, if the cumulative counters are reset, the next polling cycle will have unpredictable numbers for the data.

Configure polling intervals

To configure polling intervals, you modify the `wsconfig.xml` file to specify a polling interval in seconds.



Because the statistics are cached in memory, you might see an increase of about 1.5 MB of memory-use for each storage system.

Before you begin

- The storage systems must be discovered by the proxy.

Steps

- Open the wsconfig.xml file, located at:
 - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_services_proxy
- Add the following line inside the <env-entries> tag, in which *n* is the number of seconds for the interval between polling requests:

```
<env key="stats.poll.interval">n</env>
```

For example, if 60 is entered, polling starts at 60-second intervals. That is, the system requests polling to start 60 seconds after the prior polling period was completed (regardless of the duration of the prior polling period). All statistics are time-stamped with the exact time they were retrieved. The system uses the time stamp or time difference on which to base the 60-second calculation.

- Save the file.

Manage AutoSupport using Web Services Proxy

You can configure AutoSupport (ASUP), which collects data and then automatically sends that data to technical support for remote troubleshooting and problem analysis.

Overview of AutoSupport (ASUP)

The AutoSupport (ASUP) feature automatically transmits messages to NetApp based on manual and schedule-based criteria.

Each AutoSupport message is a collection of log files, configuration data, state data, and performance metrics. By default, AutoSupport transmits the files listed in the following table to the NetApp Support team once each week.

| File Name | Description |
|----------------------|---|
| x-headers-data.txt | A .txt file containing the X-header information. |
| manifest.xml | An .xml file detailing the contents of the message. |
| arraydata.xml | An .xml file containing the list of client persisted data. |
| appserver-config.txt | A .txt file containing application server configuration data. |
| wsconfig.txt | A .txt file containing the web service configuration data. |

| File Name | Description |
|--------------------------|--|
| host-info.txt | A .txt file containing information about the host environment. |
| server-logs.7z | A .7z file containing every available webserver log file. |
| client-info.txt | A .txt file with arbitrary key/value pairs for application-specific counters such as method and webpage hits. |
| webservices-profile.json | <p>These files contain Webservices profile data and Jersey monitoring statistical data. By default, Jersey monitoring statistics are enabled. You can enable and disable them in the wsconfig.xml file, as follows:</p> <ul style="list-style-type: none"> • Enable: <env key="enable.jersey.statistics">true</env> • Disable: <env key="enable.jersey.statistics">false</env> |

Configure AutoSupport

AutoSupport is enabled by default at installation; however, you can change that setting or modify the delivery types.

Enable or disable AutoSupport

The AutoSupport feature is enabled or disabled during the initial installation of the Web Services Proxy, but you can change that setting in the ASUPConfig file.

You can enable or disable AutoSupport through the ASUPConfig.xml file, as described in the steps below. Alternatively, you can enable or disable this feature through the API using **Configuration** and **POST/asup**, and then entering "true" or "false."

1. Open the ASUPConfig.xml file in the working directory.
2. Locate the lines for <asupdata enabled="(Boolean)" timestamp=>
3. Enter true (enable) or false (disable). For example:

```
<asupdata enabled="false" timestamp="0">
```



The timestamp entry is superfluous.

4. Save the file.

Configure AutoSupport delivery method

You can configure the AutoSupport feature to use HTTPS, HTTP, or SMTP delivery methods. HTTPS is the default delivery method.

1. Access the ASUPConfig.xml file in the working directory.
2. In the string, <delivery type="n">, enter 1, 2, or 3 as described in the table:

| Value | Description |
|-------|--|
| 1 | HTTPS (default) <delivery type="1"> |
| 2 | HTTP <delivery type="2"> |
| 3 | SMTP — To properly configure the AutoSupport delivery type to SMTP, you must include the SMTP mail server address, along with the sender and recipient user emails, similar to the following example: <pre><delivery type="3"> <smtp> <mailserver>smtp.example.com</mai lserver> <sender>user@example.com</sender> <replyto>user@example.com</replayt o> </smtp> </delivery></pre> |

Remote volume mirroring

Remote Storage Volumes overview

Use the SANtricity® Remote Storage Volumes feature to import data from a remote storage device directly to a local E-Series volume.

This feature helps streamline the process for equipment upgrades and provides data migration capabilities to move data from non-E-Series devices to E-Series systems.

Configuration overview

The Remote Storage Volumes feature is available with SANtricity System Manager on selected submodel IDs. To use this feature, you must configure a remote storage system and an E-Series storage system to

communicate with each other.

Use the following workflow:

1. [Review requirements and restrictions](#).
2. [Configure hardware](#).
3. [Import remote storage](#).

Find more information

- Online help, available in the System Manager user interface or in the [Documentation Center](#).
- For additional technical information on the Remote Storage Volumes feature, see the [Remote Storage Volumes Technical Report](#).

Requirements and restrictions for remote storage

Before configuring the Remote Storage Volumes feature, review the following requirements and restrictions.

Hardware requirements

Supported protocols

For the initial release of the Remote Storage Volumes feature, support is only available for iSCSI and IPv4 protocols.

Refer to the [NetApp Interoperability Matrix Tool](#) for up-to-date support and configuration information between the host and E-Series (destination) array used for the Remote Storage Volumes feature.

Storage system requirements

The E-Series storage system must include:

- Two controllers (duplex mode)
- iSCSI connections for both E-Series controllers to communicate with the remote storage system through one or more iSCSI connections
- SANtricity OS 11.71 or greater
- Remote Storage feature enabled in the Submodel ID (SMID)

The remote system can be either an E-Series storage system or a system from another vendor. It must include iSCSI-capable interfaces.

Volume requirements

Volumes used for imports must meet the requirements for size, status, and other criteria.

Remote storage volume

The source volume of an import is called a "remote storage volume." This volume must meet the following criteria:

- Cannot be part of another import
- Must have an online status

After the import begins, the controller firmware creates a remote storage volume in the background. Due to that background process, the remote storage volume is not manageable in System Manager and can only be used for the import operation.

After it is created, the remote storage volume is treated like any other standard volume on the E-Series system with the following exceptions:

- Can be used as proxies to the remote storage device.
- Cannot be used as candidates for other volume copies or snapshots.
- Cannot have the Data Assurance setting changed while the import is in progress.
- Cannot be mapped to any hosts, because they are reserved strictly for the import operation.

Each remote storage volume is associated with only one remote storage object; however, one remote storage object can be associated with multiple remote storage volumes. The remote storage volume is uniquely identified using a combination of the following:

- Remote storage object identifier
- Remote storage device LUN number

Target volume candidates

The target volume is the destination volume on the local E-Series system.

The destination volume must meet the following criteria:

- Must be a RAID/DDP volume.
- Must have a capacity that is equal to or larger than the remote storage volume.
- Must have a block size that is the same as the remote storage volume.
- Must have a valid state (optimal).
- Cannot have any of the following relationships: volume copy, snapshot copies, asynchronous or synchronous mirroring.
- Cannot be undergoing any reconfiguration operations: Dynamic Volume Expansion, Dynamic Capacity Expansion, Dynamic Segment Size, Dynamic RAID Migration, Dynamic Capacity Reduction, or Defragmentation.
- Cannot be mapped to a host before the import starts (however, it can be mapped after import completes).
- Cannot have Flash Read Cached (FRC) enabled.

System Manager automatically checks these requirements as part of the Import Remote Storage wizard. Only volumes that meet all the requirements are displayed for destination volume selection.

Restrictions

The Remote Storage feature has the following restrictions:

- Mirroring must be disabled.
- Destination volume on the E-Series system must not have snapshots.

- Destination volume on the E-Series system must not be mapped to any hosts before the import is started.
- Destination volume on the E-Series system must have resource-provisioning disabled.
- Direct mappings of the remote storage volume to a host or multiple hosts are not supported.
- Web Services Proxy is not supported.
- iSCSI CHAP secrets are not supported.
- SMcli is not supported.
- VMware Datastore is not supported.
- Only one storage system in the relationship/import pair can be upgraded at a time when there is an import pair present.

Preparation for production imports

You should perform a test or "dry run" import before production imports to verify proper storage and fabric configuration.

Many variables can impact the import operation and completion time. To ensure a production import is successful and to get a duration estimate, you can use these test imports to ensure all connections are working as expected and the import operation is completing in an appropriate amount of time. You can then make adjustments to achieve the desired results before the production import is initiated.

Configure hardware for Remote Storage Volumes

The E-Series storage system must be configured to communicate with the remote storage system through the supported iSCSI protocol.

Configure remote storage device and E-Series array

Before proceeding to the SANtricity System Manager to configure the Remote Storage Volumes feature, do the following:

1. Manually establish a cabled connection between the E-Series system and the remote storage system such that the two systems can be configured to communicate via iSCSI.
2. Configure the iSCSI ports such that the E-Series system and the remote storage system can communicate successfully with each other.
3. Obtain the IQN of the E-Series system.
4. Make the E-Series system visible to the remote storage system. If the remote storage system is an E-Series system, then create a host using the IQN of the destination E-Series system as the connection information for the host port.
5. If the remote storage device is in use by a host/application:
 - Stop I/O to the remote storage device.
 - Unmap/unmount the remote storage device.
6. Map the remote storage device to the host defined for the E-Series storage system.
7. Obtain the LUN number of the device used for the mapping.



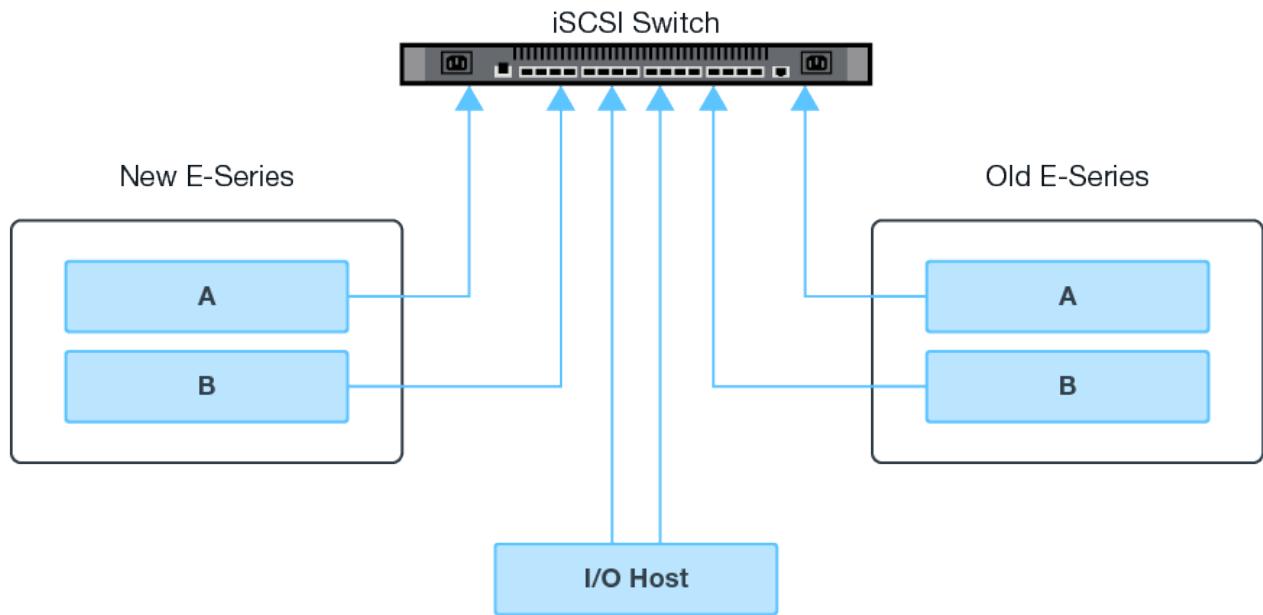
Recommended: Back up the remote source volume before starting the import process.

Cable the storage arrays

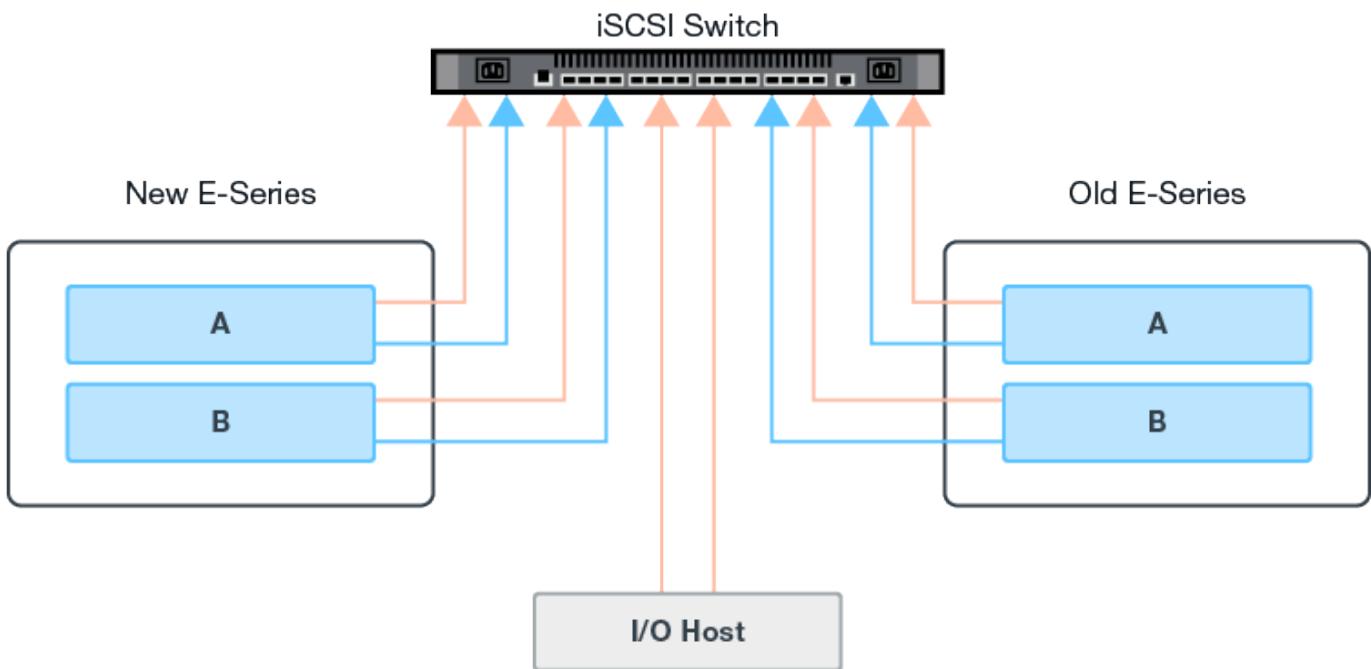
As part of the setup process, the storage arrays and I/O host must be cabled to the iSCSI-compatible interface.

The following diagrams provide examples of how to cable the systems such that they perform Remote Storage Volume operations over an iSCSI connection.

Fabric Connection - Use Case 1



Fabric Connection - Use Case 2



Configure the iSCSI ports

You must configure the iSCSI ports to ensure communication between the target (local E-Series storage array) and source (remote storage array).

The iSCSI ports can be configured multiple ways based on your subnet. The following are a few examples on how to configure the iSCSI ports for use with the Remote Storage Volumes feature.

| Source A | Source B | Target A | Target B |
|----------------|----------------|----------------|----------------|
| 10.10.1.100/22 | 10.10.2.100/22 | 10.10.1.101/22 | 10.10.2.101/22 |

| Source A | Source B | Target A | Target B |
|----------------|----------------|----------------|----------------|
| 10.10.0.100/16 | 10.10.0.100/16 | 10.10.0.101/16 | 10.10.0.101/16 |

Import remote storage

To initiate a storage import from a remote system to a local E-Series storage system, use the Import Remote Storage wizard in the SANtricity System Manager user interface.

What you'll need

- The E-Series storage system must be configured to communicate with the remote storage system. See [Configure hardware](#).
- For the remote storage system, gather the following information:
 - iSCSI IQN
 - iSCSI IP addresses
 - LUN number of the remote storage device (source volume)
- For the local E-Series storage system, create or select a volume to be used for the data import. The target volume must meet the following requirements:
 - Matches the block size of the remote storage device (the source volume).
 - Has a capacity that is equal to or larger than the remote storage device.
 - Has a state of Optimal and is available.
For a full list of requirements, see [Requirements and restrictions](#).
- Recommended: Back up volumes on the remote storage system before starting the import process.

About this task

In this task, you create a mapping between the remote storage device and a volume on the local E-Series storage system. When you finish the configuration, the import begins.



Because many variables can impact the import operation and its completion time, you should first perform smaller “test” imports. Use these tests to ensure that all connections work as expected and that the import operation completes in an appropriate amount of time.

Steps

1. From the SANtricity System Manager, click **Storage > Remote Storage**.

2. Click **Import Remote Storage**.

A wizard for importing remote storage is displayed.

3. In Step 1a of the Configure Source panel, enter connection information.

- a. Under the **Name** field, enter the name for the remote storage device.
- b. Under the **iSCSI connection properties**, enter the following for the remote storage device: IQN, IP address, and the port number (default is 3260).

If you want to add another iSCSI connection, click **+Add another IP address** to include an additional IP address for the remote storage. When you are done, click **Next**.

After you click Next, Step 1b of the Configure Source panel is displayed.

4. Under the **LUN** field, select the desired source LUN for the remote storage device, and then click **Next**.

The Configure Target panel opens and displays volume candidates to serve as the target for the import. Some volumes do not display in the list of candidates due to block size, capacity, or volume availability.

5. From the table, select a target volume on the E-Series storage system. If needed, use the slider to change the import priority. Click **Next**. Confirm the operation in the next dialog box by typing `continue`, and then clicking **Continue**.

If the target volume has a capacity that is larger than the source volume, that additional capacity is not reported to the host connected to the E-Series system. To use the new capacity, you must perform a file system expansion operation on the host after the import operation completes and is disconnected.

After you confirm the configuration in the dialog, the Review panel is displayed.

6. From the Review screen, verify the specified remote storage device, target, and import settings are accurate. Click **Finish** to complete the creation of the remote storage.

Another dialog box opens asking if you want to initiate another import.

7. If needed, click **Yes** to create another remote storage import. Clicking Yes returns to Step 1a of the Configure Source panel, where you can select the existing configuration or add a new one. If you do not want to create another import, click **No** to exit the dialog.

Once the import process begins, the entire target volume is overwritten with the copied data. If the host writes any new data to the target volume during this process, that new data is propagated back to the remote device (source volume).

8. View the progress of the operation in the View Operations dialog under the Remote Storage panel.

The time required to complete the import operation depends on the size of the remote storage system, the priority setting for the import, and the amount of I/O load on both storage systems and their associated volumes.

Once the import is complete, the local volume is a duplicate of the remote storage device.

9. When you are ready to break the relationship between the two volumes, select **Disconnect** on the import object from the Operations in Progress view. Once the relationship is disconnected, performance of the local volume returns to normal and is no longer impacted by the remote connection.

Manage import progress

After the import process begins, you can view and take action on its progress.

For each import operation, the Operations in Progress page displays a percentage of completion and estimated time remaining. Actions include changing the import priority, stopping and resuming operations, and disconnecting from the operation.



You can also view Operations in Progress from the Home page (**Home > Show operations in progress**).

Steps

1. In SANtricity System Manager, go to the Remote Storage page and select **View Operations**.

The Operations in Progress dialog is displayed.

2. If desired, use the links in the Actions column to stop and resume, change priority, or disconnect from an operation.

- **Change Priority** – Select **Change Priority** to change the processing priority of an operation that is in progress or pending. Apply a priority to the operation and then click **OK**.
- **Stop** – Select **Stop** to pause the copying of data from the remote storage device. The relationship between the import pair is still intact, and you can select **Resume** when you are ready to continue the import operation.
- **Resume** – Select **Resume** to begin a stopped or failed process from where it left off. Next, apply a priority to the Resume operation, and then click **OK**.

The Resume operation does **not** restart the import from the beginning. If you want to restart the process from the beginning, you must select **Disconnect**, and then re-create the import through the Import Remote Storage wizard.

- **Disconnect** – Select **Disconnect** to break the relationship between the source and destination volumes for an import operation that has stopped, completed, or failed.

Modify remote storage connection settings

You can edit, add, or delete connection settings for any remote storage configuration through the View/Edit Settings option.

Making changes to connection properties will affect in-progress imports. To avoid disruptions, only make changes to connection properties when imports are not running.

Steps

1. From the Remote Storage screen of the SANtricity System Manager, select the desired Remote Storage object under the result list section.
2. Click **View/Edit Settings**.

The Remote Storage Settings screen is displayed.

3. Click the **Connection Properties** tab.

The configured IP address and port settings for the remote storage import are displayed.

4. Perform one of the following actions:
 - **Edit** – Click **Edit** next to the corresponding line item for the remote storage object. Enter the revised IP address and/or port information in the fields.
 - **Add** – Click **Add**, and then enter the new IP address and port information in the fields provided. Click **Add** to confirm, and then the new connection appears in the list of remote storage objects.
 - **Delete** – Select the desired connection from the list and then click **Delete**. Confirm the operation by typing `delete` in the provided field and then click **Delete**. The connection is removed from the list of remote storage objects.

5. Click **Save**.

The modified connection settings are applied to the remote storage object.

Remove remote storage object

After an import completes, you can remove a remote storage object if you no longer want data copied between the local and remote devices.

Steps

1. Make sure that no imports are associated with the remote storage object you plan to remove.
2. From the Remote Storage screen of the SANtricity System Manager, select the desired Remote Storage object under the result list section.
3. Click **Remove**.

The Confirm Remove Remote Storage Connection dialog is displayed.

4. Confirm the operation by typing `remove` and then clicking **Remove**.

The selected Remote Storage object is removed.

Storage plugin for vCenter

Overview of the Storage Plugin for vCenter

The SANtricity Storage Plugin for vCenter provides integrated management of E-Series storage arrays from within a VMware vSphere Client session.

The following functions are available in the Plugin for vCenter:

- View and manage discovered storage arrays in the network.
- Perform batch operations on groups of multiple storage arrays.
- Perform upgrades on the software OS.
- Import settings from one storage array to another.
- Configure volumes, SSD cache, hosts, host clusters, pools, and volume groups.
- Launch the System Manager interface for additional management tasks on an array.



The plugin is not a direct replacement for the SANtricity System Manager software. System Manager is still required for performing certain storage administration tasks on a single array.

The plugin requires a VMware vCenter Server Appliance deployed in the VMware environment and an application host to install and run the plugin webserver.

Refer to the following figure for more information on communications in the vCenter environment.

[vcenter communication] | [..../media/vcenter_communication.png](#)

Configuration overview

1. [Install and register the plugin](#).
2. [Configure plugin access permissions](#).
3. [Log in to the plugin interface](#).
4. [Discover storage arrays](#).
5. [Provision storage](#).

Find more information

- For online help, see the user interface of the Storage Plugin for vCenter.
- For more information about managing datastores in the vSphere Client, see [VMware vSphere Documentation](#).

Install the Storage Plugin for vCenter

You can install the Storage Plugin for vCenter and verify the plugin registration.

Review installation prerequisites

Be sure that your systems meet the following requirements:

- VMware vCenter Server Appliance supported versions: 6.7U3J, 7.0U1, or 7.0U2
- NetApp SANtricity OS version: 11.60.2 or higher
- Supported application host versions: Windows 2016 or Windows 2019
- CPU requirements for the host system:
 - System memory: 1.5GB
 - Storage space: 275 MB + 200 MB (logging)

Install the plugin software

To install the plugin software:

1. Copy the installer file to the host that will be used as the application server, and then access the folder where you downloaded the installer.
2. Double-click the installation file:

`santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe`

In the above filename, nn.nn.nn.nnnn represents the version number.

3. When the installation starts, follow the on-screen prompts.

During the installation, you are prompted to enter some configuration parameters.

- a. On the first screen, select your preferred language for the software and click **OK**.
- b. In the Introduction screen, click **Next**.
- c. In the Copyright screen, click **Next**.
- d. In the License Agreement screen, select the box for accepting the terms and then click **Next**.
- e. Select the folder where you want to install the software and then click **Next**.
- f. In the Certificate Validation screen, keep the checkbox selected if you want to enforce certificate validation between the plugin and the storage arrays. With this enforcement, the storage array certificates are checked to be trusted against the plugin. If the certificates are not trusted, then they are not allowed to be added to the plugin. If you want to override certificate validation, deselect the checkbox so that all storage arrays can be added to the plugin using self-signed certificates. Click **Next**.

To learn more about certificates, refer to the online help available from the plugin interface.

- g. In the HTTPS Web Service Port screen, leave the default at 8445, or if necessary, change the port number. Click **Next**.
- h. In the Pre-Installation Summary screen, click **Next** to install the files.
- i. When the Webserver Started message appears, click **OK** to complete the installation.
- j. Click **Done**.



If necessary, you can change the Certificate Validation and Web Service Port settings after installation. From the installation directory, open the wsconfig.xml file. To remove the Certificate Validation on storage arrays, change the env key, trust.all.arrays, to true. To change the Web Services port, modify the sslport value to the desired port value ranging from 0-65535. Ensure that the port number used is not binding to another process. When you are done, save the changes and restart the plugin webserver. If the port value of the plugin webserver is changed after registering the plugin to a vCSA, then you must unregister and re-register the plugin so the vCSA is communicating on the changed port to the plugin webserver.

4. Verify that the application server was installed successfully by running the **services.msc** command.
5. Verify that the Application Server (vCP) service, **NetApp SANtricity Storage Plugin for vCenter**, was installed and the service has started.

Register the plugin with a vCenter Server Appliance

After the plugin software is installed, register the plugin with a vCSA.



The plugin can only be registered to one vCSA at a time. To register to a different vCSA, then you must un-register the plugin from the current vCSA and uninstall it from the application host. Then you can re-install the plugin and register it to the other vCSA.

1. Open a prompt through the command line and navigate to the following directory:

```
<install directory>\vcenter-register\bin
```

2. Execute the **vcenter-register.bat** file:

```
vcenter-register.bat ^
-action registerPlugin ^
-vcenterHostname <vCenter FQDN> ^
-username <Administrator username> ^
```

3. Verify that the script was successful.

The logs are saved to %install_dir%/working/logs/vc-registration.log.

Verify the plugin registration

After the plugin is installed and the registration script has executed, verify that the plugin successfully registered with the vCenter Server Appliance.

1. Open the vSphere Client to the vCenter Server Appliance.
2. On the menu bar, select **Administrator** > **Client Plugins**.
3. Make sure the SANtricity Storage Plugin for vCenter is listed as **Enabled**.

If the plugin is listed as Disabled with an error message stating that it cannot communicate with the application server, verify that the port number defined for the application server is enabled to pass through any firewalls that might be in use. The default application server Transmission Control Protocol (TCP) port number is 8445.

Configure plugin access permissions

You can configure access permissions for the Storage Plugin for vCenter, which includes users, roles, and privileges.

Review required vSphere privileges

To access the plugin within the vSphere Client, you must be assigned to a role that has the appropriate vSphere privileges. Users with the “Configure datastore” vSphere privilege have read-write access to the plugin, while users with the “Browse datastore” privilege have read-only access. If a user has neither of these privileges, the plugin displays an “Insufficient Privileges” message.

| Plugin access type | vSphere privilege required |
|------------------------|----------------------------|
| Read-Write (Configure) | Datastore.Configure |
| Read-Only (View) | Datastore.Browse |

Configure Storage Administrator roles

To provide read/write privileges for plugin users, you can create, clone, or edit a role. For more information about configuring roles in the vSphere Client, see the following topic in the VMware Doc Center:

- [Create a Custom Role](#)

Access role actions

1. From the home page of the vSphere Client, select **Administrator** from the access control area.
2. Click **Roles** from the access control area.
3. Perform one of the following actions:
 - **Create new role:** Click on the **Create Role** action icon.
 - **Clone role:** Select an existing role and click on the **Clone Role** action icon.
 - **Edit existing role:** Select an existing role and click on the **Edit Role** action icon.



The Administrator role is not editable.

The appropriate wizard appears, depending on the above selection.

Create a new role

1. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

2. Assign other privileges for the list if needed, and then click **Next**.
3. Name the role and provide a description.
4. Click **Finish**.

Clone a role

1. Name the role and provide a description.
2. Click **OK** to finish the wizard.
3. Select the cloned role from the list, and then click on **Edit Role**.
4. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

5. Click **Next**.
6. Update the name and description, if desired.
7. Click **Finish**.

Edit an existing role

1. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

2. Click **Next**.
3. Update the name or description, if desired.
4. Click **Finish**.

Set permissions for vCenter Server Appliance

After setting privileges for a role, you must then add a permission to the vCenter Server Appliance. This permission allows a given user or group access to the plugin.

1. From the menu dropdown list, select **Hosts and Clusters**.
2. Select the **vCenter Server Appliance** from the access control area.
3. Click the **Permissions** tab.
4. Click the **Add Permission** action icon.
5. Select the appropriate domain and user/group.
6. Select the role created that allows for the read/write plugin privilege.
7. Enable the **Propagate to Children** option, if needed.
8. Click **OK**.



You can select an existing permission and modify it to use the created role. **However, be aware that the role must have the same privileges along with read/write plugin privileges as to avoid a regress in permissions.**

To access the plugin, you must log in to the vSphere Client under the user account that has the read/write privileges for the plugin.

For more information about managing permissions, see the following topics in the VMware Doc Center:

- [Managing Permissions for vCenter Components](#)
- [Best Practices for Roles and Permissions](#)

Log in and navigate the Storage Plugin for vCenter

You can log in to the Storage Plugin for vCenter to navigate the user interface.

1. Before you log in to the plugin, make sure you are using one of the following browsers:
 - Google Chrome 79 or later
 - Mozilla Firefox 70 or later
 - Microsoft Edge 79 or later
2. Log in to the vSphere Client under the user account that has read/write privileges for the plugin.
3. From the vSphere Client Home page, click **SANtricity Storage Plugin for vCenter**.

The plugin opens within a vSphere Client window. The plugin's main page opens to **Manage-All**.

4. Access storage management tasks from the navigation sidebar on the left:
 - **Manage** – Discover storage arrays in your network, open System Manager for an array, import settings from one array to multiple arrays, manage array groups, upgrade the OS software, and provision storage.
 - **Certificate Management** – Manage certificates to authenticate between browsers and clients.
 - **Operations** – View the progress of batch operations, such as importing settings from one array to another.

- **Support** – View technical support options, resources, and contacts.

Discover storage arrays in the plugin

To display and manage storage resources, you must use the Storage Plugin for vCenter interface to discover the IP addresses of arrays in your network.

Step 1: Enter network addresses for discovery

Before you begin

- You must know the network IP addresses (or range of addresses) of the array controllers.
- The storage arrays must be correctly set up and configured, and you must know the storage array login credentials (user name and password).

Steps

1. From the Manage page, select **Add/Discover**.

The Enter Network Address Range dialog box appears.

2. Do one of the following:

- To discover one array, select the **Discover a single storage array** radio button, and then enter the IP address for one of the controllers in the storage array.
- To discover multiple storage arrays, select the **Discover all storage arrays within a network range** radio button, and then enter the starting network address and ending network address to search across your local sub-network.

3. Click **Start Discovery**.

As the discovery process begins, the dialog box displays the storage arrays as they are discovered. The discovery process might take several minutes to complete.

If no manageable arrays are discovered, verify that the storage arrays are properly connected to your network and their assigned addresses are within range. Click **New Discovery Parameters** to return to the Add/Discover page.

4. Select the checkbox next to any storage array that you want to add to your management domain.

The system performs a credential check on each array that you are adding to the management domain. You might need to resolve any issues with untrusted certificates before proceeding.

5. Click **Next** to proceed to the next step in the wizard.

If the storage arrays have valid certificates, go to [Step 3: Provide passwords](#).

If any storage arrays do not have valid certificates, the Resolve Self-Signed Certificates dialog box appears. Go to [Step 2: Resolve untrusted certificates during discovery](#).

If you want to import CA-signed certificates, cancel out of the discovery wizard and click **Certificate Management** from the left panel. Refer to the online help for further instructions.

Step 2: Resolve untrusted certificates during discovery

You must resolve any certificate issues before proceeding with the discovery process.

1. If the Resolve Self-Signed Certificates dialog box opens, review the information displayed for the untrusted certificates. For more information, you can also click the ellipses at the far end of the table and select **View** from the pop-up menu.
2. Do one of the following:
 - If you trust the connections to the discovered storage arrays, click **Next** and then click **Yes** to confirm and continue to the next dialog in the wizard. The self-signed certificates are marked as trusted and the storage arrays will be added to the plugin.
 - If you do not trust the connections to the storage arrays, select **Cancel** and validate each storage array's security certificate strategy before adding any of them.
3. Click **Next** to proceed to the next step in the wizard.

Step 3: Provide passwords

As the last step for discovery, you must enter the passwords for the storage arrays that you want to add to your management domain.

1. For each discovered array, enter its admin password in the fields.
2. Click **Finish**.

It can take several minutes for the system to connect to the specified storage arrays. When the process is finished, the storage arrays are added to your management domain and associated with the selected group (if specified).

Provision storage in the plugin

To provision storage, you create volumes, assign volumes to hosts, and then assign volumes to datastores.



For more information about storage provisioning, see the online help available from the plugin interface.

Create volumes

Volumes are data containers that manage and organize the storage space on your storage array. You create volumes from the storage capacity available on your storage array, which helps organize your system's resources. The concept of "volumes" is similar to using folders/directories on a computer to organize files for quick access.

Volumes are the only data layer visible to hosts. In a SAN environment, volumes are mapped to logical unit numbers (LUNs). These LUNs hold the user data that is accessible using one or more of the host access protocols supported by the storage array.

Steps

1. From the Manage page, select the storage array.
2. Select **Provisioning > Manage Volumes**.

3. Select **Create > Volumes**.

The Select Host dialog box appears.

4. From the drop-down list, select a specific host or host cluster to which you want to assign volumes, or choose to assign the host or host cluster at a later time.
5. To continue the volume creation sequence for the selected host or host cluster, click **Next**.

The Select Workload dialog box appears. A workload contains volumes with similar characteristics, which are optimized based on the type of application the workload supports. You can define a workload or you can select existing workloads.

6. Do one of the following:

- Select the **Create volumes for an existing workload** option and then select the workload from the drop-down list.
- Select the **Create a new workload** option to define a new workload for a supported application or for “Other” applications, and then follow these steps:
 - a. From the drop-down list, select the name of the application you want to create the new workload for. Select one of the “Other” entries if the application you intend to use on this storage array is not listed.
 - b. Enter a name for the workload you want to create.

7. Click **Next**. If your workload is associated with a supported application type, enter the information requested; otherwise, go to the next step.

The Add/Edit Volumes dialog box appears. In this dialog, you create volumes from eligible pools or volume groups. For each eligible pool and volume group, the number of drives available and the total free capacity appears. For some application-specific workloads, each eligible pool or volume group shows the proposed capacity based on the suggested volume configuration and shows the remaining free capacity in GiB. For other workloads, the proposed capacity appears as you add volumes to a pool or volume group and specify the reported capacity.

8. Before you begin adding volumes, read the guidelines in the following table.

| Field | Description |
|---------------|--|
| Free capacity | Because volumes are created from pools or volume groups, the pool or volume group you select must have sufficient free capacity. |

| Field | Description |
|-----------------------|---|
| Data Assurance (DA) | <p>To create a DA-enabled volume, the host connection you are planning to use must support DA.</p> <ul style="list-style-type: none"> If you want to create a DA-enabled volume, select a pool or volume group that is DA capable (look for Yes next to "DA" in the pool and volume group candidates table). DA capabilities are presented at the pool and volume group level. DA protection checks for and corrects errors that might occur as data is transferred through the controllers down to the drives. Selecting a DA-capable pool or volume group for the new volume ensures that any errors are detected and corrected. If any of the host connections on the controllers in your storage array do not support DA, the associated hosts cannot access data on DA-enabled volumes. |
| Drive security | <p>To create a secure-enabled volume, a security key must be created for the storage array.</p> <ul style="list-style-type: none"> If you want to create a secure-enabled volume, select a pool or volume group that is secure capable (look for Yes next to "Secure-capable" in the pool and volume group candidates table). Drive security capabilities are presented at the pool and volume group level. Secure-capable drives prevent unauthorized access to the data on a drive that is physically removed from the storage array. A secure-enabled drive encrypts data during writes and decrypts data during reads using a unique encryption key. A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities. |
| Resource provisioning | <p>To create a resource-provisioned volume, all drives must be NVMe drives with the Deallocated or Unwritten Logical Block Error (DULBE) option.</p> |

- Choose one of these actions based on whether you selected Other or an application-specific workload in the previous step:
 - Other** – Click **Add new volume** in each pool or volume group that you want to use to create one or more volumes.
 - Application-specific workload** – Either click **Next** to accept the system-recommended volumes and

characteristics for the selected workload, or click **Edit Volumes** to change, add, or delete the system-recommended volumes and characteristics for the selected workload.

The following fields appear.

| Field | Description |
|--|---|
| Volume Name | A volume is assigned a default name during the volume creation sequence. You can either accept the default name or provide a more descriptive one indicating the type of data stored in the volume. |
| Reported Capacity | Define the capacity of the new volume and the capacity units to use (MiB, GiB, or TiB). For thick volumes, the minimum capacity is 1 MiB, and the maximum capacity is determined by the number and capacity of the drives in the pool or volume group. Capacity in a pool is allocated in 4-GiB increments. Any capacity that is not a multiple of 4 GiB is allocated but not usable. To make sure that the entire capacity is usable, specify the capacity in 4-GiB increments. If unusable capacity exists, the only way to regain it is to increase the capacity of the volume. |
| Volume Type | If you selected Application-specific workload, the Volume Type field appears. This indicates the type of volume that was created for an application-specific workload. |
| Volume Block Size (EF300 and EF600 only) | Shows the block sizes that can be created for the volume: <ul style="list-style-type: none">• 512 – 512 bytes• 4K – 4,096 bytes |

| Field | Description |
|--------------|--|
| Segment Size | <p>Shows the setting for segment sizing, which only appears for volumes in a volume group. You can change the segment size to optimize performance.</p> <p>Allowed segment size transitions – The system determines the segment size transitions that are allowed. Segment sizes that are inappropriate transitions from the current segment size are unavailable on the drop-down list. Allowed transitions usually are double or half of the current segment size. For example, if the current volume segment size is 32 KiB, a new volume segment size of either 16 KiB or 64 KiB is allowed.</p> <p>SSD Cache-enabled volumes – You can specify a 4-KiB segment size for SSD Cache-enabled volumes. Make sure you select the 4-KiB segment size only for SSD Cache-enabled volumes that handle small-block I/O operations (for example, 16 KiB I/O block sizes or smaller). Performance might be impacted if you select 4 KiB as the segment size for SSD Cache-enabled volumes that handle large block sequential operations.</p> <p>Amount of time to change segment size – The amount of time to change a volume's segment size depends on these variables:</p> <ul style="list-style-type: none"> • The I/O load from the host • The modification priority of the volume • The number of drives in the volume group • The number of drive channels • The processing power of the storage array controllers <p>When you change the segment size for a volume, I/O performance is affected, but your data remains available.</p> |

| Field | Description |
|----------------|---|
| Secure-capable | <p>Yes appears next to "Secure-capable" only if the drives in the pool or volume group are encryption-capable.</p> <p>Drive Security prevents unauthorized access to the data on a drive that is physically removed from the storage array. This option is available only when the Drive Security feature has been enabled, and a security key is set up for the storage array.</p> <p>A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.</p> |
| DA | <p>Yes appears next to "DA" only if the drives in the pool or volume group support Data Assurance (DA).</p> <p>DA increases data integrity across the entire storage system. DA enables the storage array to check for errors that might occur as data is transferred through the controllers down to the drives. Using DA for the new volume ensures that any errors are detected.</p> |

10. To continue the volume creation sequence for the selected application, click **Next**.
11. In the last step, review a summary of the volumes you intend to create and make any necessary changes. To make changes, click **Back**. When you are satisfied with your volume configuration, click **Finish**.

Create host access and assign volumes

A host can be created automatically or manually:

- **Automatic** — Automatic host creation for SCSI-based (not NVMe-oF) hosts is initiated by the Host Context Agent (HCA). The HCA is a utility that you can install on each host attached to the storage array. Each host that has the HCA installed pushes its configuration information to the storage array controllers through the I/O path. Based on the host information, the controllers automatically create the host and the associated host ports and set the host type. If needed, you can make any additional changes to the host configuration. After the HCA performs its automatic detection, the host is automatically configured with the following attributes:
 - The host name derived from the system name of the host.
 - The host identifier ports that are associated with the host.
 - The Host Operating System Type of the host.



Host Context Agent software for Linux and Windows is available from [NetApp Support - Downloads](#).



Hosts are created as stand-alone hosts; the HCA does not automatically create or add to host clusters.

- **Manual** – During manual host creation, you associate host port identifiers by selecting them from a list or manually entering them. After you create a host, you can assign volumes to it or add it to a host cluster if you plan to share access to volumes.

Using the HCA to auto-discover the host

You can allow the Host Context Agent (HCA) to automatically detect the hosts, and then verify that the information is correct.

Steps

1. From the Manage page, select the storage array with the host connection.
2. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

3. Select **Storage > Hosts**.

The table lists the automatically created hosts.

4. Verify that the information provided by the HCA is correct (name, host type, host port identifiers).
5. If you need to change any of the information, select the host, and then click **View/Edit Settings**.

Manually creating the host

Before you begin

Read the following guidelines:

- You must already have added or discovered storage arrays within your environment.
- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. From the Manage page, select the storage array with the host connection.
2. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

3. Click **Create > Host**.

The Create Host dialog box appears.

4. Select the settings for the host as appropriate.

| Field | Description |
|-------|-------------------------------|
| Name | Type a name for the new host. |

| Field | Description |
|----------------------------|--|
| Host operating system type | Select the operating system that is running on the new host from the drop-down list. |
| Host interface type | (Optional) If you have more than one type of host interface supported on your storage array, select the host interface type that you want to use. |
| Host ports | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Select I/O Interface. Generally, the host ports should have logged in and be available from the drop-down list. You can select the host port identifiers from the list. • Manual add. If a host port identifier is not displayed in the list, it means that the host port has not logged in. An HBA utility or the iSCSI initiator utility may be used to find the host port identifiers and associate them with the host. <p>You can manually enter the host port identifiers or copy/paste them from the utility (one at a time) into the Host ports field.</p> <p>You must select one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the Host ports field. If necessary, you also can remove an identifier by selecting the X next to it.</p> |

| Field | Description |
|---------------------------|---|
| Set CHAP initiator secret | <p>(Optional) If you selected or manually entered a host port with an iSCSI IQN, and if you want to require a host that tries to access the storage array to authenticate using Challenge Handshake Authentication Protocol (CHAP), select the Set CHAP initiator secret checkbox. For each iSCSI host port you selected or manually entered, do the following:</p> <ul style="list-style-type: none"> • Enter the same CHAP secret that was set on each iSCSI host initiator for CHAP authentication. If you are using mutual CHAP authentication (two-way authentication that enables a host to validate itself to the storage array and for a storage array to validate itself to the host), you also must set the CHAP secret for the storage array at initial setup or by changing settings. • Leave the field blank if you do not require host authentication. <p>Currently, the only iSCSI authentication method used is CHAP.</p> |

5. Click **Create**.

6. If you need to update the host information, select the host from the table and click **View/Edit Settings**.

After the host is successfully created, the system creates a default name for each host port configured for the host (user label). The default alias is <Hostname_Port Number>. For example, the default alias for the first port created for host IPT is `IPT_1`.

7. Next, you must assign a volume to a host or a host cluster so it can be used for I/O operations. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

8. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the Filter box to make it easier to find particular volumes.

9. Select the check box next to each volume that you want to assign or select the check box in the table header to select all volumes.

10. Click **Assign** to complete the operation.

The system performs the following actions:

- The assigned volume receives the next available LUN number. The host uses the LUN number to access the volume.
- The user-supplied volume name appears in volume listings associated to the host. If applicable, the

factory-configured access volume also appears in volume listings associated to the host.

Create a datastore in vSphere Client

To create a datastore in the vSphere Client, see the following topic in the VMware Doc Center:

- [Create a VMFS Datastore in the vSphere Client](#)

Increase capacity of existing datastore by increasing volume capacity

You can increase the reported capacity (the capacity reported to hosts) of a volume by using the free capacity that is available in the pool or volume group. To learn more about pools and volume groups, see the online help for the plugin.

Before you begin

Make sure that:

- Enough free capacity is available in the volume's associated pool or volume group.
- The volume is Optimal and not in any state of modification.
- No hot spare drives are in use in the volume. (Applies only to volumes in volume groups.)



Increasing the capacity of a volume is supported only on certain operating systems. If you increase the volume capacity on a host operating system that does not support LUN expansion, the expanded capacity is unusable, and you cannot restore the original volume capacity.

Steps

1. Navigate to the plugin within vSphere Client.
2. Within the plugin, select the desired storage array.
3. Click on **Provisioning** and select **Manage Volumes**.
4. Select the volume for which you want to increase capacity, and then select **Increase Capacity**.

The Confirm Increase Capacity dialog box appears.

5. Select **Yes** to continue.

The Increase Reported Capacity dialog box appears.

This dialog box displays the volume's current reported capacity and the free capacity available in the volume's associated pool or volume group.

6. Use the **Increase reported capacity by adding...** box to add capacity to the current available reported capacity. You can change the capacity value to display in either mebibytes (MiB), gibibytes (GiB), or tebibytes (TiB).
7. Click **Increase**.
8. View the Recent Tasks pane for the progress of the increase capacity operation that is currently running for the selected volume. This operation can be lengthy and could affect system performance.
9. After the volume capacity is complete, you must manually increase the VMFS size to match as described in the following topic:
 - [Increase VMFS Datastore Capacity in the vSphere Client](#)

Increase capacity of existing datastore by adding volumes

1. You can increase the capacity of a datastore by adding volumes. Follow the steps in [Create volumes](#).
2. Next, assign the volumes to the desired host to increase the datastore's capacity. See the following topic:
 - [Increase VMFS Datastore Capacity in the vSphere Client](#)

Remove the Storage Plugin for vCenter

You can remove the plugin from the vCenter Server Appliance and uninstall the plugin webserver from the application host.

These are two distinct steps that you can perform in any order. However, if you choose to remove the plugin webserver from the application host before unregistering the plugin, the registration script is removed during that process and you cannot use Method 1 to unregister.

Unregister the plugin from a vCenter Server Appliance

To unregister the plugin from a vCenter Server Appliance, select one of these methods:

- Method 1: Executing the registration script
- Method 2: Using the vCenter Server Mob pages

Method 1: Executing the registration script

1. Open a prompt through the command line and navigate to the following directory:

```
<install directory>\vcenter-register\bin
```

2. Execute the vcenter-register.bat file:

```
vcenter-register.bat ^
-action unregisterPlugin ^
-vcenterHostname <vCenter FQDN> ^
-username <Administrator Username> ^
```

3. Verify that the script is successful.

The logs are saved to %install_dir%/working/logs/vc-registration.log.

Method 2: Using the vCenter Server Mob pages

1. Open a web browser and enter the following url:

<https://<FQDN of vCenter Server>/mob>

2. Log in under the administrator credentials.
3. Look for the property name of extensionManager and click the link associated with that property.
4. Expand the properties list by clicking the **More...** link at the bottom of the list.

5. Verify that the extension `plugin.netapp.eseries` is in the list.
6. If it is present, then click the Method `UnregisterExtension`.
7. Enter the value `plugin.netapp.eseries` in the dialog and click **Invoke Method**.
8. Close the dialog and refresh the web browser.
9. Verify that the `plugin.netapp.eseries` extension is not on the list.



This procedure unregisters the plugin from the vCenter Server Appliance; however, it does not remove plugin package files from the server. To remove package files, use SSH to access the vCenter Server Appliance and navigate to the following directory:

`etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`

Then remove the directory associated with the plugin.

Remove the plugin webserver from the Application host

To remove the plugin software from the application host, follow these steps:

1. From the application server, navigate to the **Control Panel**.
2. Go to **Apps & Features**, and then select **SANtricity Storage Plugin for vCenter**.
3. Click **Uninstall/Change**.

A confirmation dialog opens.

4. Click **Uninstall**.

A confirmation message is displayed when the uninstall is complete.

5. Click **Done**.

Legacy solutions

Cloud connector

Overview of the SANtricity® Cloud Connector

The SANtricity Cloud Connector is a host-based Linux application that enables you to perform full block-based and file-based backup and recovery of E-Series volumes to S3 compliant accounts (for example, Amazon Simple Storage Service and NetApp StorageGRID) and NetApp AltaVault appliance.

Available for installation on RedHat and SUSE Linux platforms, the SANtricity Cloud Connector is a packaged solution (.bin file). After you install SANtricity Cloud Connector, you can configure the application to perform backup and restore jobs for E-Series volumes to an AltaVault appliance or to your existing Amazon S3 or StorageGRID accounts. All jobs performed through the SANtricity Cloud Connector use REST-based APIs.

Considerations

When using these procedures, be aware that:

- Configuration and backup/restore jobs described in these procedures apply to the graphical user interface version of the SANtricity Cloud Connector.
- REST API workflows for the SANtricity Cloud Connector application are not described in these procedures. For experienced developers, endpoints are available for each SANtricity Cloud Connector operation under the API documentation. The API documentation is accessible by navigating to <http://<hostname.domain>:<port>/docs> through a browser.

Types of backups

The SANtricity Cloud Connector provides two types of backups: image-based and file-based backups.

- **Image-based backup**

An image-based backup reads the raw data blocks from a snapshot volume and backs them up to a file known as an image. All of the data blocks on the snapshot volume are backed up, including empty blocks, blocks occupied by deleted files, blocks associated with partitioning, and filesystem metadata. Image backups have the advantage of storing all information with the snapshot volume regardless of the partitioning scheme or filesystems on it.

The image is not stored on the Backup Target as a single file, but is instead broken up into a series of data chunks, which are 64MB in size. The data chunks allow SANtricity Cloud Connector to use multiple connections to the backup target, thereby improving the performance of the backup process.

For backups to StorageGRID and Amazon Web Services (S3), each data chunk uses a separate encryption key to encrypt the chunk. The key is a SHA256 hash consisting of the combination of a user supplied passphrase and the SHA256 hash of the user data. For backups to AltaVault, SANtricity Cloud Connector does not encrypt the data chunks as AltaVault performs this operation.

- **File-based backup**

A file-based backup reads the files contained with a filesystem partition and backs them up into a series of data chunks that are 64MB in size. A file-based backup does not back up deleted files or partitioning and filesystem metadata. As with image-based backups, the data chunks allow SANtricity Cloud Connector to use multiple connections to the backup target, thereby improving performance of the backup process.

For backups to StorageGRID and Amazon Web Services, each data chunk uses a separate encryption key to encrypt the chunk. The key is a SHA256 hash consisting of the combination of user-supplied pass phrase and the SHA256 hash of the user data. For backups to AltaVault, the data chunks are not encrypted by SANtricity Cloud Connector because AltaVault performs this operation.

System requirements for Cloud Connector

Your system must meet compatibility requirements for the SANtricity Cloud Connector.

Host hardware requirements

Your hardware must meet the following minimum requirements:

- At least 5 GB of memory; 4 GB for the maximum configured heap size
- At least 5 GB of free disk space is required from the software installation

You must install the SANtricity Web Services Proxy to use the SANtricity Cloud Connector. You can install the Web Services Proxy locally or you can run the application remotely on a different sever. For information on installing the SANtricity Web Services Proxy, see the [Web Services Proxy topics](#).

Supported browsers

The following browsers are supported with the SANtricity Cloud Connector application (minimum versions noted):

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

 API documentation for the SANtricity Cloud Connector application will not load when using the Compatibility View setting within the Microsoft Internet Explorer v11 browser. To ensure the API documentation displays properly under the Microsoft Internet Explorer v11 browser, it is recommended that the Compatibility View setting is disabled.

Compatible storage arrays and controller firmware

You should verify the compatibility of your storage arrays and firmware before using the SANtricity Cloud Connector application.

For a complete and up-to-date listing of all compatible storage arrays and firmware for the SANtricity Cloud Connector, see the [NetApp Interoperability Matrix Tool](#).

Compatible operating systems

The SANtricity Cloud Connector 4.0 application is compatible with and supported on the following operating systems:

| Operating System | Version | Architecture |
|-------------------------------------|---------|--------------|
| Red Hat Enterprise Linux (RHEL) | 7.x | 64 bit |
| SUSE Linux Enterprise Server (SLES) | 12.x | 64 bit |

Supported file systems

You must use supported file systems to perform backups and restores through the SANtricity Cloud Connector application.

The following file systems are supported for backup and restore operations under the SANtricity Cloud Connector application:

- ext2
- ext3

- ext4

Install SANtricity Cloud Connector

The SANtricity Cloud Connector packaged solution (.bin file) is available for RedHat and SUSE Linux platforms only.

You can install the SANtricity Cloud Connector application through graphical mode or console mode on a compatible Linux operating system. During the installation process, you must specify the non-SSL and SSL port numbers for the SANtricity Cloud Connector. When installed, the SANtricity Cloud Connector runs as a daemon process.

Before you begin

Review the following notes:

- If SANtricity Web Services Proxy is already installed on the same server as the SANtricity Cloud Connector, conflicts will occur between non-SSL port numbers and SSL port numbers conflicts. In this case, choose appropriate numbers for the non-SSL port and the SSL port during the SANtricity Cloud Connector installation.
- If any hardware changes are performed on your host, re-install the SANtricity Cloud Connector application to ensure encryption consistency.
- Backups created through version 3.1 of the SANtricity Cloud Connector application are not compatible with version 4.0 of the SANtricity Cloud Connector application. If you intend to maintain these backups, you must continue to use your previous version of the SANtricity Cloud Connector. To ensure successful installation of separate 3.1 and 4.0 releases of the SANtricity Cloud Connector, unique port numbers must be assigned for each version of the application.

Install Device Mapper Multipath (DM-MP)

Any host running the SANtricity Cloud Connector also must run Linux Device Mapper Multipath (DM-MP) and have the multipath-tools package installed.

The SANtricity Cloud Connector discovery process relies on the multipath tools package for discovery and recognition of the volumes and files to backup or restore. For more information on how to set up and configure the Device Mapper, see the *SANtricity Storage Manager Multipath Drivers Guide* for the release of SANtricity you are using under the [E-Series and SANtricity Document Resources](#).

Install Cloud Connector

You can install SANtricity Cloud Connector on Linux operating systems in either graphical mode or console mode.

Graphical mode

You can use graphical mode to install the SANtricity Cloud Connector on a Linux operating system.

Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

Steps

1. Download the SANtricity Cloud Connector installation file to the desired host location.
2. Open a terminal window.

3. Navigate to the directory file containing the SANtricity Cloud Connector installation file.
4. Start the SANtricity Cloud Connector installation process:

```
./cloudconnector-xxxx.bin -i gui
```

In this command, xxxx designates the version number of the application.

The Installer window is displayed.

5. Review the Introduction statement, and then click **Next**.

The License Agreement for NetApp, Inc. Software is displayed within the installer window.

6. Accept the terms of the License Agreement, and then click **Next**.

The Backups created with previous releases of SANtricity Cloud Connector page is displayed.

7. To acknowledge the Backups created with previous releases of SANtricity Cloud Connector message, click **Next**.



To install version 4.0 of the SANtricity Cloud Connector while maintaining a previous version, unique port numbers must be assigned for each version of the application.

The Choose Install page is displayed within the Installer window. The Where Would You Like to Install field displays the following default install folder: opt/netapp/santricity_cloud_connector4/

8. Choose one of the following options:

- To accept the default location, click **Next**.
- To change the default location, enter a new folder location.
An Enter the Non SSL Jetty Port Number page is displayed. A default value of 8080 is assigned to the non-SSL port.

9. Choose one of the following options:

- To accept the default SSL port number, click **Next**.
- To change the default SSL port number, enter the new desired port number value.

10. Choose one of the following options:

- To accept the default Non SSL port number, click **Next**.
- To change the default Non SSL port number, enter the new desired port number value.
The Pre-Installation Summary page is displayed.

11. Review the displayed Pre-Installation Summary, and then click **Install**.

The installation of the SANtricity Cloud Connector begins and a Webserver Daemon Setup prompt is displayed.

12. Click **OK** to acknowledge the Webserver Daemon Setup prompt.

The Installation Complete message is displayed.

13. Click **Done** to exit the SANtricity Cloud Connecter installer.

Console mode

You can use the console mode to install the SANtricity Cloud Connector on a Linux operating system.

Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

Steps

1. Download the SANtricity Cloud Connector installation file to the desired IO host location.
2. Open a terminal window.
3. Navigate to the directory file containing the SANtricity Cloud Connector installation file.
4. Start the SANtricity Cloud Connector installation process:

```
./cloudconnector-xxxx.bin -i console
```

In this command, xxxx indicates the version number of the application.

The installation process for the SANtricity Cloud Connector is initialized.

5. Press **Enter** to proceed with the installation process.

The End User License Agreement for NetApp, Inc. Software is displayed within the installer window.



To cancel the installation process at any time, type **quit** under the installer window.

6. Press **Enter** to proceed through each portion of the End User License Agreement.

The License Agreement acceptance statement is displayed under the installer window.

7. To accept the terms of the End User License Agreement and proceed with the installation of the SANtricity Cloud Connector, enter **Y** and press **Enter** under the installer window.

The Backups created with previous releases of SANtricity Cloud Connector page is displayed.



If you do not accept the terms of the End User Agreement, type **N** and press **Enter** to terminate the installation process for the SANtricity Cloud Connector.

8. To acknowledge the Backups created with previous releases of SANtricity Cloud Connector message, press **Enter**.



To install version 4.0 of the SANtricity Cloud Connector while maintaining a previous version, unique port numbers must be assigned for each version of the application.

A Choose Install Folder message with the following default install folder for the SANtricity Cloud Connector is displayed:`/opt/netapp/santricity_cloud_connector4/`.

9. Choose one of the following options:

- To accept the default install location, press **Enter**.

- To change the default install location, enter the new folder location.
An Enter the Non SSL Jetty Port Number message is displayed. A default value of 8080 is assigned to the Non SSL port.
- Choose one of the following options:
 - To accept the default SSL port number, press **Next**.
 - To change the default SSL port number, enter the new desired port number value.
 - Choose one of the following options:
 - To accept the default Non SSL port number, press **Enter**.
 - To change the default Non SSL port number, enter the new port number value.
The Pre-Installation Summary for the SANtricity Cloud Connector is displayed.
 - Review the displayed Pre-Installation Summary, and press **Enter**.
 - Press **Enter** to acknowledge the Webserver Daemon Setup prompt.
The Installation Complete message is displayed.
 - Press **Enter** to exit the SANtricity Cloud Connector installer.

Add server certificate and CA certificate into a keystore

To use a secure https connection from the browser to the SANtricity Cloud Connector host, you can accept the self-signed certificate from the SANtricity Cloud Connector host or add a certificate and a trust chain recognized by both the browser and the SANtricity Cloud Connector application.

Before you begin

The SANtricity Cloud Connector application must be installed on a host.

Steps

- Stop the service using the `systemctl` command.
- From the default install location, access the working directory.



The default install location for the SANtricity Cloud Connector is
`/opt/netapp/santricity_cloud_connector4`.

- Using the `keytool` command, create your server certificate, and certificate signing request (CSR).

EXAMPLE

```
keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
-sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
keystore_cloudconnect.jks -storepass changeit
keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
-storepass changeit -file cloudconnect.csr
```

- Send the generated CSR to the certificate authority (CA) of your choosing.

The certificate authority signs the certificate request and returns a signed certificate. In addition, you receive a certificate from the CA itself. This CA certificate must be imported into your keystore.

- Import the certificate and the CA certificate chain into the application keystore: /<install Path>/working/keystore

EXAMPLE

```
keytool -import -alias ca-root -file root-ca.cer -keystore  
keystore_cloudconnect.jks -storepass <password> -noprompt  
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore  
keystore_cloudconnect.jks -storepass <password> -noprompt  
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer  
-keystore keystore_cloudconnect.jks -storepass <password>
```

- Restart the service.

Add StorageGRID certificate into a keystore

If you are configuring StorageGRID as the target type for the SANtricity Cloud Connector application, you must first add a StorageGRID certificate into the SANtricity Cloud Connector keystore.

Before you begin

- You have a signed StorageGRID certificate.
- You have the SANtricity Cloud Connector application installed on a host.

Steps

- Stop the service using the `systemctl` command.
- From the default install location, access the working directory.



The default install location for the SANtricity Cloud Connector is
`/opt/netapp/santricity_cloud_connector4`.

- Import the StorageGRID certificate into the application keystore: /<install Path>/working/keystore

EXAMPLE

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import  
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file  
/home/ictlabsg01.cer -keystore  
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

- Restart the service.

Configure the SANtricity Cloud Connector for the first time

Upon successful installation, you can set up the SANtricity Cloud Connector application through the configuration wizard. The configuration wizard is displayed after you initially log in to the SANtricity Cloud Connector.

Log in to the SANtricity Cloud Connector for the first time

When initializing the SANtricity Cloud Connector for the first time, you must enter a default password to access the application.

Before you begin

Make sure you have access to an internet-connected browser.

Steps

1. Open a supported browser.
2. Connect to the configured SANtricity Cloud Connector server (e.g., `http://localhost:8080/`).

The initial login page for the SANtricity Cloud Connector application is displayed.

3. In the Administrator Password field, enter the default password of `password`.
4. Click **Log In**.

The SANtricity Cloud Connector Configuration Wizard is displayed.

Using the Configuration Wizard

The Configuration Wizard is displayed upon successful initial login to the SANtricity Cloud Connector.

Through the Configuration Wizard, you set up the administrator password, Web Services Proxy login management credentials, desired backup target type, and encryption pass phrase for the SANtricity Cloud Connector.

Step 1: Set administrator password

You can customize the password used for subsequent logins to the SANtricity Cloud Connector through the Set Administrator Password page.

Establishing a password through the Set Administrator Password page effectively replaces the default password used during the initial login for the SANtricity Cloud Connector application.

Steps

1. On the Set Administrator Password page, enter the desired login password for the SANtricity Cloud Connector in the **Enter the new administrator password** field.
2. In the **Re-enter the new administrator password** field, re-enter the password from first field.
3. Click **Next**.

The password setup for the SANtricity Cloud Connector is accepted and the Set Pass Phrase page is displayed under the Configuration Wizard.



The user defined administrator password is not set until you complete the configuration wizard.

Step 2: Set pass phrase

Under the Enter the Encryption Pass Phrase page, you can specify an alphanumeric pass phrase between 8 and 32 characters.

A user-specified pass phrase is required as part of the data encryption key used by the SANtricity Cloud Connector application.

Steps

1. In the **Define a pass phrase** field, enter the desired pass phrase.
2. In the **Re-enter your pass phrase** field, re-enter the pass phrase from the first field.
3. Click **Next**.

The entered pass phrase for the SANtricity Cloud Connector application is accepted and the Select Target Type page for the configuration wizard is displayed.

Step 3: Select target type

Backup and restore capabilities are available for Amazon S3, AltaVault, and StorageGRID target types through the SANtricity Cloud Connector. You can specify the desired storage target type for the SANtricity Cloud Connector application under the Select the Target Type page.

Before you begin

Make sure you have one of the following: AltaVault mount point, Amazon AWS account, or StorageGRID account.

Steps

1. In the dropdown menu, select one of the following options:
 - Amazon AWS
 - AltaVault
 - StorageGRID

A Target Type page for the selected option is displayed in the Configuration Wizard.

2. Refer to the appropriate configuration instructions for AltaVault, Amazon AWS, or StorageGRID.

Configure AltaVault appliance

After selecting the AltaVault appliance option under the Select the Target Type page, configuration options for the AltaVault target type are displayed.

Before you begin

- You have the NFS mount path for an AltaVault appliance.
- You specified AltaVault appliance as the target type.

Steps

1. In the **NFS Mount Path** field, enter the mount point for the AltaVault target type.



Values in the **NFS Mount Path** field must follow the Linux path format.

2. Select the **Save a backup of the configuration database on this target** check box to create a backup of the configuration database on the selected target type.



If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered under the configuration wizard.

3. Click **Test Connection** to test the connection for the specified AltaVault settings.

4. Click **Next**.

The specified target type for the SANtricity Cloud Connector is accepted and the Web Services Proxy page is displayed in the Configuration Wizard.

5. Proceed to "Step 4: Connect to Web Services Proxy."

Configure Amazon AWS account

After selecting the Amazon AWS option under the Select the Target Type page, configuration options for the Amazon AWS target type are displayed.

Before you begin

- You have an established Amazon AWS account.
- You specified Amazon AWS as the target type.

Steps

1. In the **Access Key ID** field, enter the access ID for the Amazon AWS target.
2. In the **Secret Access Key** field, enter the secret access key for the target.
3. In the **Bucket Name** field, enter the bucket name for the target.
4. Select the **Save a backup of the configuration database on this target** checkbox to create a backup of the configuration database on the selected target type.



It is recommended you enable this setting to ensure that data from the backup target can be restored if the database is lost.



If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered under the configuration wizard.

5. Click **Test Connection** to verify the entered Amazon AWS credentials.

6. Click **Next**.

The specified target type for the SANtricity Cloud Connector is accepted, and the Web Services Proxy page is displayed under the Configuration Wizard.

7. Proceed to "Step 4: Connect to Web Services Proxy."

Configure StorageGRID account

After selecting the StorageGRID option under the Select the Target Type page, configuration options for the StorageGRID target type are displayed.

Before you begin

- You have an established StorageGRID account.
- You have a signed StorageGRID certificate in the SANtricity Cloud Connector keystore.
- You specified StorageGRID as the target type.

Steps

1. In the **URL** field, enter the URL for the Amazon S3 cloud service
2. In the **Access Key ID** field, enter the access ID for the S3 target.
3. In the **Secret Access Key** field, enter the secret access key for the S3 target.
4. In the **Bucket Name** field, enter the bucket name for the S3 target.
5. To use path style access, select the **Use path-style access** checkbox.



If unchecked, virtual host-style access is used.

6. Select the **Save a backup of the configuration database on this target** checkbox to create a backup of the configuration database on the selected target type.



It is recommended you enable this setting to ensure that data from the backup target can be restored if the database is lost.



If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered in the configuration wizard.

7. Click **Test Connection** to verify the entered S3 credentials.



Some S3-compliant accounts may require secured HTTP connections. For information on placing a StorageGRID certificate in the keystore, see [Add StorageGRID certificate into a keystore](#).

8. Click **Next**.

The specified target type for the SANtricity Cloud Connector is accepted and the Web Services Proxy page is displayed under the Configuration Wizard.

9. Proceed to "Step 4: Connect to Web Services Proxy."

Step 4: Connect to Web Services Proxy

Login and connection information for the Web Services Proxy used in conjunction with the SANtricity Cloud Connector is entered through the Enter Web Services Proxy URL and Credentials page.

Before you begin

Make sure you have an established connection to the SANtricity Web Services Proxy.

Steps

1. In the **URL** field, enter the URL for the Web Services Proxy used for the SANtricity Cloud Connector.
2. In the **User Name** field, enter the user name for the Web Services Proxy connection.
3. In the **Password** field, enter the password for the Web Services Proxy connection.
4. Click **Test Connection** to verify the connection for the entered Web Services Proxy credentials.
5. After verifying the entered Web Services Proxy credentials through the test connection.
6. Click **Next**

The Web Services Proxy credentials for the SANtricity Cloud Connector is accepted and the Select Storage Arrays page is displayed in the Configuration Wizard.

Step 5: Select storage arrays

Based on the SANtricity Web Services Proxy credentials entered through the Configuration Wizard, a list of available storage arrays is displayed under the Select Storage Arrays page. Through this page, you can select which storage arrays the SANtricity Cloud Connector uses for backup and restore jobs.

Before you begin

Make sure you have storage arrays configured to your SANtricity Web Services Proxy application.

 Unreachable storage arrays observed by the SANtricity Cloud Connector application will result in API exceptions in the log file. This is the intended behavior of the SANtricity Cloud Connector application whenever a volume list is pulled from an unreachable array. To avoid these API exceptions in the log file, you can resolve the root issue directly with the storage array or remove the affected storage array from the SANtricity Web Services Proxy application.

Steps

1. Select each checkbox next to the storage array that you want to assign to the SANtricity Cloud Connector application for backup and restore operations.
2. Click **Next**.

The selected storage arrays are accepted, and the Select Hosts page is displayed in the Configuration Wizard.



You must configure a valid password for any storage array selected under the Select Storage Arrays page. You can configure storage array passwords through the SANtricity Web Services Proxy API Documentation.

Step 6: Select hosts

Based on the Web Services Proxy-hosted storage arrays selected through the Configuration Wizard, you can select an available host to map backup and restore candidate volumes to the SANtricity Cloud Connector application through the Select Hosts page.

Before you begin

Make sure you have a host available through the SANtricity Web Services Proxy.

Steps

1. In the drop-down menu for the listed storage array, select the desired host.
2. Repeat step 1 for any additional storage arrays listed under the Select Host page.
3. Click **Next**.

The selected host for the SANtricity Cloud Connector is accepted and the Review page is displayed in the Configuration Wizard.

Step 7: Review the initial configuration

The final page of the SANtricity Cloud Connector configuration wizard provides a summary of the entered results for your review.

Review the results of the validated configuration data.

- If all configuration data is successfully validated and established, click **Finish** to complete the configuration process.
- If any section of the configuration data cannot be validated, click **Back** to navigate to the applicable page of the configuration wizard to revise the submitted data.

Log into the SANtricity Cloud Connector

You can access the graphical user interface for the SANtricity Cloud Connector application through the configured server in a supported browser. Make sure you have an established SANtricity Cloud Connector account.

Steps

1. In a supported browser, connect to the configured SANtricity Cloud Connector server (for example, <http://localhost:8080/>).

The login page for the SANtricity Cloud Connector application is displayed.

2. Enter your configured administrator password.
3. Click **Login**.

The landing page for the SANtricity Cloud Connector application is displayed.

Backups

You can access the Backups option in the left navigation panel of the SANtricity Cloud Connector application. The Backups option displays the Backups page, which allows you to create new image-based or file-based backup jobs.

Use the **Backups** page of the SANtricity Cloud Connector application to create and process backups of E-Series volumes. You can create image-based or file-based backups and then perform those operations immediately or at a later time. In addition, you can choose to perform full backups or incremental backups based on the last performed full backup. A maximum of six incremental backups can be performed based on the last full backup performed through the SANtricity Cloud Connector application.



All timestamps for backup and restore jobs listed under the SANtricity Cloud Connector application use local time.

Create a new image-based backup

You can create new image-based backups through the Create function on the Backups page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector.

Steps

1. In the Backups page, click **Create**.

The Create Backup window is displayed.

2. Select **Create an image-based backup**.

3. Click **Next**.

A list of available E-Series volumes is displayed in the Create Backup window.

4. Select the desired E-Series volume and click **Next**.

The **Name the backup and provide a description** page of Create Backup confirmation window is displayed.

5. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.

6. If needed, add a description for the backup in the **Job Description** field.



You should enter a job description that allows you to easily identify the contents of the backup.

7. Click **Next**.

A summary of the selected image-based backup is displayed under the **Review backup information** page of the Create Backup window.

8. Review the selected backup and click **Finish**.

The confirmation page of the Create Backup window is displayed.

9. Select one of the following options:

- **YES** — Initiates a full backup for the selected backup.
- **NO** — A full backup for the selected image-based backup is not performed.



A full backup for the selected image-based backup can be performed at a later time through the Run function on the Backups page.

10. Click **OK**.

The backup for the selected E-Series volume is initiated, and the status for the task is displayed under the

result list section of the Backups page.

Create a new folder/file-based backup

You can create new folder/file-based backups through the Create function on the Backups page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector.

A file-based backup unconditionally backs up all files on the filesystem you specify. However, you can perform a selective restore of files and folders.

Steps

1. In the Backups page, click **Create**.

The Create Backup window is displayed.

2. Select **Create a folder/file-based backup**.
3. Click **Next**.

A list of volumes containing file systems available for backup is displayed in the Create Backup window.

4. Select the desired volume and click **Next**.

A list of available filesystems on the selected volume is displayed in the Create Backup window.



If your filesystem does not appear, verify your filesystem type is supported by the SANtricity Cloud Connector application. For more information, refer to [Supported file systems](#).

5. Select the desired filesystem containing the folder or files to backup, and click **Next**.

The **Name the backup and provide a description** page of Create Backup confirmation window is displayed.

6. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.
7. If needed, add a description for the backup in the **Job Description** field.



You should enter a job description that allows you to easily identify the contents of the backup.

8. Click **Next**.

A summary of the selected folder/file-based backup is displayed under the **Review backup information** page of the Create Backup window.

9. Review the selected folder/file-based backup and click **Finish**.

The confirmation page of the Create Backup window is displayed.

10. Select one of the following options:

- **YES** — Initiates a full backup for the selected backup.

- **NO** — A full backup for the selected backup is not performed.



A full backup for the selected file-based backup can also be performed at a later time through the Run function on the Backups page.

11. Click **Close**.

The backup for the selected E-Series volume is initiated, and the status for the task is displayed under the result list section of the Backup page.

Run Full and Incremental Backups

You can perform full and incremental backups through the Run function on the Backups page. Incremental backups are only available for file-based backups.

Before you begin

Make sure you have created a backup job through the SANtricity Cloud Connector.

Steps

1. In the Backups tab, select the desired backup job and click **Run**.



A full backup is performed automatically whenever an image-based backup job or a backup job without a previously performed initial backup is selected.

The Run Backup window is displayed.

2. Select one of the following options:

- **Full** — Backs up all data for the selected file-based backup.
- **Incremental** — Backs up changes made only since the last performed backup.



A maximum number of six incremental backups can be performed based on the last full backup performed through the SANtricity Cloud Connector application.

3. Click **Run**.

The backup request is initiated.

Delete a backup job

The Delete function deletes backed up data at the specified target location for the selected backup along with backup set.

Before you begin

Make sure there is a backup with a status of Completed, Failed, or Canceled.

Steps

1. In the Backups page, select the desired backup and click **Delete**.



If a full base backup is selected for deletion, all associated incremental backups are also deleted.

The Confirm Delete window is displayed.

2. In the **Type delete** field, type `DELETE` to confirm the delete action.
3. Click **Delete**.

The selected backup is deleted.

Restores

You can access the Restore option in the left navigation panel of the SANtricity Cloud Connector application. The Restore option displays the Restore page, which allows you to create new image-based or file-based restore jobs.

The SANtricity Cloud Connector uses the concept of jobs to perform the actual restore of an E-Series volume. Before performing a restore, you must identify which E-Series volume will be used for the operation. After you add an E-Series volume for restore to the SANtricity Cloud Connector host, you can use the `Restore` page of the SANtricity Cloud Connector application to create and process restores.



All timestamps for backup and restore jobs listed under the SANtricity Cloud Connector application use local time.

Create a new image-based restore

You can create new image-based restores through the Create function on the Restore page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have an image-based backup available through the SANtricity Cloud Connector.

Steps

1. In the Restore page of the SANtricity Cloud Connector application, click **Create**.

The Restore window is displayed.

2. Select the desired backup.
3. Click **Next**.

The Select Backup Point page is displayed in the Restore window.

4. Select the desired completed backup.
5. Click **Next**.

The Select Restore Target page is displayed in the Restore window.

6. Select the restore volume and click **Next**.
7. Review the selected restore operation and click **Finish**.

The restore for the selected target host volume is initiated, and the status for the task is displayed in the result list section of the Restore page.

Create a new file-based restore

You can create new file-based restores through the Create function in the Restore page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have a file-based backup available through the SANtricity Cloud Connector.

Steps

1. In the Restore page of the SANtricity Cloud Connector application, click **Create**.

The Restore window is displayed.

2. In the Restore window, select the desired file-based backup.

3. Click **Next**.

The Select Backup Point page is displayed in the Create Restore Job window.

4. In the Select Backup Point page, select the desired completed backup.

5. Click **Next**.

A list of available filesystems or folders/files page is displayed in the Restore window.

6. Select the desired folders or files to restore and click **Next**.

The Select Restore Target page is displayed in the Restore window.

7. Select the restore volume and click **Next**.

The Review page is displayed in the Restore window.

8. Review the selected restore operation and click **Finish**.

The restore for the selected target host volume is initiated, and the status for the task is displayed in the result list section of the Restore page.

Delete a restore

You can use the Delete function to delete a selected restore item from the result list section of the Restore page.

Before you begin

Make sure there is a restore job with a status of Completed, Failed or Canceled.

Steps

1. In the Restore page, click **Delete**.

The Confirm Delete window is displayed.

2. In the **Type delete** field, type `delete` to confirm the delete action.

3. Click **Delete**.



You cannot delete a suspended restore.

The selected restore is deleted.

Modify the SANtricity Cloud Connector settings

The Settings option allows you to modify the application's current configurations for the S3 account, managed storage arrays and hosts, and Web Services Proxy credentials. You can also change the password for the SANtricity Cloud Connector application through the Settings option.

Modify S3 Account settings

You can modify existing S3 settings for the SANtricity Cloud Connector application in the S3 Account Settings window.

Before you begin

When modifying the URL or S3 Bucket Label settings, be aware that access to any existing backups configured through the SANtricity Cloud Connector will be affected.

Steps

1. In the left toolbar, click **Settings > Configuration**.

The Settings - Configuration page is displayed.

2. Click **View/Edit Settings** for S3 Account Settings.

The S3 Account Settings page is displayed.

3. In the URL file, enter the URL for the S3 cloud service.
4. In the **Access Key ID** field, enter the access ID for the S3 target.
5. In the **Secret Access Key** field, enter the access key for the S3 target.
6. In the **S3 Bucket Name** field, enter the bucket name for the S3 target.
7. Select the **Use Path Style Access** check box if needed.
8. Click **Test Connection** to verify the connection for the entered S3 credentials.
9. Click **Save** to apply the modifications.

The modified S3 account settings are applied.

Manage storage arrays

You can add or remove storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector host in the Manage Storage Arrays page.

The Manage Storage Arrays page displays a list of storage arrays from the Web Services Proxy available for registration with the SANtricity Cloud Connector host.

Steps

1. In the left toolbar, click **Settings > Storage Arrays**.

The Settings - Storage Arrays screen is displayed.

2. To add storage arrays to the SANtricity Cloud Connector, click **Add**.
 - a. In the Add Storage Arrays window, select each checkbox next to the desired storage arrays from the result list.
 - b. Click **Add**.

The selected storage array is added to the SANtricity Cloud Connector and displays in the result list section of the Settings - Storage Arrays screen.

3. To modify the host for an added storage array, click **Edit** for the line item in the result list section of the Settings - Storage Arrays screen.
 - a. In the Associated Host drop-down menu, select the desired host for the storage array.
 - b. Click **Save**.

The selected host is assigned to the storage array.

4. To remove an existing storage array from the SANtricity Cloud Connector host, select the desired storage arrays from the bottom result list, and click **Remove**.
 - a. In the Confirm Remove Storage Array field, type REMOVE.
 - b. Click **Remove**.

The selected storage array is removed from the SANtricity Cloud Connector host.

Modify Web Services Proxy settings

You can modify existing Web Services Proxy settings for the SANtricity Cloud Connector application in the Web Services Proxy Settings window.

Before you begin

The Web Services Proxy used with the SANtricity Cloud Connector needs to have the appropriate arrays added and the corresponding password set.

Steps

1. In the left toolbar, click **Settings > Configuration**.

The Settings - Configuration screen is displayed.

2. Click **View/Edit Settings** for Web Services Proxy.

The Web Services Proxy settings screen is displayed.

3. In the URL field, enter the URL for the Web Services proxy used for the SANtricity Cloud Connector.
4. In the User Name field, enter the user name for the Web Services Proxy connection.
5. In the Password field, enter the password for the Web Services Proxy connection.
6. Click **Test Connection** to verify the connection for the entered Web Services Proxy credentials.
7. Click **Save** to apply the modifications.

Change SANtricity Cloud Connector password

You can change the password for the SANtricity Cloud Connector application in the Change Password screen.

Steps

1. In the left toolbar, click **Settings** > **Configuration**.

The Settings - Configuration screen is displayed.

2. Click **Change Password** for SANtricity Cloud Connector.

The Change Password screen is displayed.

3. In the Current password field, enter your current password for the SANtricity Cloud Connector application.
4. In the New Password field, enter your new password for the SANtricity Cloud Connector application.
5. In the Confirm new password field, re-enter the new password.
6. Click **Change** to apply the new password.

The modified password is applied to the SANtricity Cloud Connector application.

Uninstall the SANtricity Cloud Connector

You can uninstall the SANtricity Cloud Connector through the graphical uninstaller or console mode.

Uninstall using graphical mode

You can use the graphical mode to uninstall the SANtricity Cloud Connector on a Linux operating system.

Steps

1. From a terminal window, navigate to the directory containing the SANtricity Cloud Connector uninstall file.

The uninstall file for the SANtricity Cloud Connector is available at the following default directory location:

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. From the directory containing the SANtricity Cloud Connector uninstall file, run the following command:

```
./uninstall_cloud_connector4 -i gui
```

The uninstall process for the SANtricity Cloud Connector is initialized.

3. In the uninstall window, click **Uninstall** to proceed with uninstalling the SANtricity Cloud Connector.

The uninstall process is completed, and the SANtricity Cloud Connector application is uninstalled in the Linux operating system.

Uninstall using console mode

You can use the console mode to uninstall the SANtricity Cloud Connector on a Linux operating system.

Steps

1. From a terminal window, navigate to the directory containing the SANtricity Cloud Connector uninstall file.

The uninstall file for the SANtricity Cloud Connector is available at the following default directory location:

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. From the directory containing the SANtricity Cloud Connector uninstall file, run the following command:

```
./uninstall_cloud_connector4 -i console
```

The uninstall process for the SANtricity Cloud Connector is initialized.

3. In the uninstall window, press **Enter** to proceed with uninstalling the SANtricity Cloud Connector.

The uninstall process is completed, and the SANtricity Cloud Connector application is uninstalled in the Linux operating system.

Earlier versions

Check out the links below to access documentation for earlier versions of E-Series hardware and SANtricity software. The links take you to a different documentation site.

Hardware documentation for earlier releases

- [Install E2712, E2724, E5612, E5624 controller-drive trays and DE1600 and DE5600 expansion drive trays](#)
- [Install E2760 and E5660 controller-drive trays and DE6600 expansion drive trays](#)
- [Install EF560 flash arrays and DE5600 flash expansion trays](#)
- [Install older systems](#)
- [Maintain older systems](#)
- [Add second controller to E2600 and E2700](#)
- [Change or add host protocols](#)
- [Convert from AC to DC power](#)

Software documentation for earlier releases

SANtricity Release 11.6

- [System Manager online help](#)
- [Unified Manager online help](#)

SANtricity Release 11.5

- [System Manager online help](#)

SANtricity Release 11.4

- [AMW \(E2700, E5600/EF560\) online help](#)
- [EMW \(E2700, E5600/EF560\) online help](#)

Technical reports

Browse platform technical reports

Platform TRs

| | | |
|---|--|---|
| TR-4725: E2800 arrays feature overview | TR-4724: E5700 arrays feature overview | TR-4877: EF300 arrays feature overview |
| Describes the hardware and software features of the E2800 hybrid array and the latest SANtricity OS features. | Describes E5700 product information including new hardware and software features introduced with the latest version of SANtricity. | Describes the hardware and software features of the EF300 all-flash array and new SANtricity OS features. |
| TR-4800: EF600 arrays feature overview | | |
| Describes the hardware and software features of the EF600 all-flash array and new SANtricity OS features. | | |

Browse security technical reports

Security TRs

| | | |
|--|--|---|
| TR-4474: SANtricity Drive Security Feature Guide | TR-4712: SANtricity Management Security Features | TR-4813: Managing Certificates for E-Series Systems |
| Describes the full disk encryption feature for E-Series systems, including support for FIPS 140-2 validated drives, and both internal and external key management support. | Describes SANtricity security features for NetApp E-Series E2800, E5700, EF280, EF570, EF300, and EF600 storage systems. | Describes how to manage security certificates with the latest E-Series controllers and applications. |
| TR-4855: Security Hardening Guide for SANtricity | | |
| Describes how to deploy SANtricity to meet prescribed security objectives for information system confidentiality, integrity, and availability. | TR-4853: Access Management for E-Series Systems | Describes how to configure Access Management, including role-based access control (RBAC), Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML). |

Browse featured technical reports

Feature TRs

| | | |
|--|---|--|
| TR-4893: SANtricity Remote Storage Volumes | TR-4839: SANtricity Synchronous and Asynchronous Mirroring | TR-4747: SANtricity Snapshot Feature Overview and Deployment Guide |
| Describes the solution architecture and how to use the E-Series storage system to import data from an existing remote storage device. | Describes the SANtricity Synchronous and Asynchronous Mirroring feature. | Describes the SANtricity Snapshot feature including GUI navigation instructions using SANtricity System Manager. |
| TR-4652: SANtricity Dynamic Disk Pools | TR-4737: SANtricity Automatic Load Balancing | TR-4736: SANtricity Web Services API |
| Describes how storage administrators can group sets of like disks into a pool topology where all the drives in the pool participate in the I/O workflow. | Describes an overview of the behavior of the ALB feature, its key configuration parameters, and its host interoperability enhancements. | Describes an overview of SANtricity Web Services, an API used for configuring and managing E-Series storage systems. |

Browse solution technical reports

Splunk

| | |
|---|--|
| TR-4623: E5700 with Splunk Enterprise | TR-4903: EF300 with Splunk Enterprise |
| Describes the integrated architecture of the E5700 system and Splunk design. This document also summarizes the performance test results obtained from a Splunk machine log event simulation tool. | Describes the integrated architecture of the EF300 all-flash array and Splunk design. This document also summarizes the performance test results obtained from a Splunk machine log event simulation tool. |

Enterprise Databases

| | |
|--|--|
| TR-4764: Best Practice Guide for Microsoft SQL Server with NetApp EF-Series | TR-4794: Oracle Databases on NetApp EF-Series |
| Helps storage administrators and database administrators successfully deploy Microsoft SQL Server on NetApp EF-Series storage. | Helps storage administrators and database administrators successfully deploy Oracle on NetApp EF-Series storage. |

Backup & Recovery

TR-4320: Best Practices with Commvault Data Platform V11

Describes the reference architecture and best practices when using NetApp E-Series storage in a Commvault Data Platform V11 environment.

TR-4471: Best Practices with Veeam Backup and Replication

Describes the reference architecture and best practices when using NetApp E-Series storage in a Veeam Backup & Replication 9.5 environment.

TR-4704: Deploying Veritas NetBackup with NetApp E-Series Storage

Describes the deployment of Veritas NetBackup on NetApp E-Series storage.

VSS

TR-4825: NetApp E-Series for Video Surveillance Best Practice Guide

Describes best practices for deploying E-Series arrays into video surveillance environments.

TR-4818: Virtualizing Video Management Systems with NetApp E-Series Storage

Describes how to design and deploy video management systems with NetApp E-Series storage.

TR-4848: Bosch Video Recording Solution with NetApp E-Series E2800 Disk Storage Array

Describes the video surveillance solution architecture and includes details of the components and storage best practices.

HPC

TR-4884: Entry-level HPC systems with NetApp E-Series and IBM Spectrum Scale

Describes the reference architecture for entry-level HPC systems based on NetApp E-Series storage systems and IBM Spectrum Scale.

TR-4859: Deploying IBM Spectrum Scale with NetApp E-Series Storage

Describes the process of deploying a full parallel file system solution based on IBM's Spectrum Scale software stack.

TR-4856: BeeGFS High Availability with E-Series using Red Hat Enterprise Linux Server

Describes the required configurations for implementing high availability in a BeeGFS architecture backed by the NetApp E-Series system and using RedHat Enterprise Linux for BeeGFS storage, metadata and management services.

TR-4862: BeeGFS High Availability with E-Series using SUSE Linux Enterprise Server

Describes the required configurations for implementing high availability in a BeeGFS architecture backed by the NetApp E-Series system and using SUSE Linux Enterprise Server for BeeGFS storage, metadata, and management services.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[Notice for E-Series/EF-Series SANtricity OS](#)

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.