Technical Report

Introduction to NetApp EF600 array

Feature overview with SANtricity

Mitch Blackburn, NetApp

November 2024 | TR-4800

Abstract

The NetApp® EF600 NVMe (NVM Express) all-flash array delivers optimal performance without compromising on the Reliability, Availability, and Serviceability (RAS) features that deliver up to 99.9999% availability. This document provides detailed information about the hardware and software features of the EF600 all-flash array and new NetApp SANtricity® OS features. The newest release of the EF600 array broadens the abilities of the array to manage more use cases with SAS expansion shelves supporting NL-SAS HDD drives.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

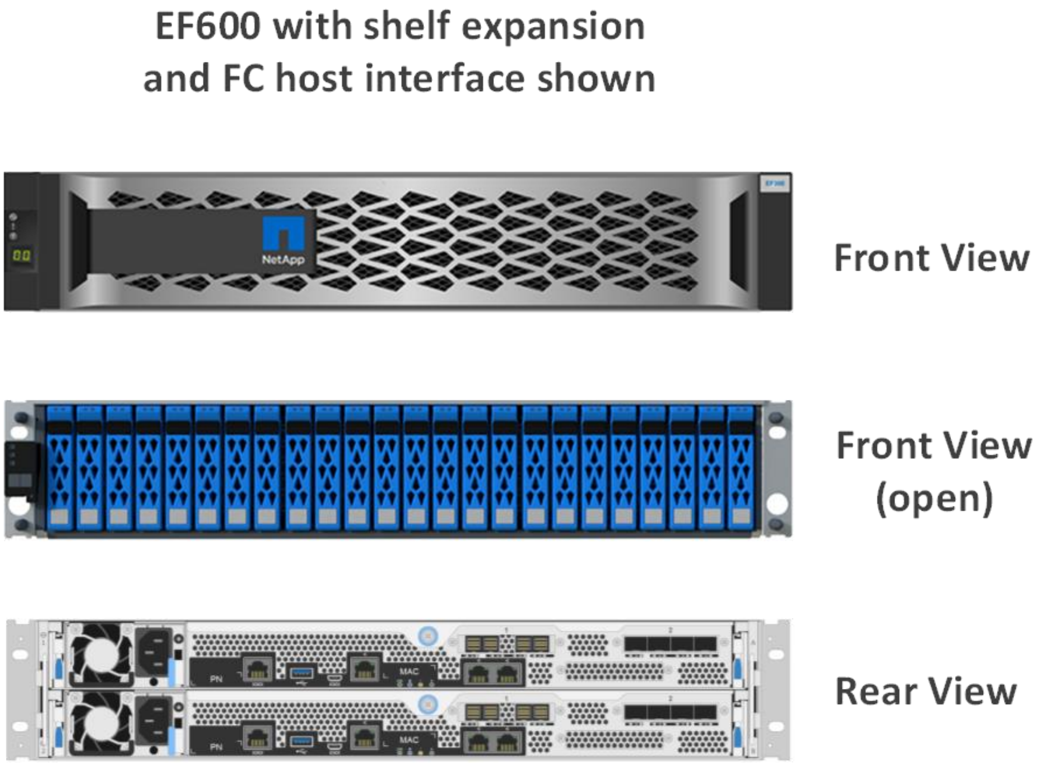
NetApp EF600 arrays have a modern look, as shown in Figure 1, use end-to-end NVMe NE224 drive shelves, and are managed by the secure web-based NetApp SANtricity System Manager UI. The array's performance capabilities enable new-generation analytics and artificial intelligence (AI) workloads to run faster.

The EF600 can also provide SAS expansion shelves for additional use cases, such as a hot and cold tier for Splunk or a backup location for a high-performance Oracle database.

The release of SANtricity OS 11.80 increases the breadth of use cases for the EF-Series with the following improvements:

- Addition of support for expansion shelves without requiring any NVMe drives in the controller shelf.
- Ability to provide up to 8TB of SSD read cache for HDD drives in the expansion shelves.
- Capability to asynchronously mirror from SAS drives in the expansion shelves to SAS drives in another E-Series system or from the NVMe drives to another system with NVMe drives.

Figure 1) New-generation EF600 all-flash array.



In one powerful all-flash array package, the EF600 array delivers optimal performance for both random workloads and large sequential workloads. The array can deliver consistent response times for up to two million 4KB random read IOPS at 250µsec with as few as 24 NVMe SSDs. The same configuration can deliver up to 44GBps large sequential read throughput and about 12.5GBps cache-mirrored large sequential write throughput. When your workload meets the criteria of the built-in full stripe write acceleration feature, you can accelerate write performance up to 24GBps.

The EF600 array is used for storage solutions that require the depth of enterprise-grade SAN storage and that consistently deliver response times in the sub-150µsec range. The array supports the SCSI over FC protocol and the NVMe/FC protocol on the 32Gb FC host interface card (HIC). The iSCSI protocol is supported on the 25Gb iSCSI HIC. NVMe/IB, NVMe/RoCE, and iSER/IB are supported on the 200Gb HIC whereas the 100Gb HIC has additional support for SRP/IB as well as the other IB protocols.

Note: NVMe/IB, NVMe/RoCE, and NVMe/FC protocols are supported on the EF600. The EF570 and E5700 controllers also support these protocols with the 64GB memory option.

This performance versatility is enhanced by multiple SSD choices to achieve the price/performance combination that fits your business need. Current drive choices include:

- Entry-level 1.9TB SSDs for small fast, random workloads
- Fast, large-capacity (3.8TB) SSDs to support higher-capacity sequential workloads, random workloads, or mixed workloads
- 7.6TB and 15.3TB SSDs for fast, large-capacity requirements

EF-Series products have a documented history of delivering up to 99.9999% availability when systems are properly sized, deployed, and maintained with NetApp Support agreements. EF-Series products also include NetApp AutoSupport® technology to enhance your ongoing product experience.

Each EF600 controller provides a single Ethernet management port for out-of-band management. The EF600 array also introduces new, faster host interface options that fit the needs of the world’s most demanding storage environments. These options are in one easy-to-install and easy-to-maintain hardware and integrated management software package.

This package includes your choice of the following HICs:

- Two four-port 25Gb iSCSI
- Two four-port 32Gb FC (OM4 fiber required)
- Two two-port 100Gb IB (requires 100Gb-capable cables and host channel adapters [HCAs])
- One two-port 200Gb IB (requires 200Gb-capable cables and HCAs)

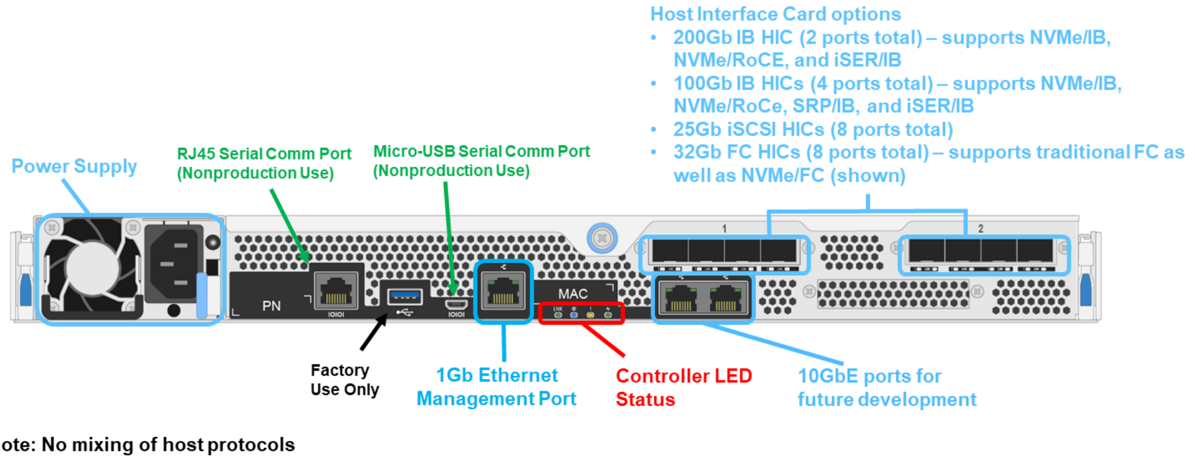
Note: If the optional 12Gb SAS drive expansion card is installed in HIC 1 slot, then only one HIC card can be used.

Note: It is not possible to use the 200Gb IB HIC card with the optional 12Gb SAS expansion card installed.

Note: You can download and install a software feature pack in the field to change the host protocol between the various available protocols on each HIC.

Figure 2 identifies the various interface ports on the EF600 controller without the optional drive expansion card.

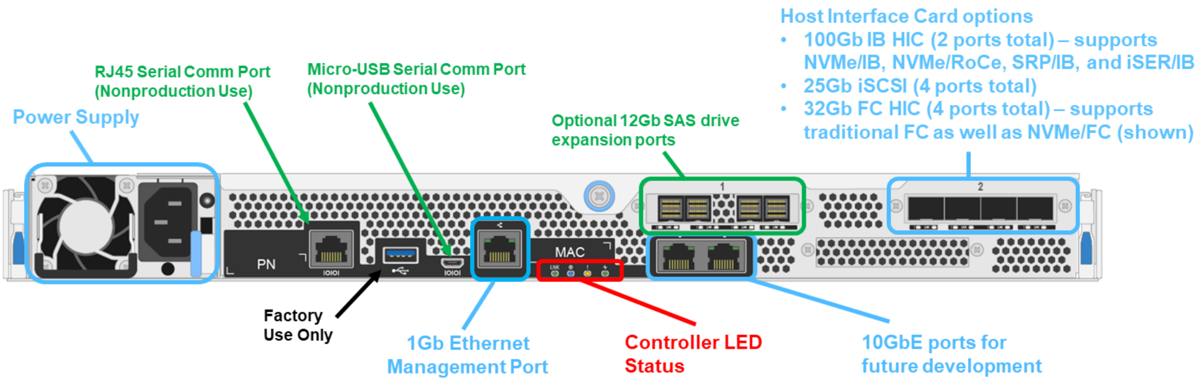
Figure 2) EF600 controller with ports identified.


Host Interface Card options
• 200Gb IB HIC (2 ports total) – supports NVMe/IB, NVMe/RoCE, and iSER/IB
• 100Gb IB HICs (4 ports total) – supports NVMe/IB, NVMe/RoCe, SRP/IB, and iSER/IB
• 25Gb iSCSI HICs (8 ports total)
• 32Gb FC HICs (8 ports total) – supports traditional FC as well as NVMe/FC (shown)
Power Supply
RJ45 Serial Comm Port (Nonproduction Use)
Micro-USB Serial Comm Port (Nonproduction Use)
PN
MAC
1
2
Factory Use Only
1Gb Ethernet Management Port
Controller LED Status
10GbE ports for future development

Note: No mixing of host protocols

Figure 3 shows the EF600 controller with the optional 12Gb SAS expansion card installed.

Figure 3) EF600 with optional 12Gb SAS drive expansion ports.


Host Interface Card options
• 100Gb IB HIC (2 ports total) – supports NVMe/IB, NVMe/RoCe, SRP/IB, and iSER/IB
• 25Gb iSCSI (4 ports total)
• 32Gb FC HIC (4 ports total) – supports traditional FC as well as NVMe/FC (shown)
RJ45 Serial Comm Port (Nonproduction Use)
Micro-USB Serial Comm Port (Nonproduction Use)
Power Supply
Optional 12Gb SAS drive expansion ports
PN
MAC
1
2
Factory Use Only
1Gb Ethernet Management Port
Controller LED Status
10GbE ports for future development

Note: No mixing of host protocols

Note: Type-A USB port for factory use only is disabled if using SANtricity OS 11.80 or newer.

For optical connections, you must order appropriate SFP modules for your specific implementation. Consult the NetApp Hardware Universe for a full listing of available host interface equipment.

For detailed instructions about how to change host protocols, go to Upgrading > Hardware Upgrade on the E-Series and SANtricity 11 Resources page.

The EF600 continues the E-Series legacy of providing fast, simple, reliable, and flexible SAN storage regardless of the workload. NetApp EF600 all-flash arrays can support the workload if the following conditions are met:

- Hosts are qualified with EF-Series arrays.
- The hosts use SAN access to the storage, whether directly connected or fabric connected.
- The storage is managed at the host or file system level.

In fact, some of the world’s most demanding online transactional workloads run on EF-Series arrays because these arrays are blazing fast, simple to install and operate, and extremely reliable, providing up to 99.9999% data availability. These highly flexible SAN building blocks can be applied when you need them and can be plugged into your current application environment on demand without disrupting your primary storage management strategy. EF-Series arrays can operate in a space as small as 2U, seamlessly integrate with many software layers, and still deliver consistently low-latency performance. These capabilities make EF-Series arrays an optimal SAN building block for any size enterprise that needs to support demanding online or database-reliant workloads.

Whether you are running Oracle Automatic Storage Management (ASM), Microsoft SQL Server, Splunk real-time analytics, or specialty applications with demanding response-time requirements, the EF600 array maintains its performance profile. To fully maximize performance, only minor setting changes are required when you create disk pools, volume groups, or volumes to switch between high-IOPS configurations and high-throughput configurations. This characteristic makes EF-Series arrays easy to deploy regardless of your workload.

EF600 arrays use the web-based NetApp SANtricity System Manager UI to manage individual arrays, and SANtricity Unified Manager enables you to organize and manage multiple new-generation E-Series and EF-Series arrays from the new API-based central management application. The built-in web services API integration or the management client-based web services package makes the EF-Series product line easier than ever to integrate with your standard API-driven environment.

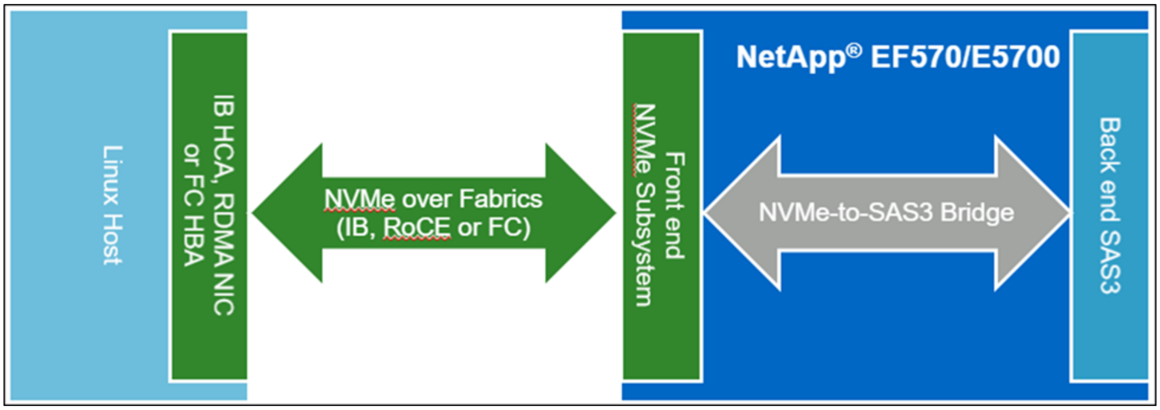
The following sections provide broad product information, including technical details about SANtricity features. Some familiarity with basic configuration concepts such as volumes, Dynamic Disk Pools (DDP), and RAID volume groups is assumed.

Key architectural differences between EF600 and previous-generation EF-Series arrays

End-to-end NVMe

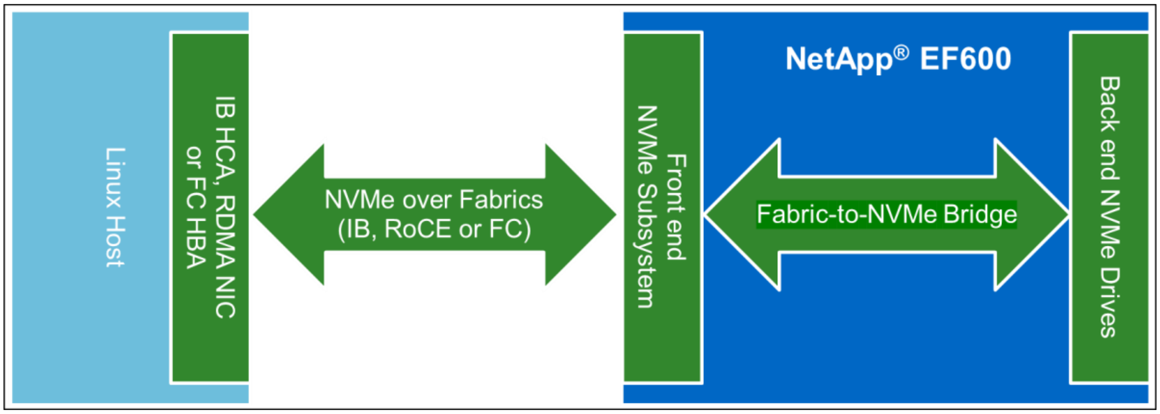
This is not the first venture into NVMe for NetApp EF-Series arrays. NetApp EF570 and E5700 systems set the stage for the NetApp EF600 system. The same NVMe over Fabrics (NVMe-oF) protocols that are available on the EF600 are also available on the EF570 and E5700 systems: NVMe/FC, NVMe/RoCE, and NVMe/IB. However, these systems were not end-to-end NVMe and only supported NVMe on the front end from the host to the HIC and SCSI from the HIC to the drives, as shown in Figure 4. This approach enabled NetApp to drop the latency on the front end by roughly 20µsec.

Figure 4) NVMe-oF front-end only on the EF570 and E5700.



The EF600 now supports end-to-end NVMe from the host to the drives (Figure 5). For more information about the NetApp E-Series implementation of NVMe technology, see TR-4766: NetApp E-Series and NVMe over Fabrics Support.

Figure 5) End-to-end NVMe on the EF600.



Advanced format (4KB block format)

The primary reason for implementing a 4KB block format on the EF600 is to take advantage of the change to NVMe drive technology. A side effect is that you cannot migrate 512B format drives (available on previous systems such as the EF570) over to the EF600 by simply importing the drives.

A second advantage of moving to a larger block size is the need for less metadata management for the same capacity volumes. This advantage allows you to raise the maximum disk pool capacity without adding more records to the configuration database. It also reduces metadata overhead for the configuration database itself on the EF600.

Tracking of data in cache is also less granular compared with the 512B block format. Therefore, there are future opportunities to support larger cache block sizes.

512e support

Despite the advantages of a 4KB block format, there are environments where 512B support is needed. VMware ESXi lacks support of 4KB blocks for external storage, as does the NetApp iSCSI HIC. SANtricity OS 11.70 adds 512-byte emulation (512e) on the EF300 and EF600. This enables VMware support for the EF300 and EF600, as well as general support of iSCSI on the NVMe-based platforms for any supported OS. When appropriate, you have the option to select block size when creating a volume. For iSCSI hosts, block size automatically defaults to 512e.

Operating system support of NVMe

There are few operating systems that support NVMe-oF protocols and the multipathing required for these protocols. If you want full end-to-end support for NVMe, you are limited to certain Linux distributions. With the release of 11.70.1, VMware NVMe/FC is also supported.

With SCSI over FC and iSCSI host protocols, you are not limited in operating system choice when you choose EF600.

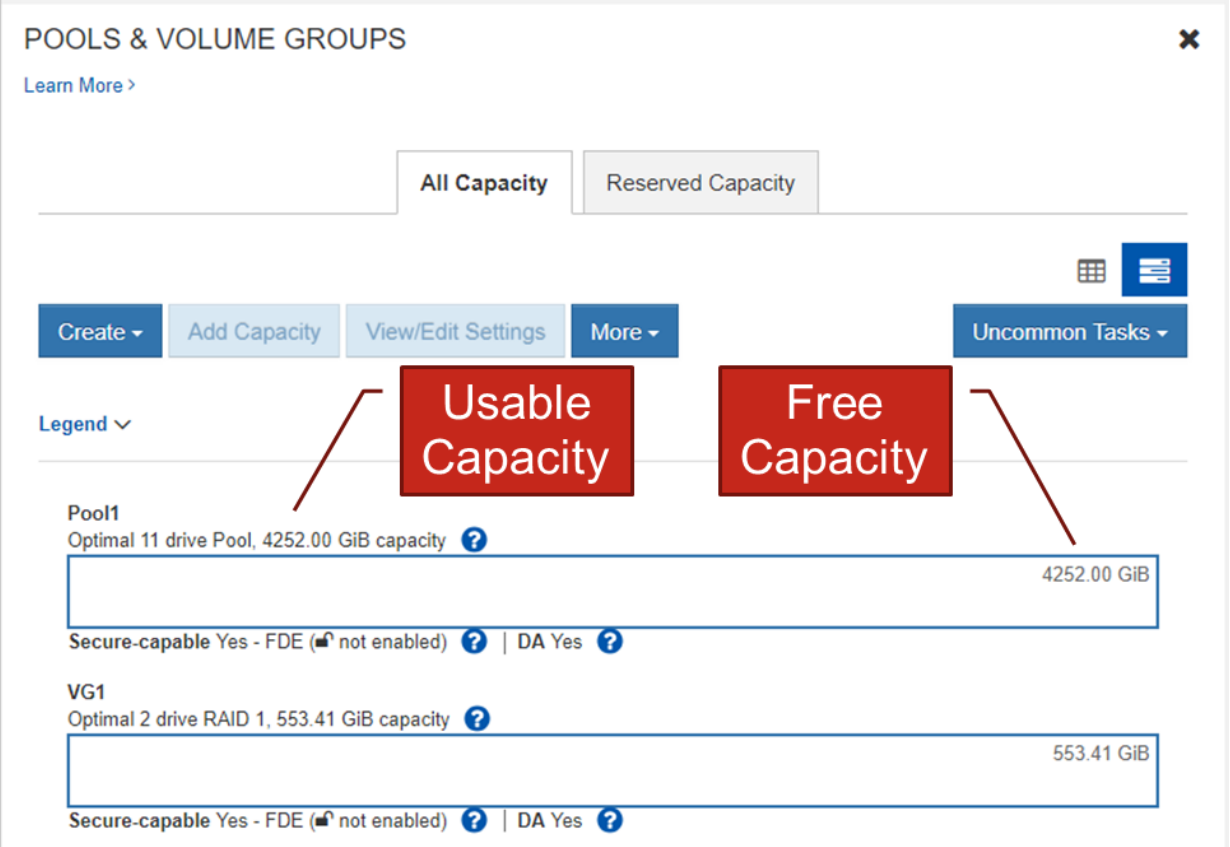
For questions about supported configurations, see the NetApp Interoperability Matrix Tool (IMT).

Endurance and performance optimization

SANtricity capacity optimization with NVMe SSD drives

Beginning in SANtricity 11.60.2, when a volume group or a Dynamic Disk Pool (DDP) is created with the EF600 NVMe SSDs using the System Manager UI, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. A portion of the usable capacity is automatically set aside to increase effective overprovisioning and improve endurance and write performance. The usable capacity and free capacity presented to the user is decreased accordingly, as shown in Figure 6.

Figure 6) Summary view showing usable and free capacity.

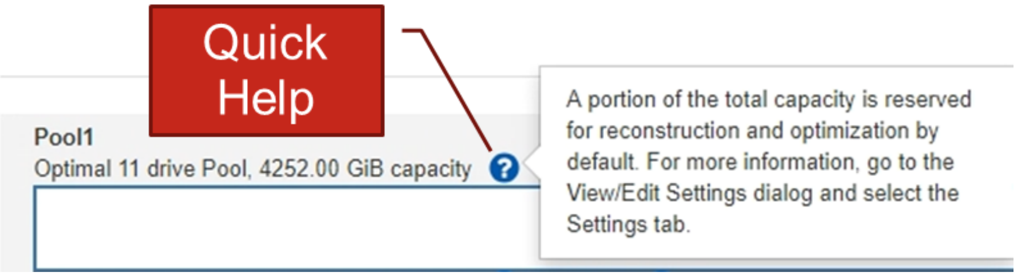


Pool1
Optimal 11 drive Pool, 4252.00 GiB capacity
4252.00 GiB
Secure-capable Yes - FDE (not enabled) | DA Yes

VG1
Optimal 2 drive RAID 1, 553.41 GiB capacity
553.41 GiB
Secure-capable Yes - FDE (not enabled) | DA Yes

A Quick Help function has also been added to the Usable Capacity feature, as shown in Figure 7.

Figure 7) Quick help for usable capacity.



Pool1
Optimal 11 drive Pool, 4252.00 GiB capacity

A portion of the total capacity is reserved for reconstruction and optimization by default. For more information, go to the View/Edit Settings dialog and select the Settings tab.

Users are not prompted to choose an SSD optimization setting when creating a volume group or DDP, just as they are not prompted to select the number of preservation drives when creating a DDP. Instead, System Manager automatically selects a default value for the optimization capacity based on the drive model. Smaller capacity drives need a larger percentage of the total capacity reserved for optimization to increase endurance and to reach performance targets for write-intensive workloads. DDP preservation capacity serves as optimization capacity when not in use for reconstruction, so System Manager automatically decreases the amount of capacity reserved for optimization based on the number of preservation drives in the pool. Table 1 shows the recommended optimization capacities for different drive sizes.

Table 1) Optimization capacity and effective overprovisioning.

Drive capacity	Recommended optimization capacity (System Manager defaults)	Approximate effective overprovisioning
1.92TB	28%	49%
3.84TB	14%	24%
7.68TB	10%	19%
15.36TB	4%	12%

SSD drives have longer life and better maximum write performance when a portion of their capacity is unallocated. The rated endurance is based on the amount of overprovisioning in the SSD.

The topics of endurance, overprovisioning, write amplification factor, and workload conditioning are explored in the Appendix at the end of this document to provide a basis for understanding how leaving free capacity effectively increases the level of overprovisioning in the drives in each volume group or DDP. Increasing overprovisioning can be expected to increase both SSD endurance and maximum sustained write performance, especially for lower-capacity drives.

Note: Optimization capacity is reserved by default only for volume groups or DDPs created with System Manager. It is not reserved for volume groups or DDPs created with the CLI or with existing REST scripts. Optimization capacity settings are managed with the REST key-value endpoint, so REST scripts can be updated to mirror the functionality in System Manager.

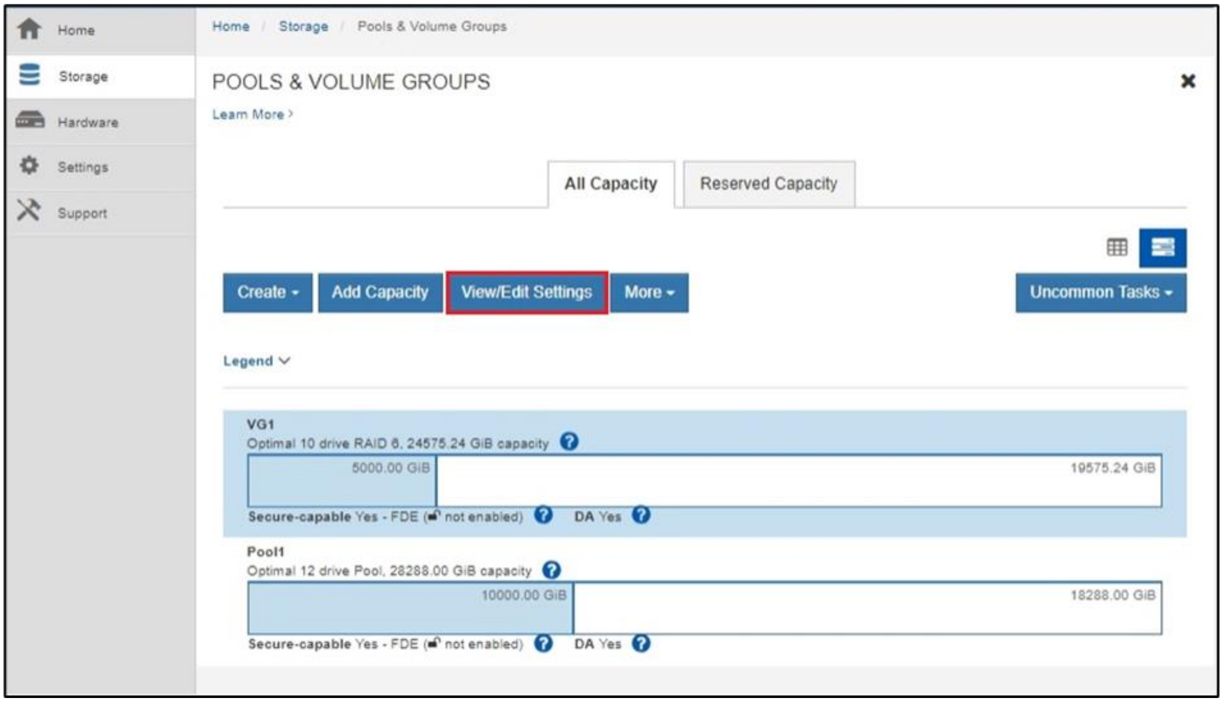
Adjusting capacity optimization

When a volume group or DDP is created, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. The Optimization Capacity slider in the Volume Group Settings dialog box allows adjustments to a volume group's optimization capacity. Adjusting the slider provides for better performance and drive wear life at the expense of available capacity or additional available capacity at the expense of performance and drive wear life.

The appearance of the feature is slightly different for DDPs than for volume groups. It should also be noted that the default percentage for optimization capacity is different for DDPs and volume groups. This difference is due to DDPs having built-in preservation capacity. The default for the feature is to have 14% total preservation capacity between built-in preservation and additional optimization.

The user can increase or decrease the additional capacity set aside after creating the volume group or DDP using a slider. To do so, complete the following steps:

1. In System Manager, go to Storage > Pools & Volume Groups.
2. Select the desired volume group and then click View/Edit Settings.

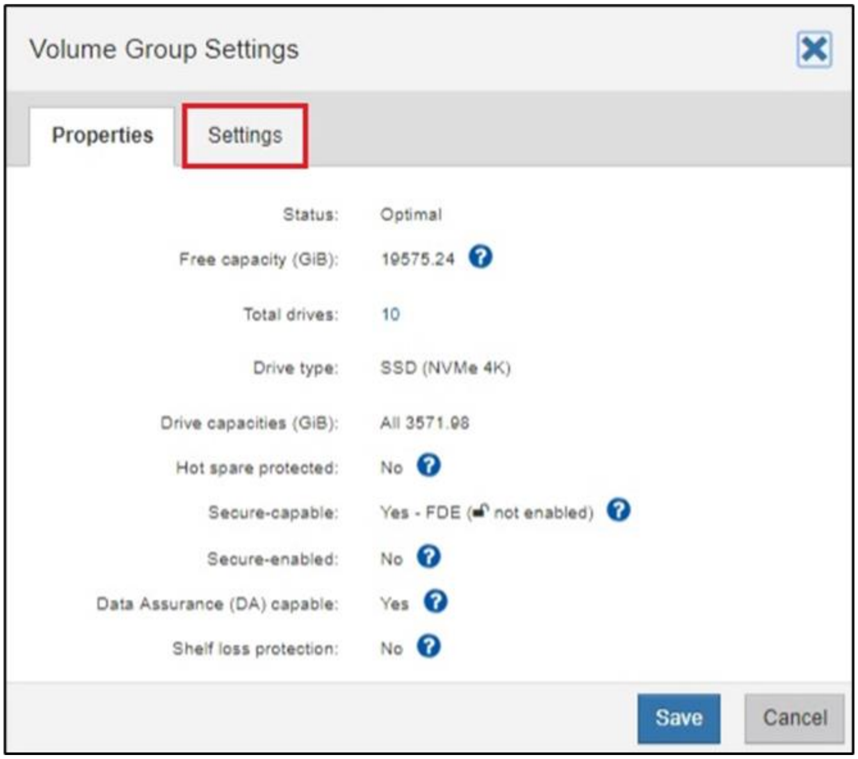


POOLS & VOLUME GROUPS

VG1
Optimal 10 drive RAID 6, 24575.24 GiB capacity
5000.00 GiB 19575.24 GiB
Secure-capable Yes - FDE (not enabled) DA Yes

Pool1
Optimal 12 drive Pool, 28288.00 GiB capacity
10000.00 GiB 18288.00 GiB
Secure-capable Yes - FDE (not enabled) DA Yes

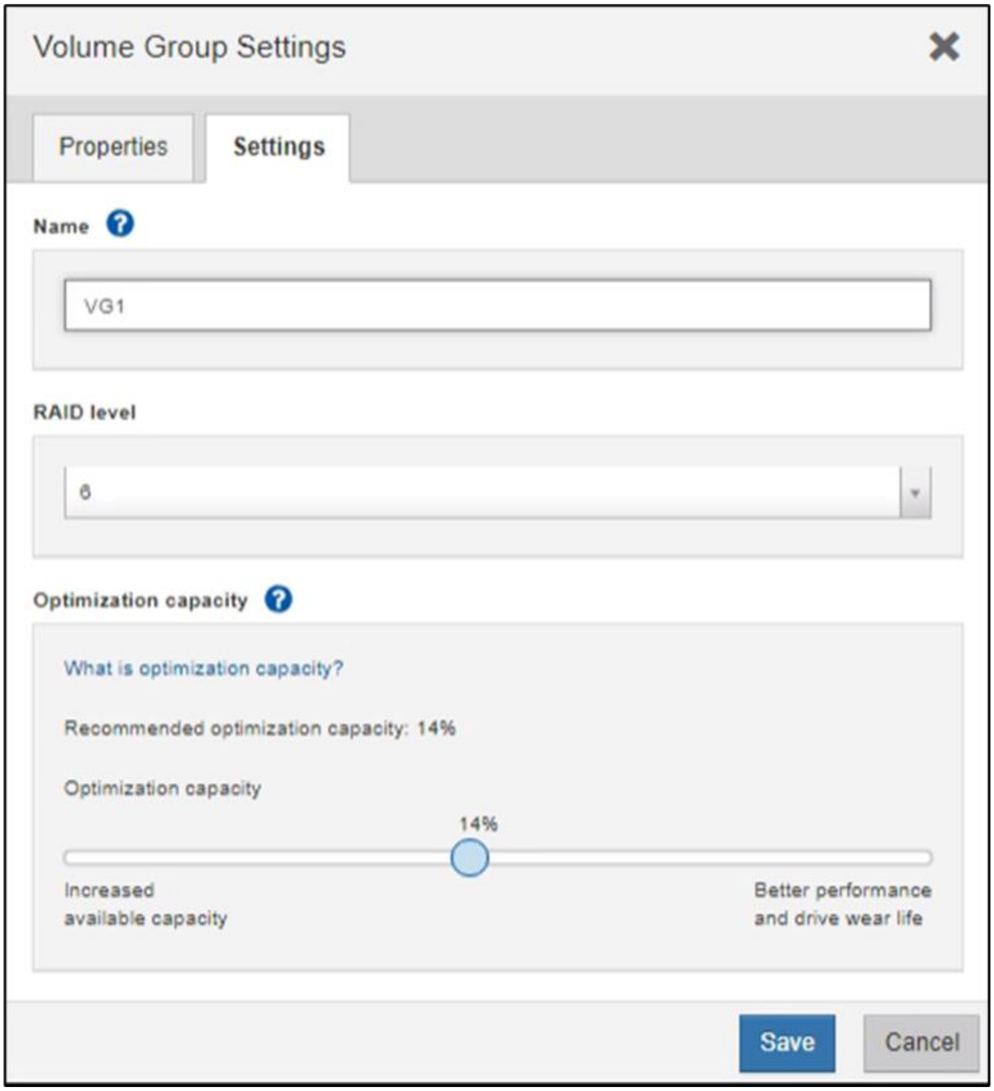
3. Navigate to the Settings tab.



Volume Group Settings

Status: Optimal
Free capacity (GiB): 19575.24
Total drives: 10
Drive type: SSD (NVMe 4K)
Drive capacities (GiB): All 3571.98
Hot spare protected: No
Secure-capable: Yes - FDE (not enabled)
Secure-enabled: No
Data Assurance (DA) capable: Yes
Shelf loss protection: No

4. Use the slider to adjust the Optimization Capacity for Volume Groups.



Name: VG1

RAID level: 6

Optimization capacity

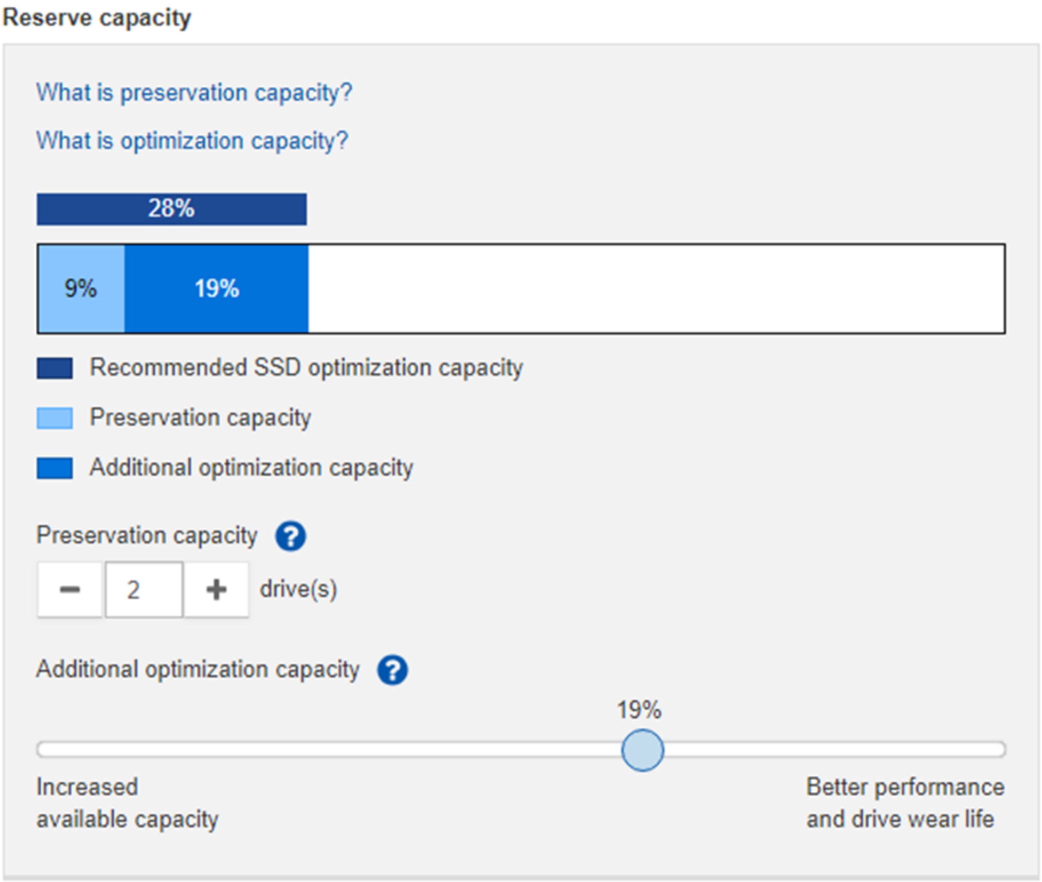
What is optimization capacity?

Recommended optimization capacity: 14%

Optimization capacity: 14%

Increased available capacity — Better performance and drive wear life

5. Or, for DDP, use the slider to adjust the Additional Optimization Capacity.



Reserve capacity
What is preservation capacity?
What is optimization capacity?
28%
9%
19%
Recommended SSD optimization capacity
Preservation capacity
Additional optimization capacity

Preservation capacity ?

− 2 + drive(s)

Additional optimization capacity ?

19%

Increased
available capacity
Better performance
and drive wear life

Note: There is nothing to prevent a user from creating a volume group or DDP with the UI and then using REST to create volumes that exceed the usable capacity presented by the UI, because the UI adjusts to these changes.

Resource-provisioned volumes

Resource provisioning is a feature available in the EF300 and EF600 storage arrays that allows volumes to be put in use immediately with no background initialization process.

A resource-provisioned volume is a thick volume in an SSD volume group or pool where drive capacity is allocated (assigned to the volume) when the volume is created, but the drive blocks are deallocated (unmapped). **This means that there is no time-bound background initialization to affect performance. Instead, each RAID stripe is initialized upon the first write to a volume block in the stripe.**

By comparison, in a traditional thick volume all drive blocks are mapped or allocated during a background volume initialization operation in order to initialize the Data Assurance protection information fields and to make data and RAID parity consistent in each RAID stripe.

Resource-provisioned volumes are supported only on SSD volume groups and pools where all drives in the group or pool support the NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE) error recovery capability.

- If the DULBE capability is present on all drives, RPV is the default and does not have to be chosen.
- When a resource-provisioned volume is created, all drive blocks assigned to the volume are deallocated (unmapped).

In addition, hosts can deallocate logical blocks in the volume using the NVMe Dataset Management command. **Deallocating blocks can improve SSD wear life and increase maximum write performance.** The improvement varies with each drive model and capacity.

For random write workloads, the first write to each stripe has higher latency because the partial stripe writes are turned into a full-stripe operation.

For more information about resource-provisioned volumes, see the E-Series online help center and the E-Series Documentation Center.

Drive loading for maximum performance

With the release of the NE224 shelf, the process by which drive slots are assigned to the PCIe bus has changed. In previous versions of EF-Series, alternate drive slots were assigned to a different PCIe bus. With the EF-600 array, the first PCIe bus is connected to the drive slots 0 through 11, the first 12 drive slots; and the second PCIe bus is connected to drive slots 12 through 23, the second 12 drive slots.

When inserting fewer than 24 drives into an NE224 shelf, you must alternate between the two halves of the drive shelf. You must evenly load drives either from the middle drive slots (11,12) outward, Figure 8, or from the outside drive slots (0, 23) inward, Figure 9.

Note: Storage system performance can be significantly reduced if drives are not loaded so that both PCIe busses are employed.

Figure 8) Loading drives from the inside drive slots outward.

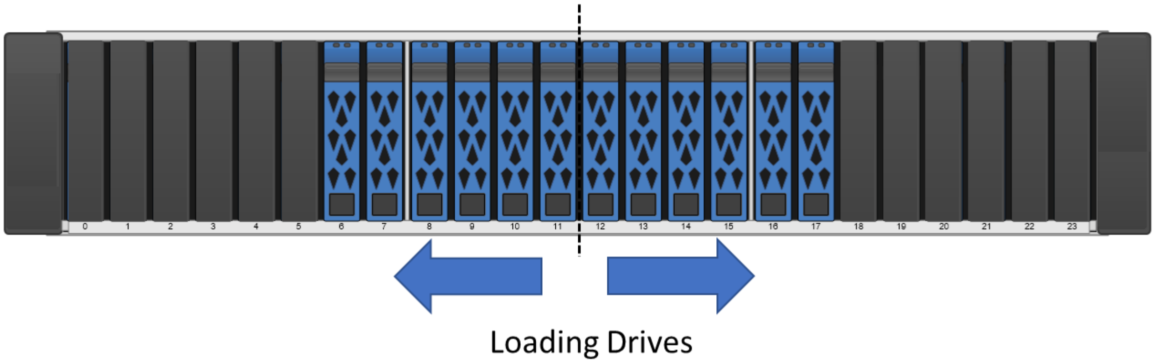
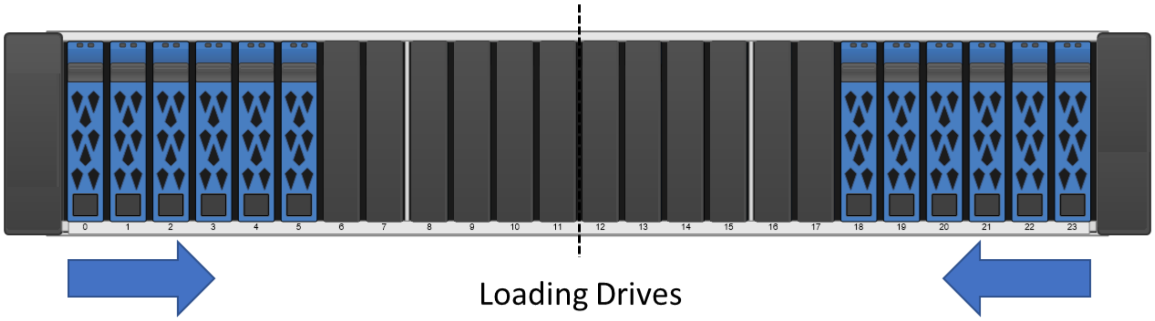


Figure 9) Loading drives from the outside drive slots inward.



When configuring the storage array, each controller should have access to an equal number of drives in the first 12 slots and from the last 12 slots to use both drive-side PCIe busses effectively. After you create a pool or volume group, create an even number of volumes split equally across the two controllers. Figure 10 shows an example of creating a pool from the middle drives. For DDP creation, NetApp recommends using all drives in the storage array.

Figure 10) Example DDP using 12 drives.

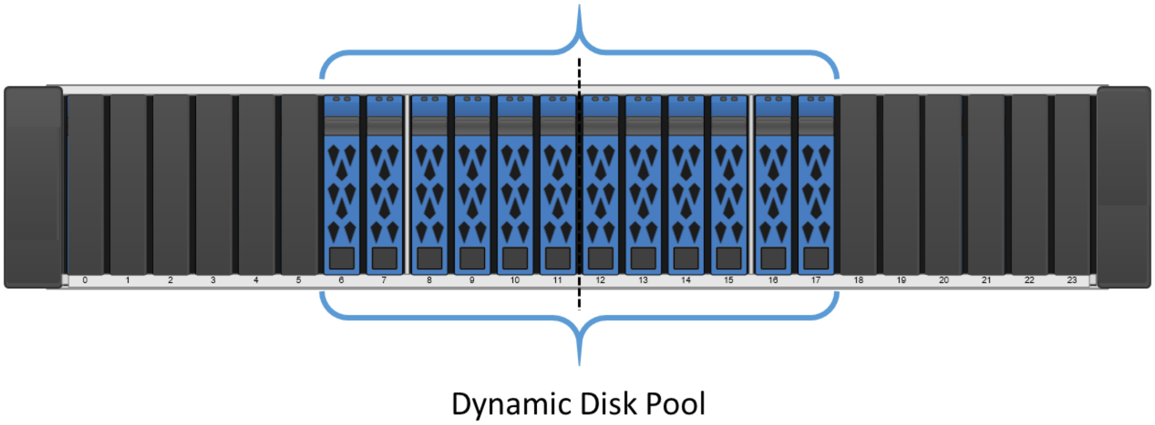
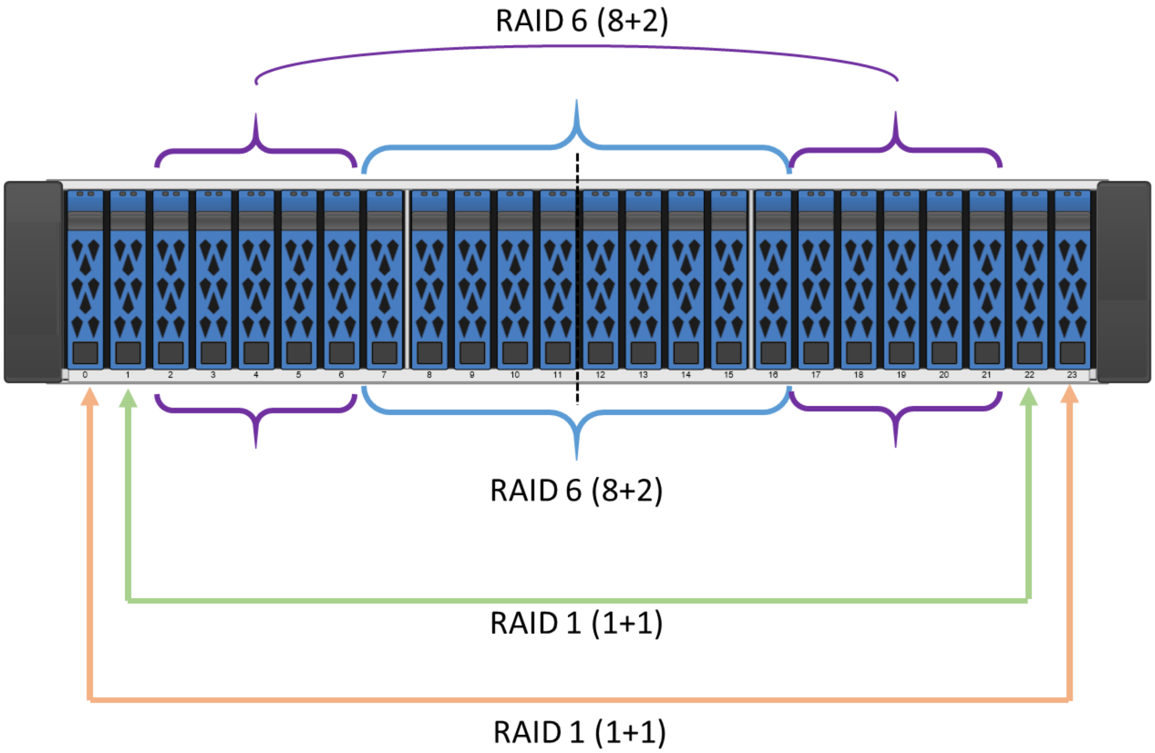


Figure 11 shows an example where RAID 6 volume groups are created from the middle drives then from an outside set of drives, then two RAID 1 volume groups are built from the outside in. SANtricity currently allows drive selection under the Advanced feature when creating a volume group.

Figure 11) Example of using all 24 drives in a configuration.



SANtricity management features

NetApp E-Series and EF-Series arrays have a rock-solid reputation for reliability, availability, simplicity, and security. The NetApp SANtricity 11.70 release builds on that legacy with the addition of 512e, which allows general support of the iSCSI host interface and support for VMware for FC and iSCSI hosts for NVMe-based platforms.

The new-generation E-Series and EF-Series arrays running the latest SANtricity OS are common criteria certified (NDcPP v2 certification).

Deployment

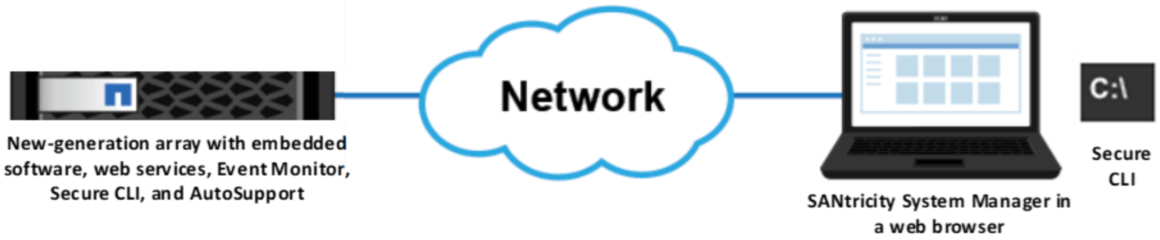
Deciding which components to install on an EF600-based storage array depends on if you want to manage single storage arrays individually or if you are managing multiple arrays.

Note: If you are using asynchronous mirroring features, then Unified Manager is required.

Managing storage arrays individually

If you are not using synchronous or asynchronous mirroring features, then all configurations can be handled from SANtricity System Manager. Simply bookmark each array in a web browser. Figure 12 illustrates this configuration.

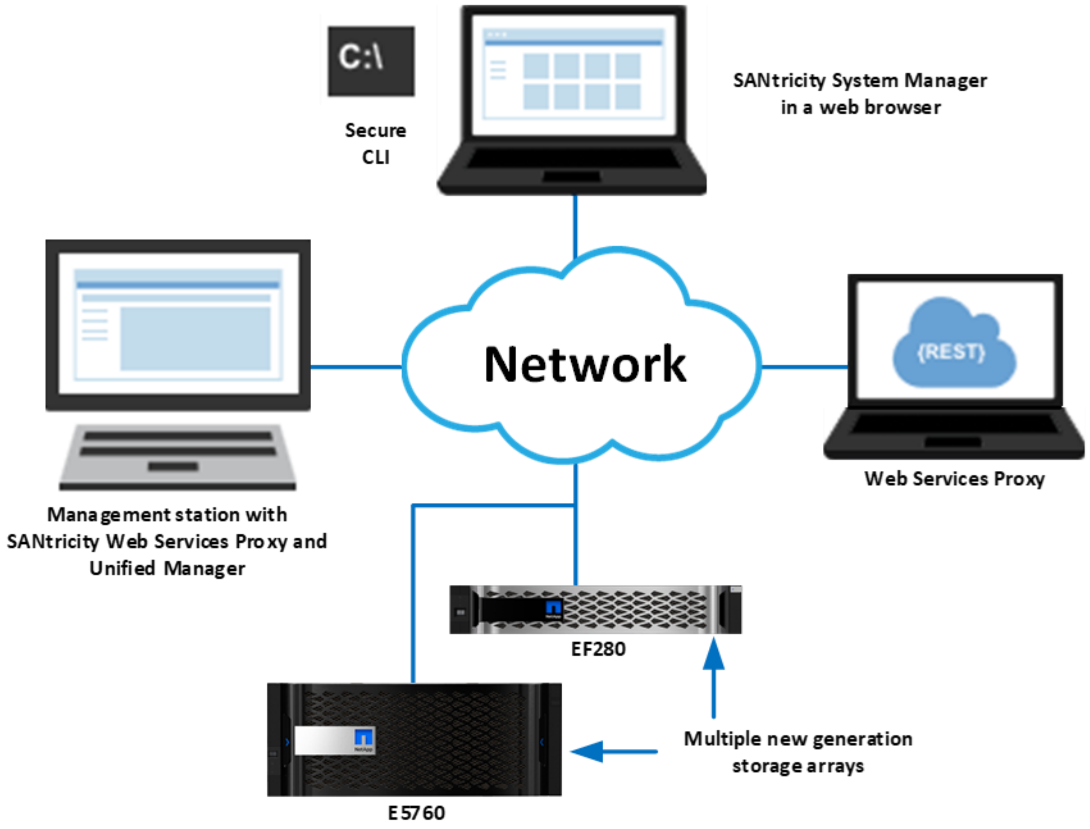
Figure 12) Managing a single EF600 with SANtricity System Manager.


New-generation array with embedded software, web services, Event Monitor, Secure CLI, and AutoSupport
Network
SANtricity System Manager in a web browser
C:\
Secure CLI

Multiple storage arrays

If you have one or more storage arrays, you can install Unified Manager to manage your overall environment while still managing all storage array-based configuration through SANtricity System Manager. To manage multiple arrays, you can launch SANtricity System Manager from Unified Manager, as shown in Figure 13.

Figure 13) Managing multiple new generation systems with SANtricity Unified Manager and SANtricity System Manager.


C:\
Secure CLI
SANtricity System Manager in a web browser
Network
{REST}
Management station with SANtricity Web Services Proxy and Unified Manager
Web Services Proxy
EF280
Multiple new generation storage arrays
E5760

SANtricity Unified Manager

SANtricity Unified Manager is a web-based central management interface that replaces the legacy SANtricity Storage Manager EMW for managing the new-generation E-Series arrays. The Unified Manager GUI is bundled with the SANtricity Web Services Proxy and installs on a management server with IP access to the managed arrays. Unified Manager can manage hundreds of arrays.

SANtricity Unified Manager adds the following time-saving features:

- Upgrades multiple arrays with the same type of controller at one time.

  Note: To upgrade to SANtricity OS 11.80.x the array must have already been upgraded to SANtricity OS 11.70.5.

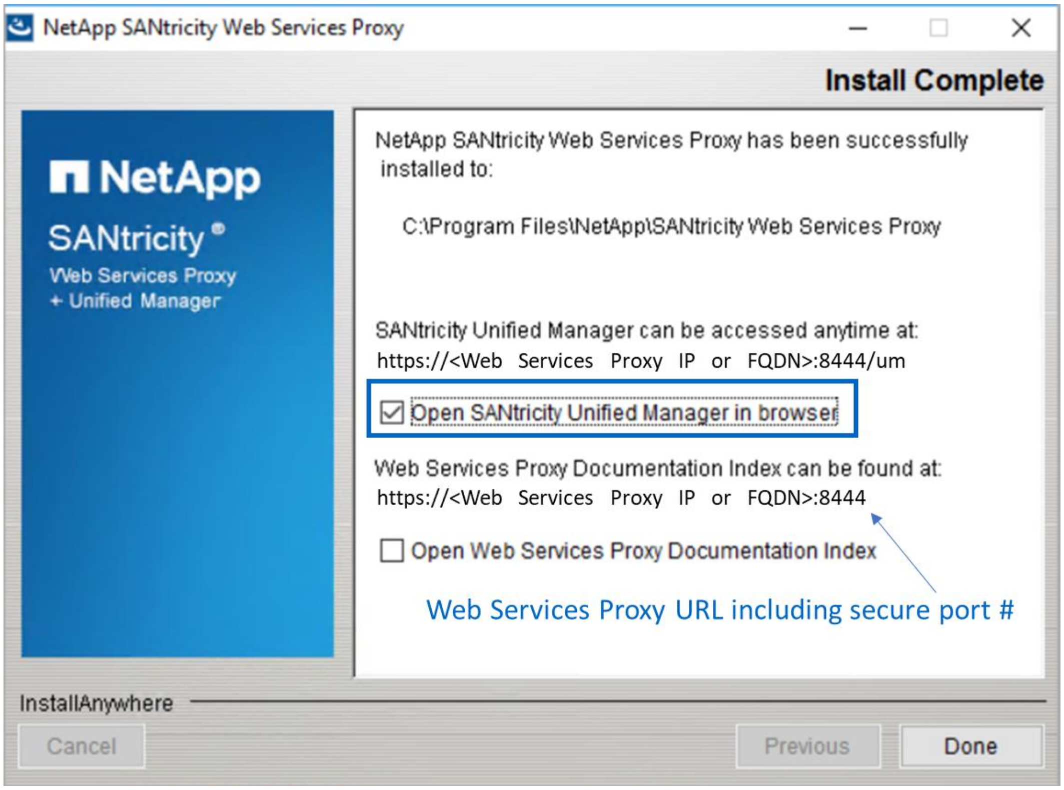
- Supports Lightweight Directory Access Protocol (LDAP) and role-based access control (RBAC) just like SANtricity System Manager. It includes a simplified certificate management workflow to manage the Unified Manager or Web Services Proxy server certificates (truststore and keystore certificates).
- Supports organizing arrays by groups that you can create, name, and arrange.
- Supports importing common settings from one array to another. You save time by not duplicating setup steps for each array.
- Supports synchronous and asynchronous mirroring for all new generation arrays through the secure SSL interface. The EMW is only required if the initiator or target array is a legacy E2700, E5600/EF560, or earlier array model.

  Note: There is no synchronous mirroring support for EF600 systems.

The E-Series SANtricity Unified Manager or E-Series SANtricity Web Services Proxy is available on the NetApp Support Site's software download page. Either listing takes you to the combined Web Services Proxy with SANtricity Unified Manager download page.

After the installation wizard completes, you can open Unified Manager, or you can directly access the SANtricity Web Services Proxy as shown in Figure 14.

Figure 14) Final dialog box in the Web Services Proxy installation wizard.



NetApp SANtricity Web Services Proxy

Install Complete

NetApp SANtricity Web Services Proxy has been successfully installed to:

C:\Program Files\NetApp\SANtricity Web Services Proxy

SANtricity Unified Manager can be accessed anytime at:
https://<Web Services Proxy IP or FQDN>:8444/um

☑ Open SANtricity Unified Manager in browser

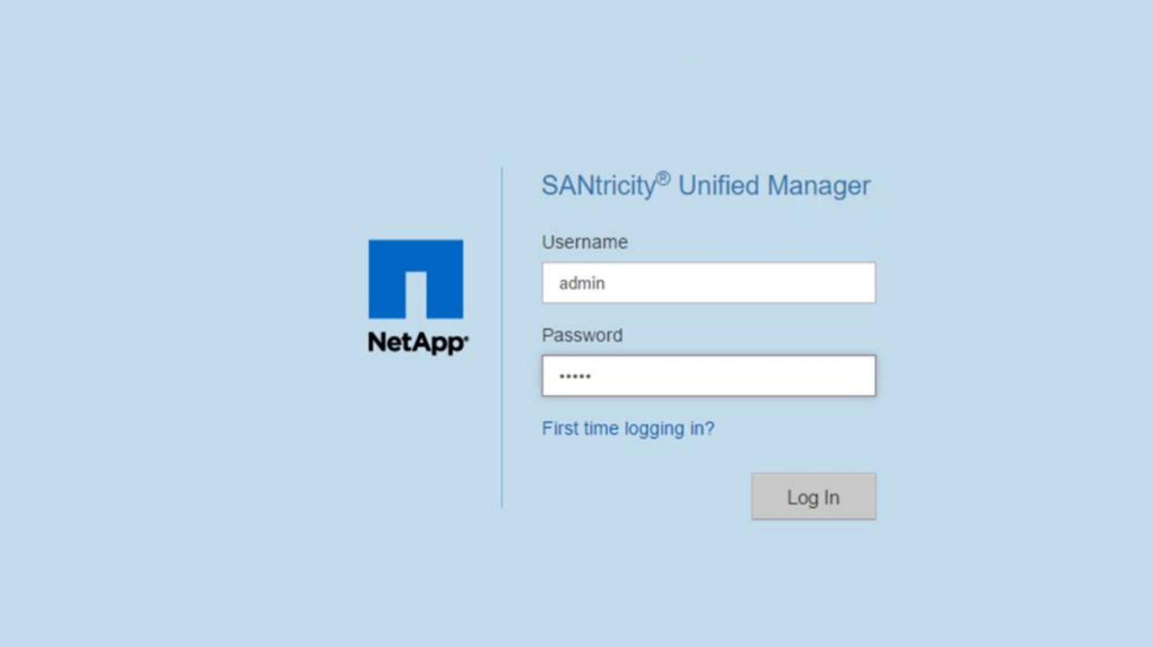
Web Services Proxy Documentation Index can be found at:
https://<Web Services Proxy IP or FQDN>:8444

□ Open Web Services Proxy Documentation Index

Web Services Proxy URL including secure port #

If you want to open the Unified Manager UI after the Web Services Proxy installation, open a browser, navigate to the server IP address, and secure port number that was reserved during the Web Services Proxy software installation. For example, enter the URL in the form `https://<proxy-FQDN>:<port #>/`, and then select the link for Unified Manager. You could go directly to the Unified Manager login page (Figure 15) by adding `/um` to the URL—for example, `https://<proxy-FQDN>:<port #>/um`.

Figure 15) SANtricity Unified Manager login page.



SANtricity® Unified Manager

Username: admin

Password: •••••

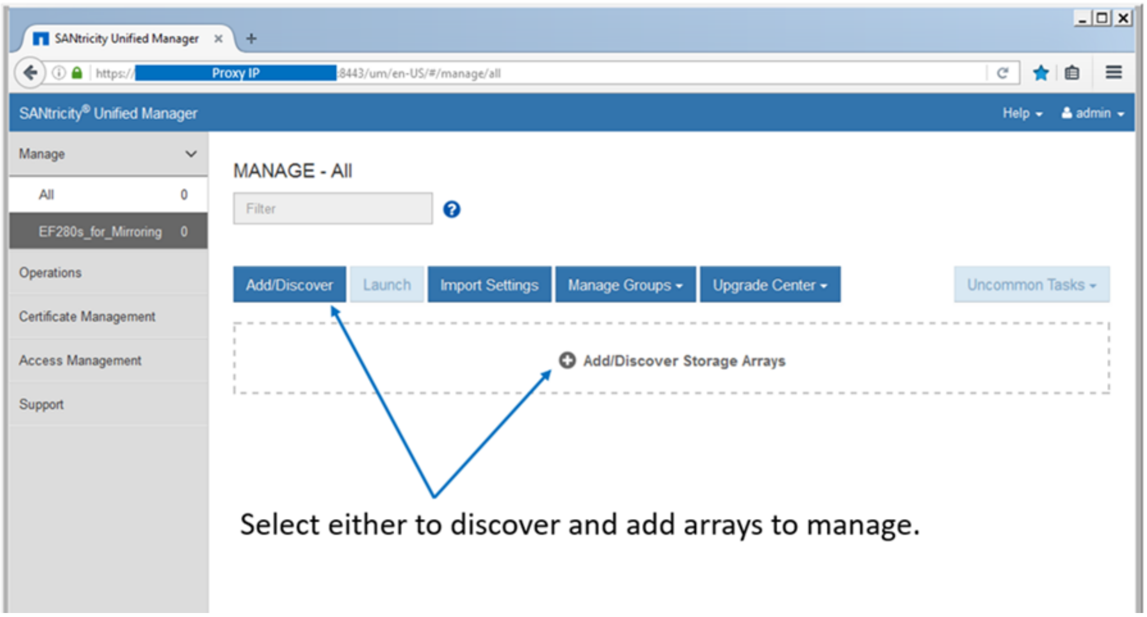
SANtricity Unified Manager navigation

The login page for SANtricity Unified Manager has a similar appearance to SANtricity System Manager and requires administrators to set the array admin password as part of the initial login. SANtricity Unified Manager has a factory default admin account: `admin`.

Discovering and adding storage arrays

Like the SANtricity EMW, SANtricity Unified Manager must discover arrays to manage, and, like the EMW, you can discover a single array or scan a range of IP addresses to discover multiple arrays simultaneously. Select the tab or link shown in Figure 16 to open the Add/Discover wizard. After discovering arrays, you then choose to add them to be managed by Unified Manager.

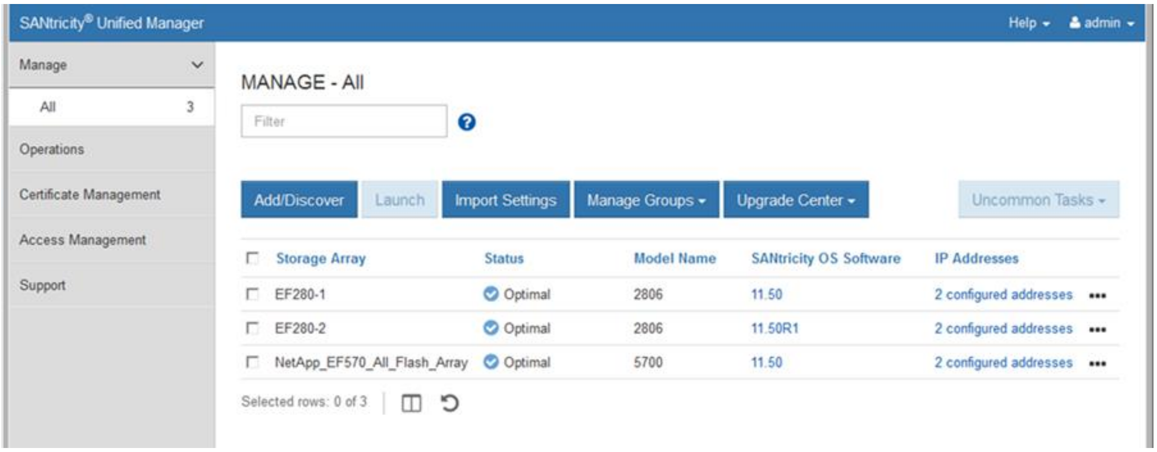
Figure 16) SANtricity Unified Manager landing page—discover and add arrays.



Select either to discover and add arrays to manage.

After the arrays are discovered and added, they are displayed on the landing page of Unified Manager (Figure 17).

Figure 17) SANtricity Unified Manager landing page.



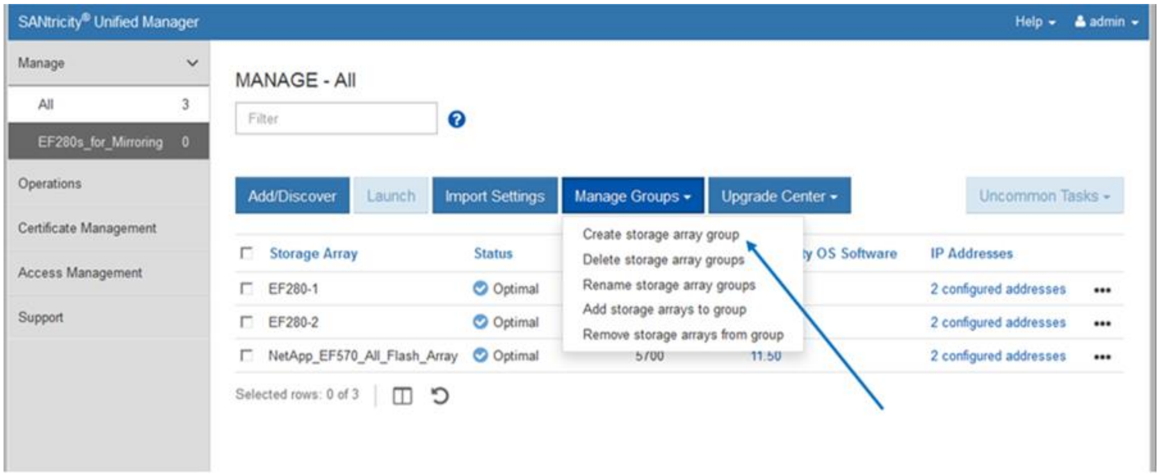
	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses
□	EF280-1	Optimal	2806	11.50	2 configured addresses •••
□	EF280-2	Optimal	2806	11.50R1	2 configured addresses •••
□	NetApp_EF570_All_Flash_Array	Optimal	5700	11.50	2 configured addresses •••

Selected rows: 0 of 3

Organizing arrays by group

After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 18 shows the EF280 arrays added to a group. This capability is available for all new-generation E-Series and EF-Series arrays.

Figure 18) Creating a group to organize arrays in SANtricity Unified Manager.

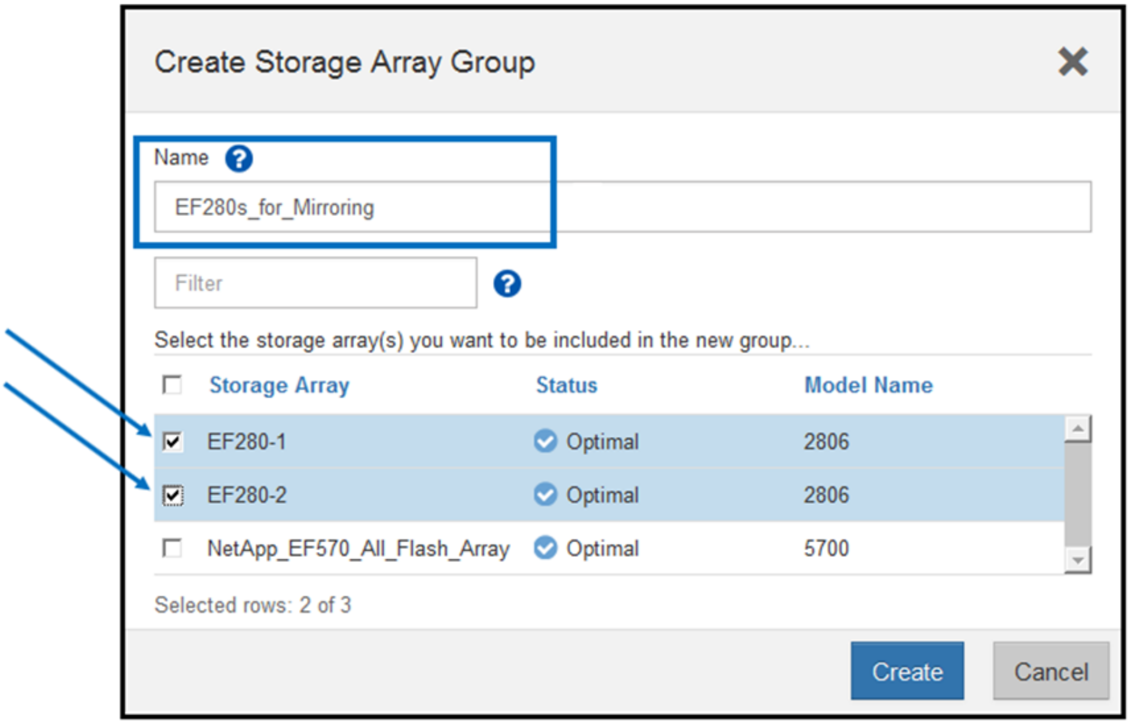


☐	Storage Array	Status		ty OS Software	IP Addresses	
☐	EF280-1	Optimal			2 configured addresses	•••
☐	EF280-2	Optimal			2 configured addresses	•••
☐	NetApp_EF570_All_Flash_Array	Optimal	5700	11.50	2 configured addresses	•••

Selected rows: 0 of 3

The built-in wizard makes adding arrays to groups quick and easy, as shown in Figure 19.

Figure 19) Creating a group in Unified Manager.



Name: EF280s_for_Mirroring

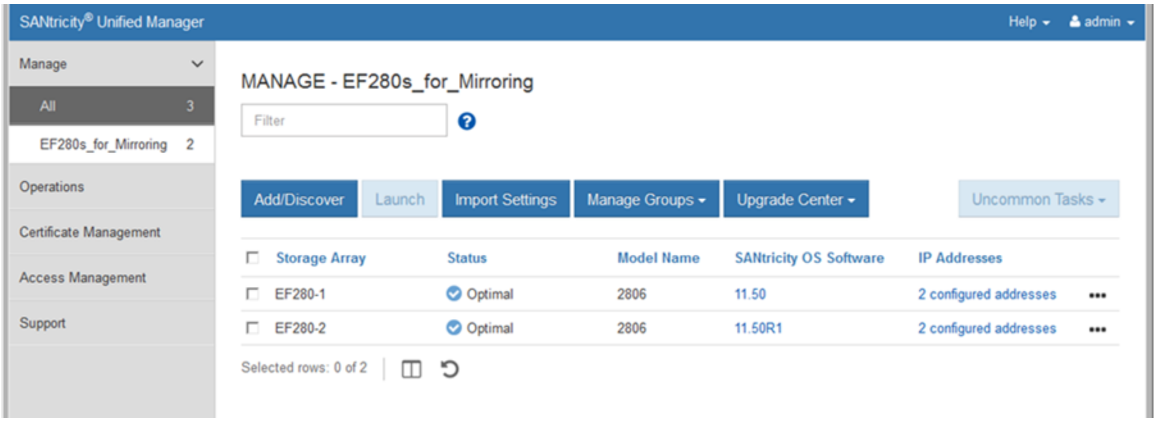
Select the storage array(s) you want to be included in the new group...

☐	Storage Array	Status	Model Name
☑	EF280-1	Optimal	2806
☑	EF280-2	Optimal	2806
☐	NetApp_EF570_All_Flash_Array	Optimal	5700

Selected rows: 2 of 3

SANtricity Unified Manager enables you to see just the subset of arrays in the new group, as shown in Figure 20.

Figure 20) SANtricity Unified Manager showing a newly created group.



□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses
□	EF280-1	Optimal	2806	11.50	2 configured addresses
□	EF280-2	Optimal	2806	11.50R1	2 configured addresses

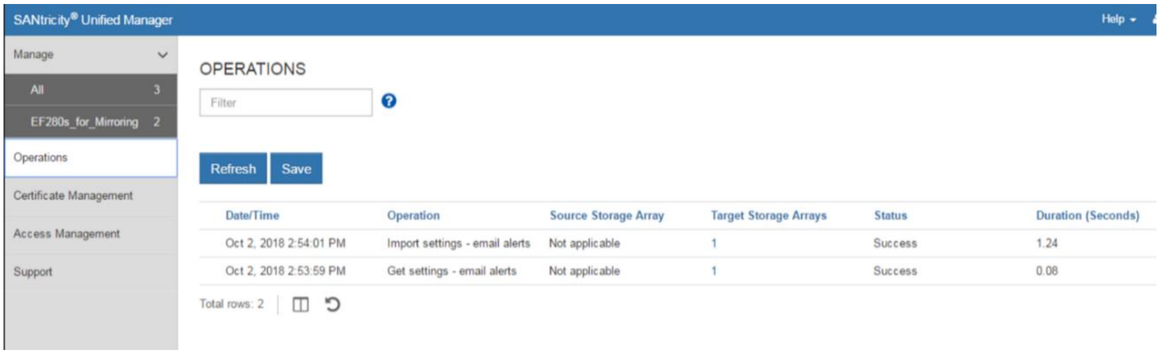
Selected rows: 0 of 2

Importing settings and view operations

Other features in SANtricity Unified Manager require the ability to view operations that take some time to complete. One example is importing settings from one storage array to another. This feature is especially helpful and time saving when you install a new array in an environment that already contains E-Series or EF-Series arrays running SANtricity 11.60 or later. For example, if you want the same alerting and NetApp AutoSupport settings on all systems, use the Import Settings wizard to select the setting category, the array to copy from, and the array to import to, and click Finish. The operation to copy the settings is displayed in the Operations view, as shown in Figure 21.

Note: Be careful when importing settings from another storage array, especially if you have different alerting requirements and unique storage configurations. The storage configuration option is successful only when the source and destination arrays have identical hardware configurations. The import feature does not show details about the pending import and does not prompt for confirmation. When you click Finish, you cannot stop the copy/import process.

Figure 21) SANtricity Unified Manager Operations view.



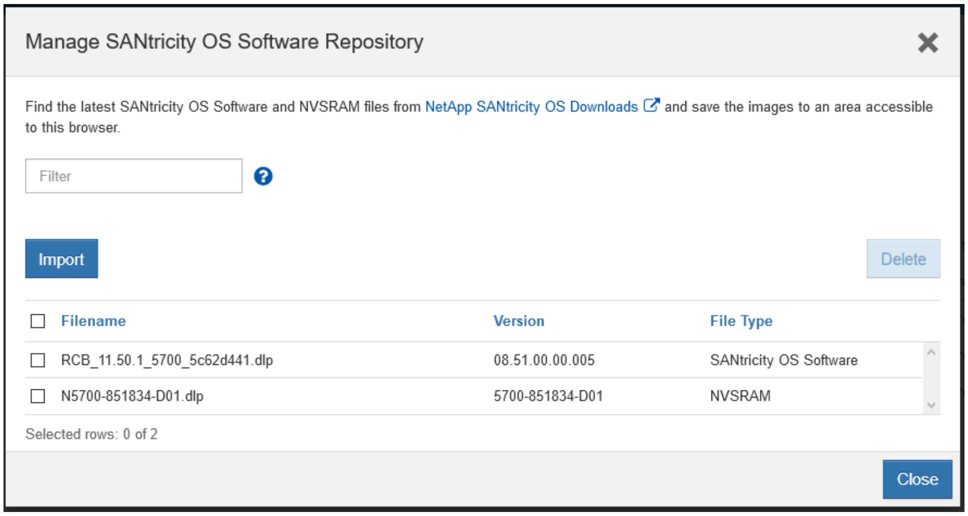
Date/Time	Operation	Source Storage Array	Target Storage Arrays	Status	Duration (Seconds)
Oct 2, 2018 2:54:01 PM	Import settings - email alerts	Not applicable	1	Success	1.24
Oct 2, 2018 2:53:59 PM	Get settings - email alerts	Not applicable	1	Success	0.08

Total rows: 2

Updating SANtricity OS through Unified Manager

To upgrade the array’s firmware, complete the following steps:

1. Import SANtricity OS software into Unified Manager’s SANtricity OS Software Repository by using Manage SANtricity OS Software Repository under Upgrade Center on the landing page.

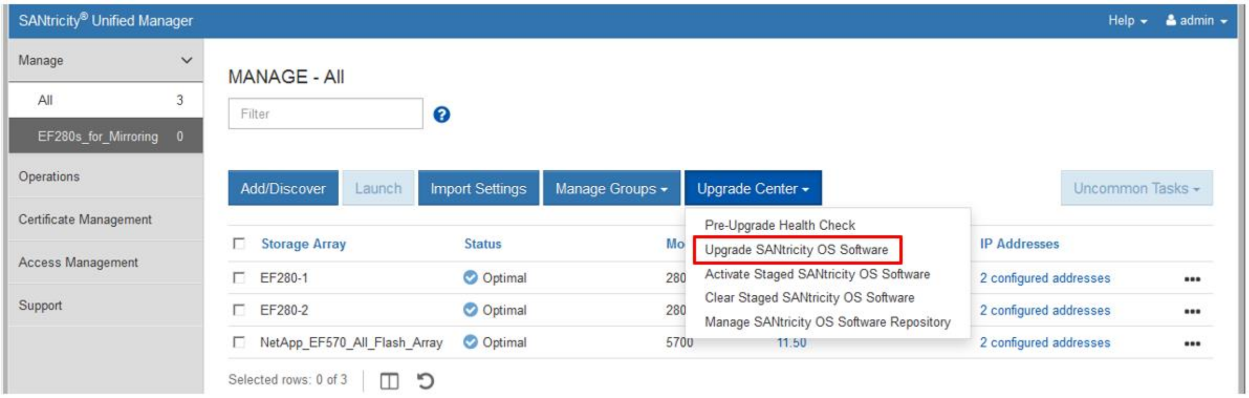


Find the latest SANtricity OS Software and NVSRAM files from NetApp SANtricity OS Downloads and save the images to an area accessible to this browser.

□	Filename	Version	File Type
□	RCB_11.50.1_5700_5c62d441.dlp	08.51.00.00.005	SANtricity OS Software
□	N5700-851834-D01.dlp	5700-851834-D01	NVSRAM

Selected rows: 0 of 2

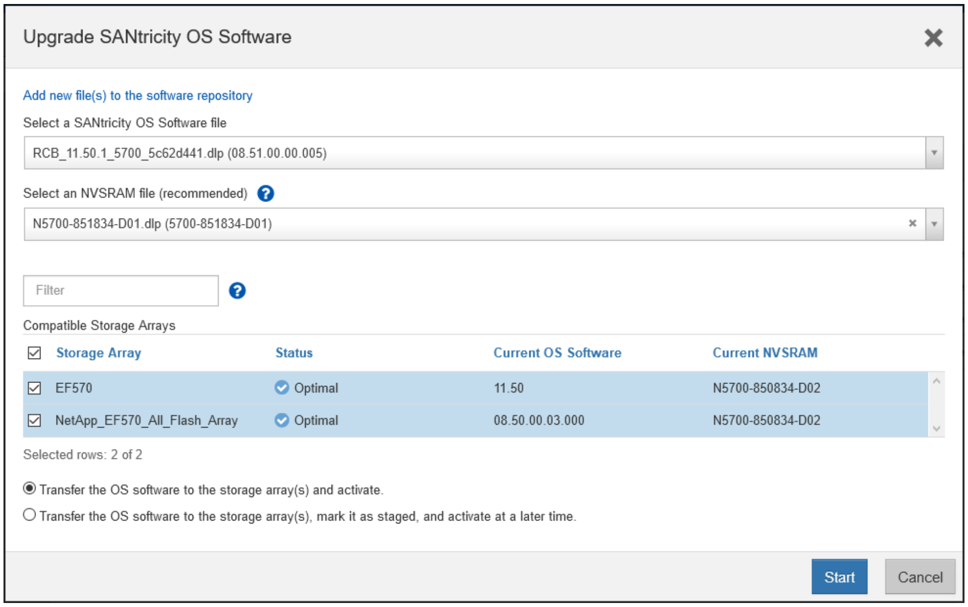
2. On the Unified Manager landing page, click Upgrade Center, and then click Upgrade SANtricity OS Software.



□	Storage Array	Status	Mo		IP Addresses	
□	EF280-1	Optimal	280		2 configured addresses	•••
□	EF280-2	Optimal	280		2 configured addresses	•••
□	NetApp_EF570_All_Flash_Array	Optimal	5700	11.50	2 configured addresses	•••

Selected rows: 0 of 3

3. In the Upgrade SANtricity OS Software window, select the following items:
   - The desired SANtricity OS and/or NVSRAM files
   - The arrays to be upgraded that are appropriate to the selected SANtricity OS files
   - Whether to transfer and activate the OS files immediately or later
4. Click Start to continue.


Upgrade SANtricity OS Software
Add new file(s) to the software repository
Filter
Start
Cancel

Select a SANtricity OS Software file

RCB_11.50.1_5700_5c62d441.dlp (08.51.00.00.005)

Select an NVSRAM file (recommended)

N5700-851834-D01.dlp (5700-851834-D01)

Compatible Storage Arrays

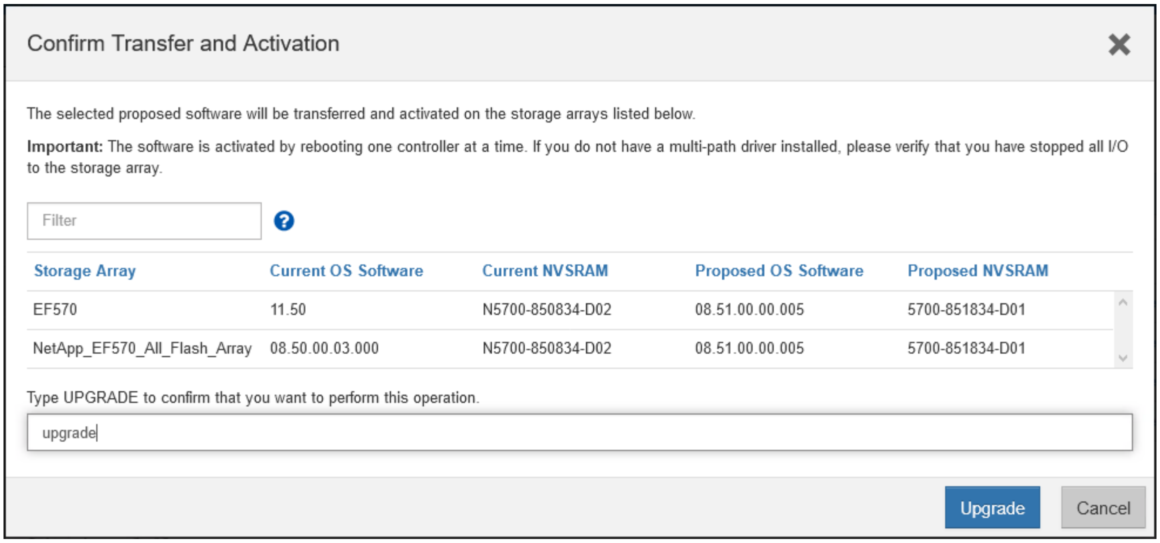
☑	Storage Array	Status	Current OS Software	Current NVSRAM
☑	EF570	Optimal	11.50	N5700-850834-D02
☑	NetApp_EF570_All_Flash_Array	Optimal	08.50.00.03.000	N5700-850834-D02

Selected rows: 2 of 2

● Transfer the OS software to the storage array(s) and activate.

○ Transfer the OS software to the storage array(s), mark it as staged, and activate at a later time.

5. On the Confirm Transfer and Activation page, type `upgrade` and then click Upgrade button to begin the SANtricity OS files transfer.



The selected proposed software will be transferred and activated on the storage arrays listed below.

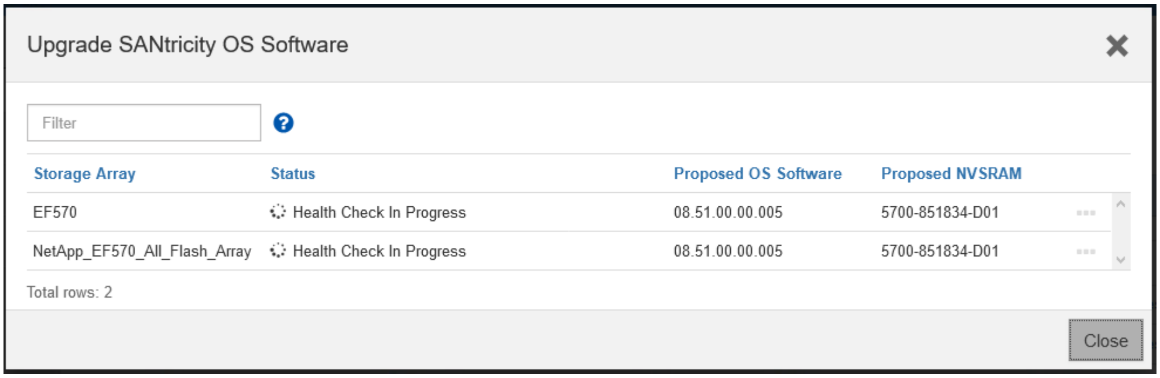
Important: The software is activated by rebooting one controller at a time. If you do not have a multi-path driver installed, please verify that you have stopped all I/O to the storage array.

Storage Array	Current OS Software	Current NVSRAM	Proposed OS Software	Proposed NVSRAM
EF570	11.50	N5700-850834-D02	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	08.50.00.03.000	N5700-850834-D02	08.51.00.00.005	5700-851834-D01

Type UPGRADE to confirm that you want to perform this operation.

upgrade

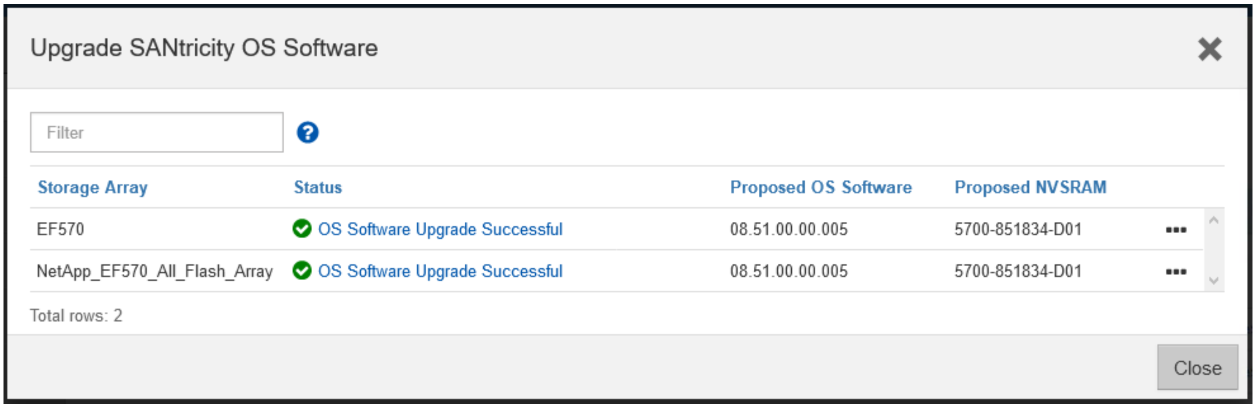
6. After the transfer starts, the Upgrade SANtricity OS Software page is displayed. The status of the selected arrays is displayed throughout the upgrade process. The first status is Health Check in Progress, then File Transfer in Progress, and finally Reboot in Progress.



Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	Health Check In Progress	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	Health Check In Progress	08.51.00.00.005	5700-851834-D01

Total rows: 2

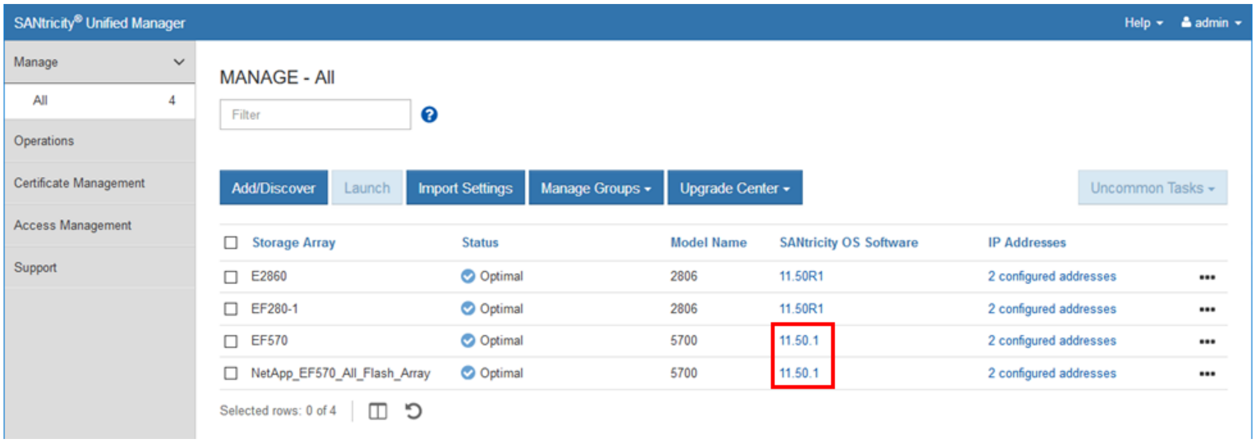
7. After the files have been transferred and the controllers have completed rebooting, the status changes to OS Software Upgrade Successful.



Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	✓ OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	✓ OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01

Total rows: 2

8. On the Unified Manager landing page, the SANtricity OS Software version reflects the newly installed SANtricity OS version.



□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses
□	E2860	✓ Optimal	2806	11.50R1	2 configured addresses
□	EF280-1	✓ Optimal	2806	11.50R1	2 configured addresses
□	EF570	✓ Optimal	5700	11.50.1	2 configured addresses
□	NetApp_EF570_All_Flash_Array	✓ Optimal	5700	11.50.1	2 configured addresses

Selected rows: 0 of 4

SANtricity Unified Manager security

SANtricity Unified Manager supports the same secure management features as SANtricity System Manager, including LDAP, RBAC, and SSL certificates. For complete details and workflow examples, see TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide, TR-4855: Security Hardening Guide for NetApp SANtricity, and TR-4813: Managing Certificates for NetApp E-Series Storage Systems.

Remote mirroring with SANtricity Unified Manager

With Unified Manager, you can set up remote mirroring between two new generation arrays. Starting with SANtricity 11.62, Unified Manager is used to create mirror relationships. See SANtricity Synchronous and Asynchronous Mirroring (11.62 and above) in the E-Series and SANtricity 11 Documentation Center or the Online Help in SANtricity Unified Manager for a complete description. SANtricity Unified Manager must be version 4.2 or later and SANtricity System Manager must be OS version 11.62 or later.

Note: Asynchronous mirroring is only supported on EF300 and EF600 for SANtricity OS version 11.80 or later.

Note: Drive types should be the same on source and destination. Either both NVMe drives or both non-NVMe drives. NVMe 4Kn volumes mirror only to another NVMe 4Kn volume, and 512e to 512e.

Note: EF300 and EF600 do not support synchronous mirroring.

Prior to SANtricity 11.62, for a description of mirroring between two new generation E-Series arrays or between a new generation E-Series array and a legacy E-Series array, see SANtricity Synchronous and Asynchronous Mirroring (11.61 and below).

SANtricity System Manager

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for EF600 arrays. Previous arrays, such as EF560 and E2700, do not have this embedded functionality or the newer security features introduced with SANtricity System Manager 11.40 and later versions. These older arrays require installation of SANtricity Storage Manager.

EF600 storage systems are shipped preloaded with SANtricity OS, which includes SANtricity System Manager. To discover multiple EF600 storage systems running SANtricity OS from a central view, download the latest version of the Web Services Proxy, which includes the latest version of SANtricity Unified Manager.

If you do not want to use SANtricity Unified Manager to discover and manage your E-Series arrays, you do not need to download and install the Web Services Proxy software. When customers implement E-Series with Windows and Linux operating systems, they can use the settings in the Host Utilities to properly configure each host, according to the latest Interoperability Matrix Tool (IMT) guidance. See the appropriate OS Express Guide for host setup requirements, instructions, and references. The guides are available on the E-Series and SANtricity documentation resources page.

Note: Host packages are not required for NVMe-oF installations. See the appropriate OS Express Guide for host setup requirements, instructions, and references. The guides are available from the NetApp Support Site at https://mysupport.netapp.com/eseries.

Note: For first-time customers, creating an account on the NetApp Support Site can take 24 hours or more. New customers should register for Support site access well before the initial product installation date.

System Manager navigation

After you log in to SANtricity System Manager, the home page is displayed, as shown in Figure 22.

- The icons on the left let you navigate through the System Manager pages and are available on all pages. The text can be toggled on and off.
- The items on the top right (Preferences, Help, Log Out) are also available from any location in System Manager.
- At the bottom-right corner is an architectural view of your array that lets you provision the storage.

Figure 22) SANtricity System Manager home page.

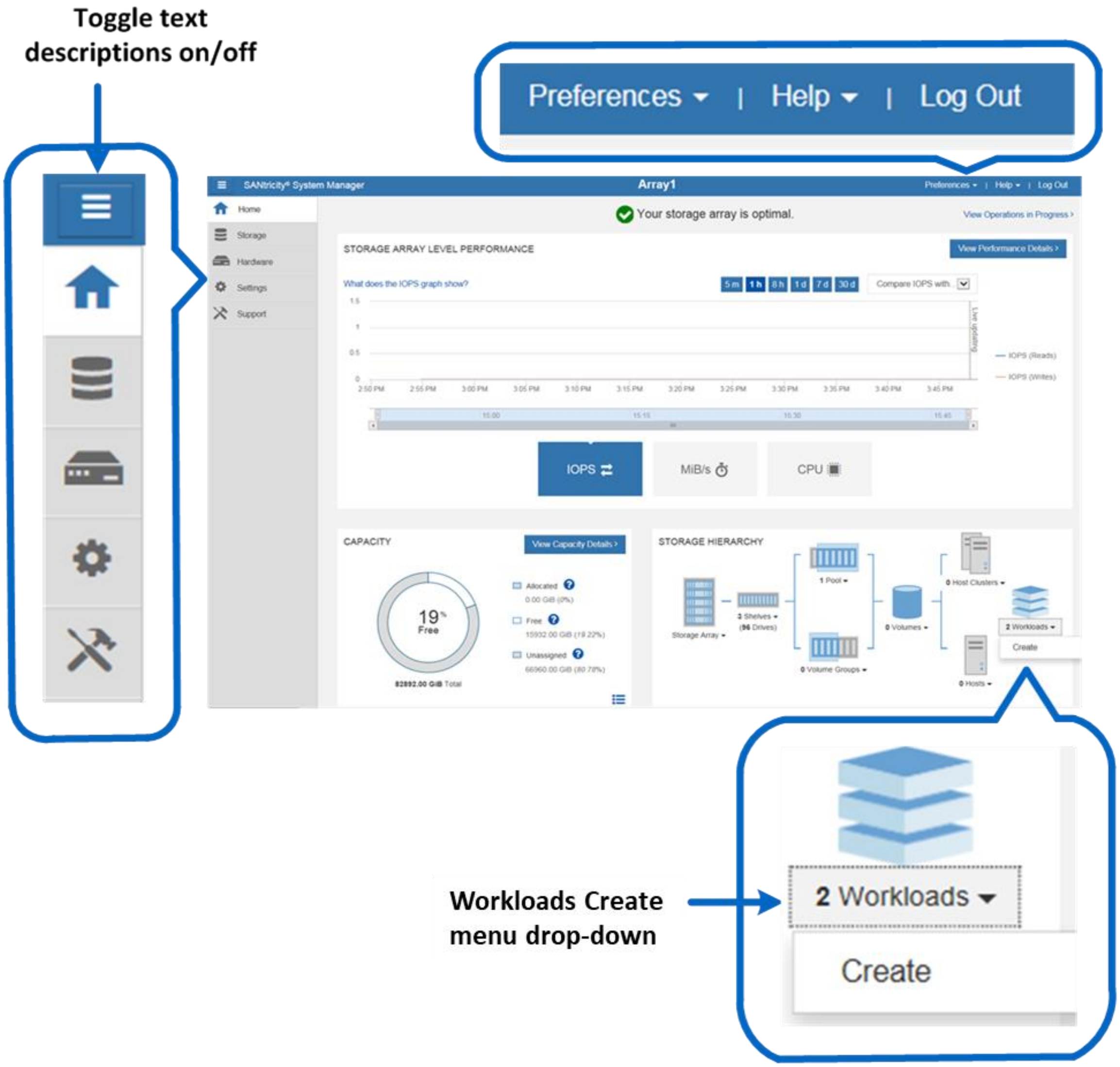
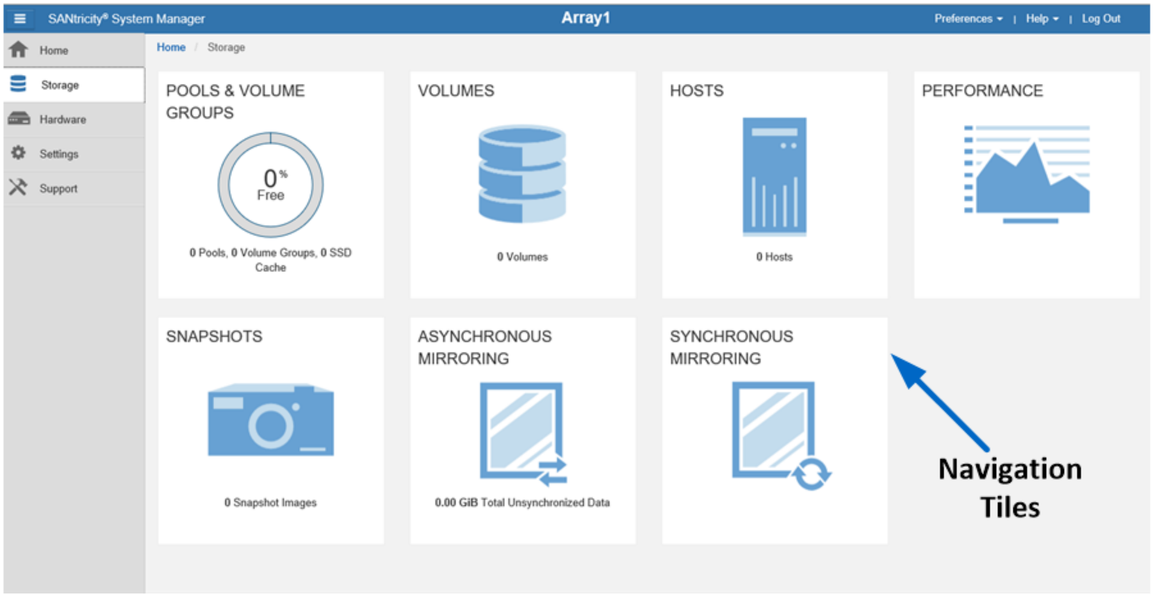


Figure 23, Figure 24, Figure 25, and Figure 26 show the other four main pages that are used in SANtricity System Manager and that are accessible from anywhere in the application.

Figure 23) System Manager Storage page.



0 Pools, 0 Volume Groups, 0 SSD Cache

0 Volumes

0 Hosts

0 Snapshot Images

0.00 GiB Total Unsynchronized Data

Figure 24) System Manager Hardware page.

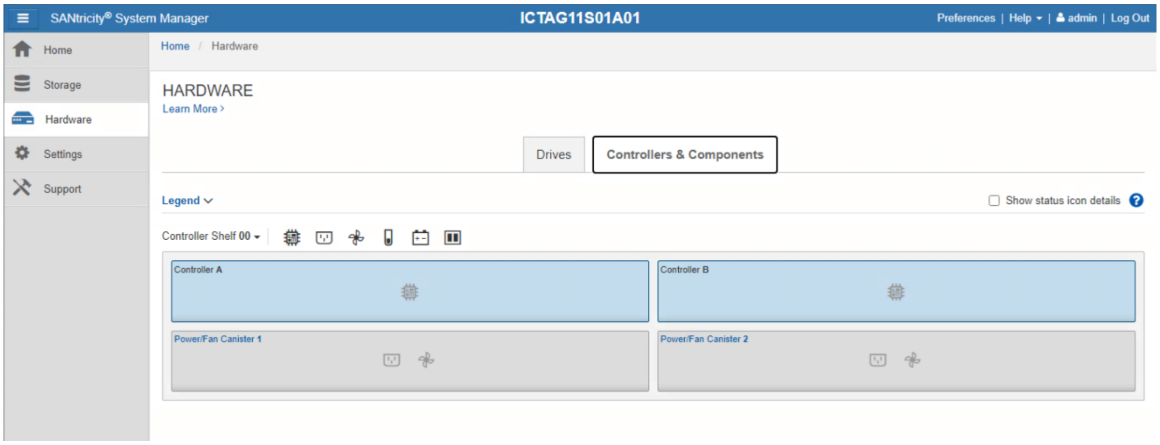
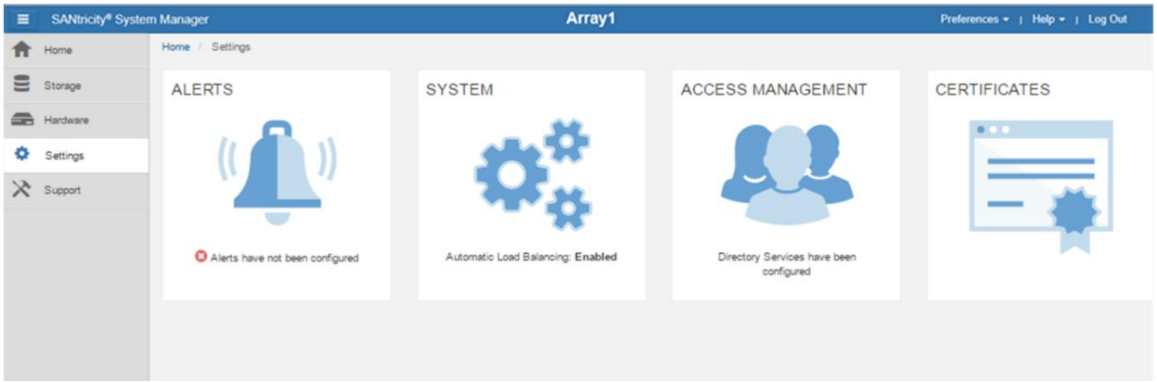


Figure 25) System Manager Settings page with new security tiles.



Alerts have not been configured

Automatic Load Balancing: Enabled

Directory Services have been configured

Note: Figure 25 shows the view for an administrator or security administrator. Others with a lower access permission level will see only the Alerts and System tiles.

Figure 26) System Manager Support page.

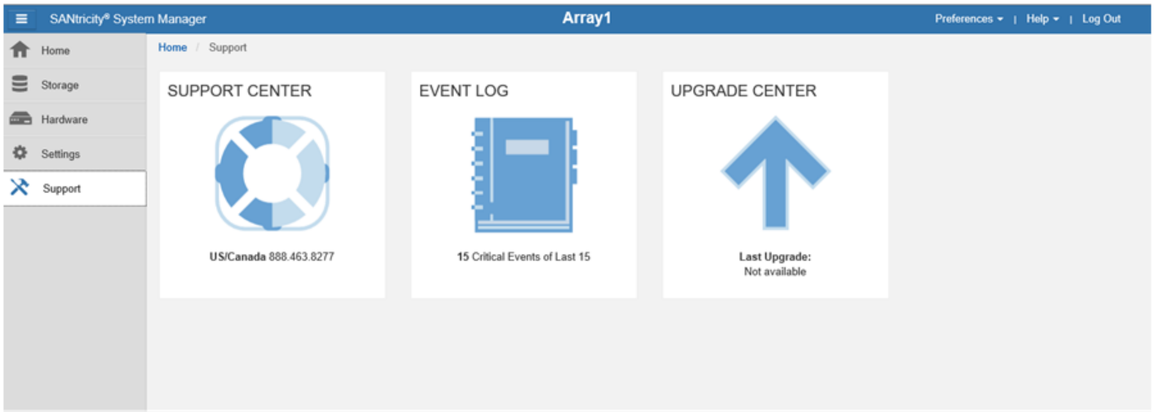
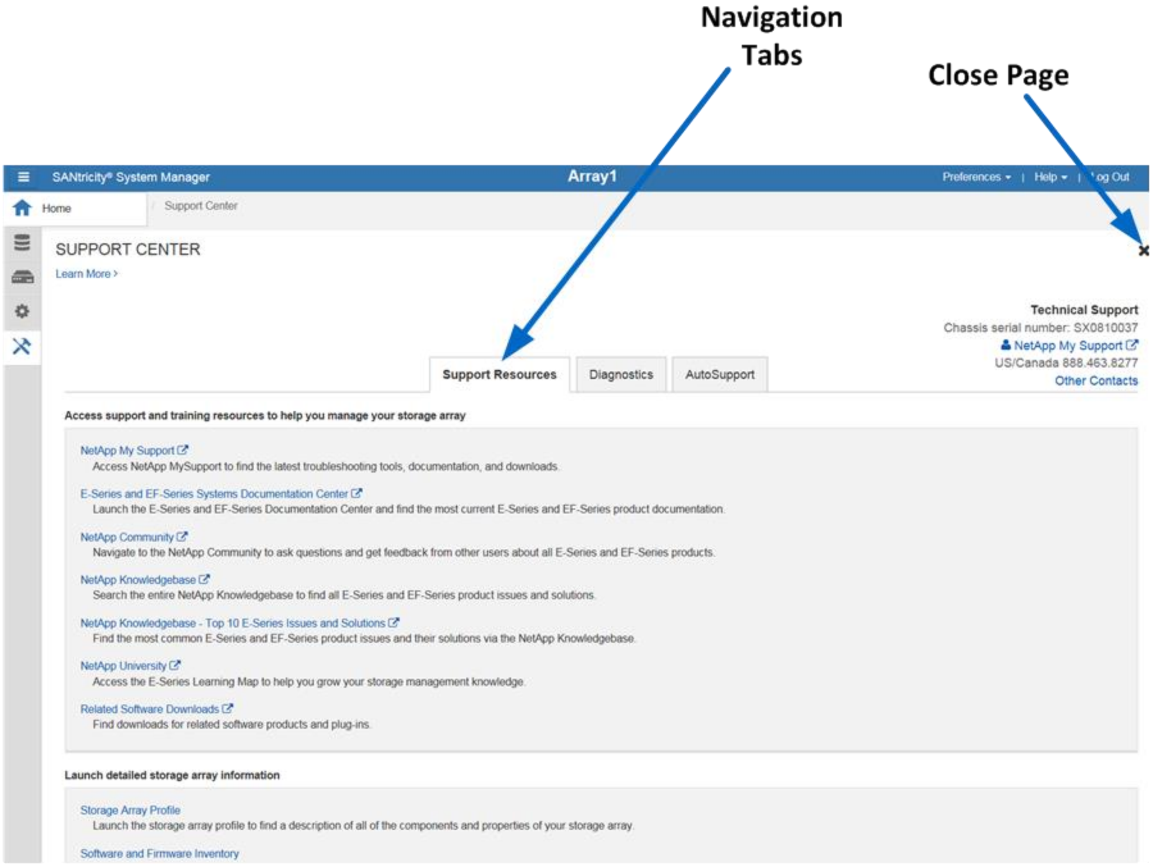


Figure 27 displays the Support Center, which you can reach by selecting the Support Center tile on the Support page (Figure 26). From the Support Center, use navigation tabs to reach support topics.

Figure 27) System Manager Support Center.



Access support and training resources to help you manage your storage array

NetApp My Support
Access NetApp MySupport to find the latest troubleshooting tools, documentation, and downloads.

E-Series and EF-Series Systems Documentation Center
Launch the E-Series and EF-Series Documentation Center and find the most current E-Series and EF-Series product documentation.

NetApp Community
Navigate to the NetApp Community to ask questions and get feedback from other users about all E-Series and EF-Series products.

NetApp Knowledgebase
Search the entire NetApp Knowledgebase to find all E-Series and EF-Series product issues and solutions.

NetApp Knowledgebase - Top 10 E-Series Issues and Solutions
Find the most common E-Series and EF-Series product issues and their solutions via the NetApp Knowledgebase.

NetApp University
Access the E-Series Learning Map to help you grow your storage management knowledge.

Related Software Downloads
Find downloads for related software products and plug-ins.

Launch detailed storage array information

Storage Array Profile
Launch the storage array profile to find a description of all of the components and properties of your storage array.

Software and Firmware Inventory

SANtricity System Manager security

SANtricity System Manager supports multiple levels of management interface security including:

- Support for directory services through LDAP.
- Support for RBAC: five standard roles with varying permission levels.
- Support for certification authority (CA) and SSL certificates.
- Implementation of a secure CLI. The CLI is secure when the certificates are installed. Syntax and invocation are the same as in the legacy CLI, but additional security parameters are supplied.
- Security enhancements that extend to the onboard web services API, where user account passwords are now required.

  Note: If you want to run in the previous security mode with a single administrative password and still use symbols to communicate through the legacy API, the new security features can be disabled by the admin or security users.

LDAP and RBAC

LDAP is a commonly used communication protocol that enables directory servers such as Microsoft Active Directory to provide centralized identity control over user and group definitions. The directory service is used by many devices in a network infrastructure to identify and authenticate users seeking access to devices in the network.

RBAC is software on the E-Series array that defines standard user levels, each with a well-defined set of access permissions. A user is authenticated as a member of a group, and specific permissions are set on the array side to define the type of access that user or group is allowed. This approach enables SANtricity 11.40 and later versions to provide the granularity of access that customers require.

The permission level with each role is defined in Table 2.

Table 2) Built-in roles and associated permissions.

Role name (log in as)	Access permissions
Root Admin (admin)	This role allows you to change the passwords of any local users and execute any command supported by the array. The admin password is set at initial login or any time after.
Security Admin (security)	This role allows you to modify security configuration settings on the array. It allows you to view audit logs; configure secure syslog server, LDAP, or LDAP over SSL (LDAPS) server connections; and manage certificates. This role provides read access but does not provide write access to storage array properties such as pool or volume creation or deletion. This role also has privileges to enable or disable SYMbol access to the array.
Storage Admin (storage)	This role allows full read and write access to the storage array properties and maintenance/diagnostics functions. However, it does not include access to perform any security configuration functions.
Support Admin (support)	This role provides access to all hardware resources on the array, failure data, event log/audit log, and controller firmware (CFW) upgrades. You can view the storage configuration but cannot change it.
Monitor (monitor)	This role provides read-only access to all storage array properties. However, you will not be able view the security configuration.

Setting up the directory server and roles

Directory servers, like most data center devices, are complex and designed to fulfill many use cases. However, the E-Series LDAP/RBAC implementation focuses on authentication and two main elements: users and groups. As with most applications, you must understand a few acronyms and follow a few conventions to set up communication between the E-Series array and the directory server. The most critical acronyms to understand are as follows:

- **CN.** Stands for `commonName`, used to identify group names as defined by the directory server tree structure.
- **DC.** Stands for `domainComponent`, the network in which user and groups exist (for example, netapp.com).
- **DN.** Stands for `distinguishedName`, the fully qualified domain name made up of one or more comma-separated common names, followed by one or more comma-separated DCs (for example, `CN=functional_group_name,CN=Users,DC=netapp,DC=com`).

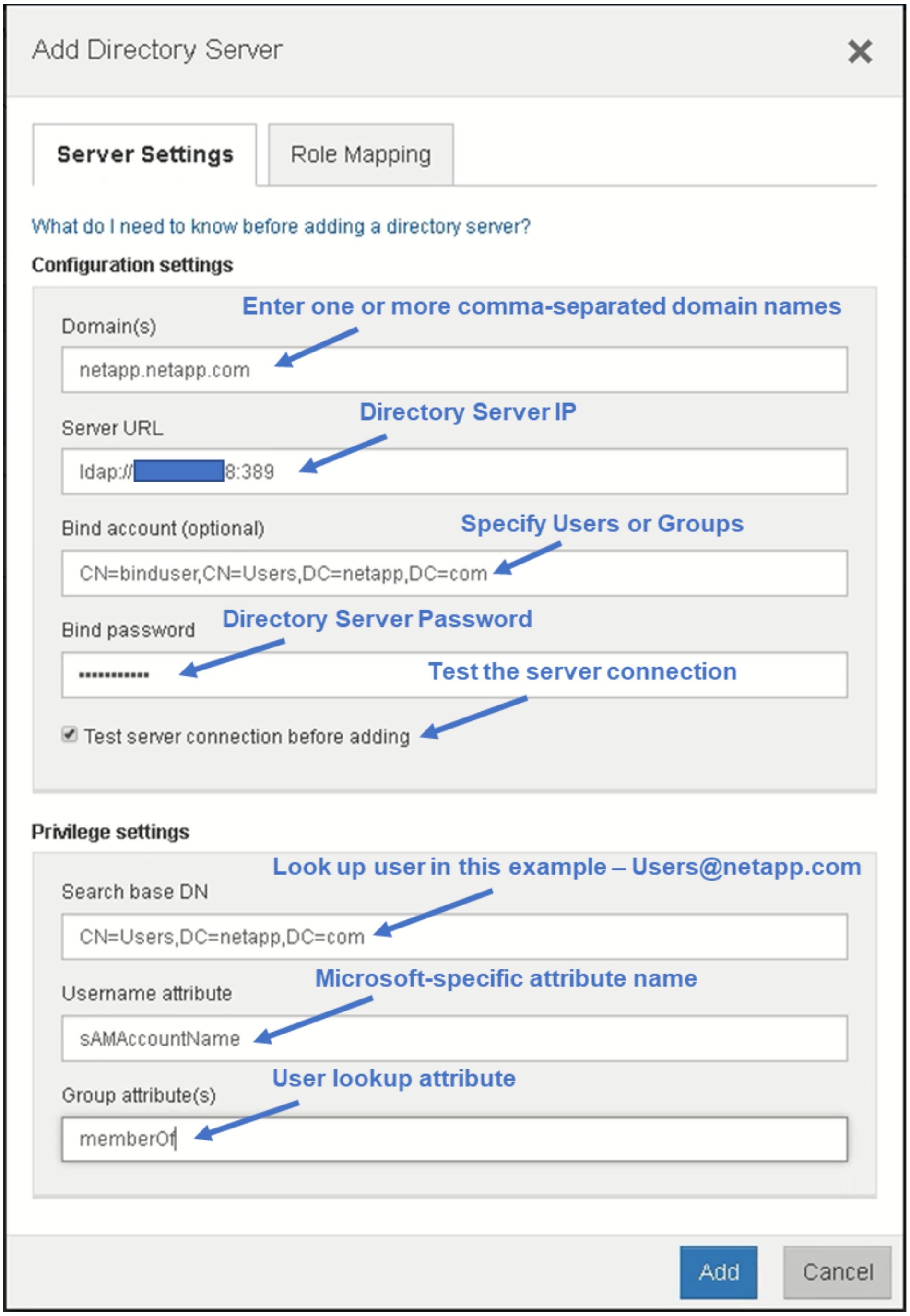
E-Series systems follow a standard web server implementation on the controllers, and information about the general directory services setup is available on the web. As a result, setting up the service on E-Series systems only requires some fields, which are listed in Table 3.

Table 3) LDAP/RBAC required fields and definitions.

Field name	Definitions
Domain (for example, netapp.com)	Network domains defined in the directory server of which users accessing the storage array are members.
Server URL	Could be a fully qualified domain name or IP and port number with the format `ldap://<IP:port_number>` (port 389 or port 636 for LDAPS).
Bind account	Format is `CN=binduser,CN=Users,DC=<some_name>,DC=com`.
Bind account password	Password for bind account user.
Search base DN	Format is `CN=Users,DC=<some_name>,DC=com`.
Username attribute	The LDAP attribute that defines the username. Example: `sAMAccountName`: standard entry for legacy Windows-based browsers, including Windows 95, Windows 98, and Windows XP. Linux can have other designations.
Group attributes	The LDAP attributes that define the groups to which a given user belongs. Example: `memberOf` is a standard attribute.

Figure 28 shows an example Active Directory server integration with SANtricity System Manager. The entries are all examples except for username attributes and group attributes in the privileges section. Those items are standard entries for Windows and are not likely to change for most implementations.

Figure 28) SANtricity System Manager directory server setup wizard.



Configuration settings

Domain(s): netapp.netapp.com

Enter one or more comma-separated domain names

Server URL: ldap://[redacted]8:389

Directory Server IP

Bind account (optional): CN=binduser,CN=Users,DC=netapp,DC=com

Specify Users or Groups

Bind password: ••••••••••••

Directory Server Password

☑ Test server connection before adding

Test the server connection

Privilege settings

Search base DN: CN=Users,DC=netapp,DC=com

Look up user in this example – Users@netapp.com

Username attribute: sAMAccountName

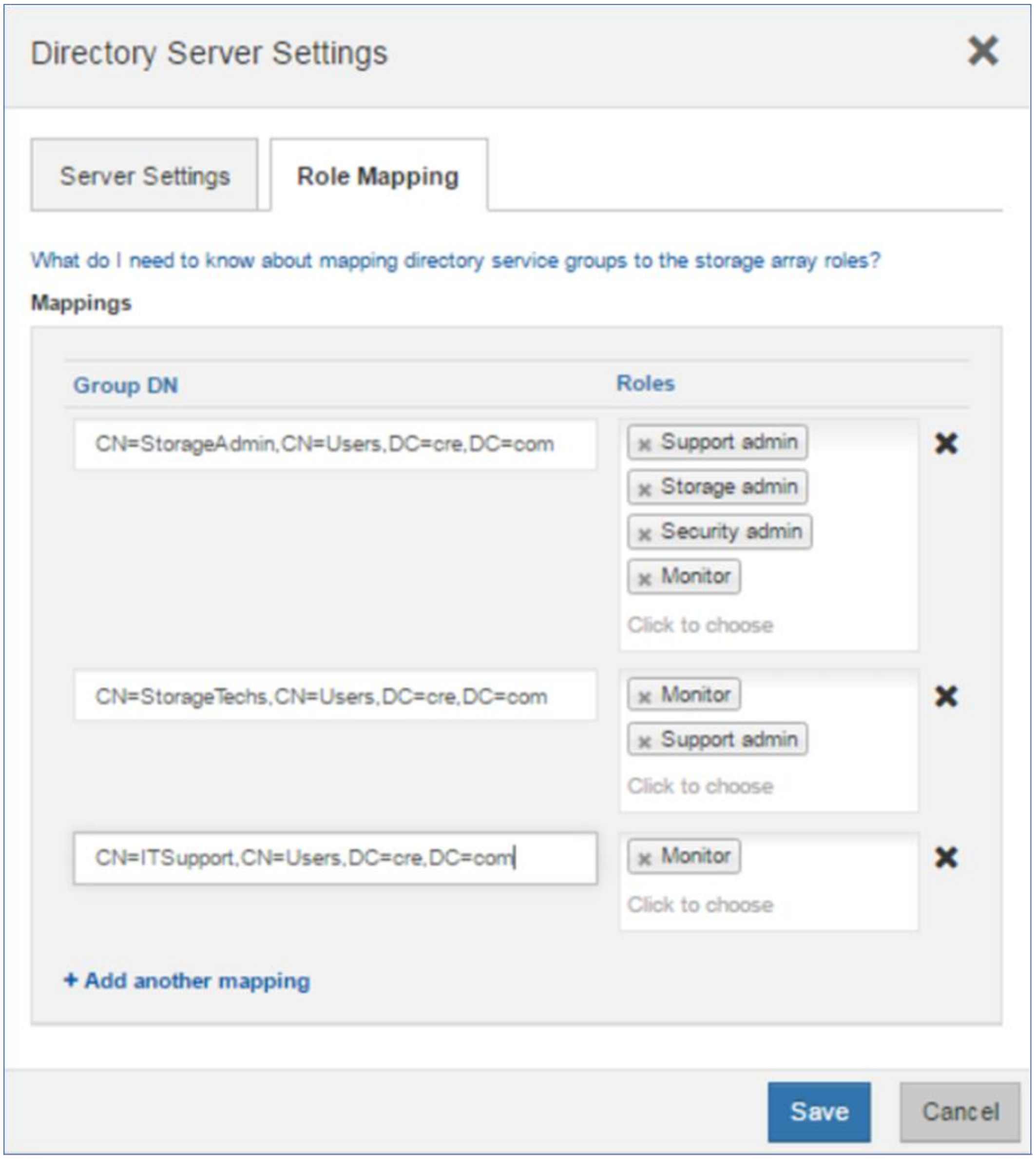
Microsoft-specific attribute name

Group attribute(s): memberOf

User lookup attribute

The array roles for the specified user groups are set in the Role Mapping tab. As shown in Figure 29, users who are members of the StorageAdmin, StorageTechs, and ITSupport groups are authenticated as branches of the Users group `@cre.com`. When users in one of those groups log in to the array, they are allowed access to certain views and functions in the management interface according to the permissions granted.

Figure 29) Role Mapping tab in the directory server settings wizard.



Directory Server Settings

What do I need to know about mapping directory service groups to the storage array roles?

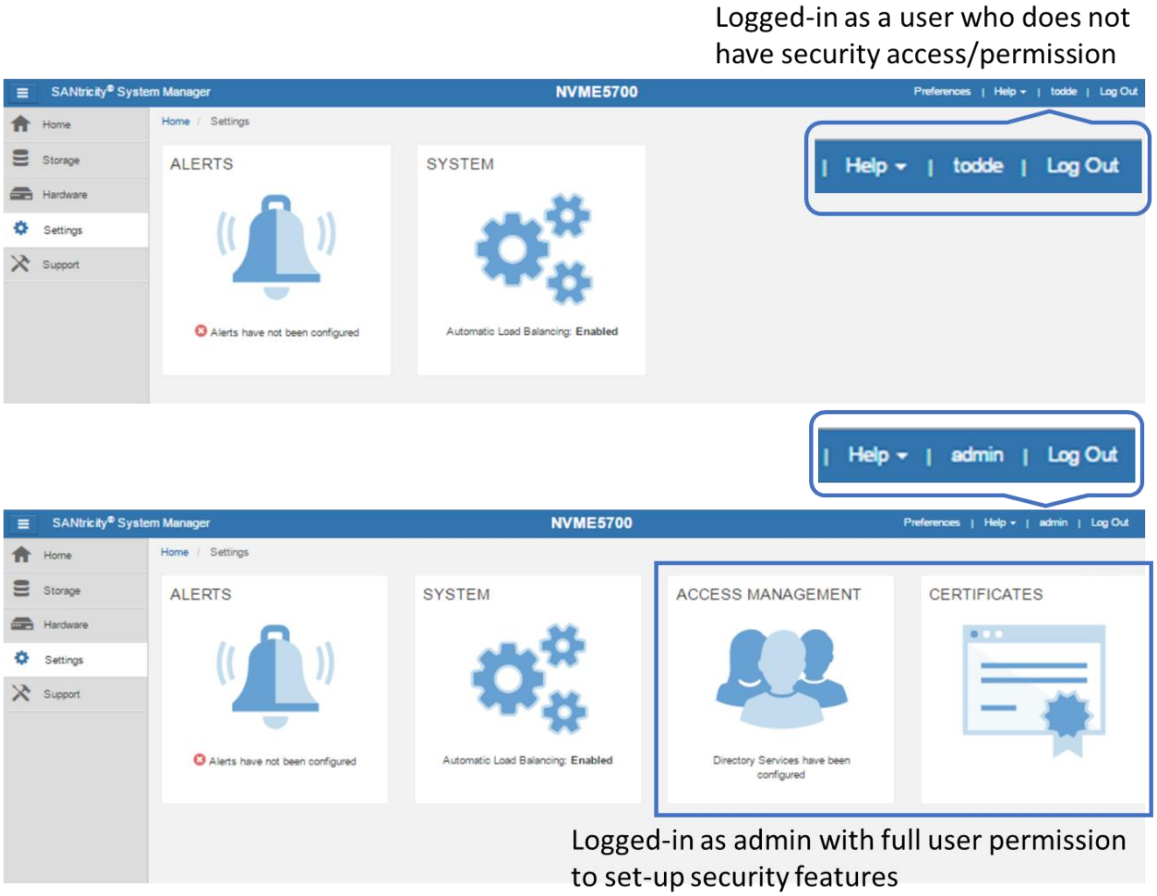
Mappings

Group DN	Roles
CN=StorageAdmin,CN=Users,DC=cre,DC=com	Support admin Storage admin Security admin Monitor
CN=StorageTechs,CN=Users,DC=cre,DC=com	Monitor Support admin
CN=ITSupport,CN=Users,DC=cre,DC=com	Monitor

Note: The monitor role is automatically added to all group DNs. Without monitor permission, users in the associated mapped group are not able to log in to the array.

Multiple groups can be defined and mapped to specific roles that meet individual business requirements. Figure 30 shows the difference in user views and access to features according to access permission level. The login on top provides monitor and support access, but it does not provide security access like the admin login below it.

Figure 30) SANtricity System Manager views change according to user permission level.



Logged-in as a user who does not have security access/permission

Logged-in as admin with full user permission to set-up security features

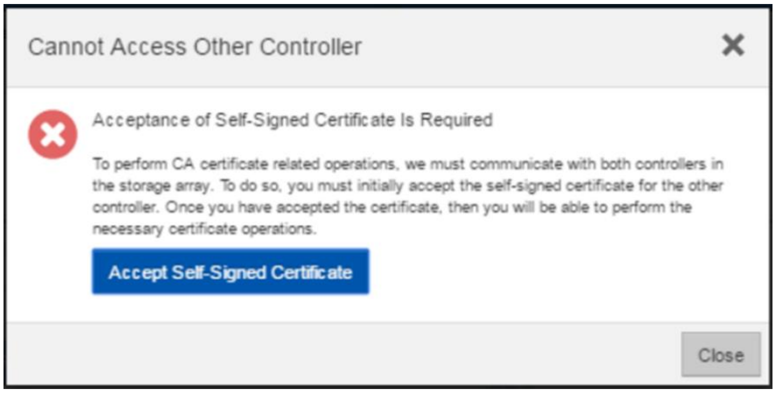
SANtricity® System Manager
NVME5700
Preferences | Help ▾ | todde | Log Out
Home
Storage
Hardware
Settings
Support
Home / Settings
ALERTS
Alerts have not been configured
SYSTEM
Automatic Load Balancing: Enabled
| Help ▾ | todde | Log Out
| Help ▾ | admin | Log Out
SANtricity® System Manager
NVME5700
Preferences | Help ▾ | admin | Log Out
Home
Storage
Hardware
Settings
Support
Home / Settings
ALERTS
Alerts have not been configured
SYSTEM
Automatic Load Balancing: Enabled
ACCESS MANAGEMENT
Directory Services have been configured
CERTIFICATES

SANtricity web server security certificates

In addition to authentication and access control, SANtricity System Manager supports standard CA certificates. This support enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On EF600 arrays, the SANtricity System Manager UI is accessed through one of the two controllers. (In the legacy SANtricity Storage Manager application, access was through both controllers simultaneously.) As a result, all communication to the other controller in the EF600 array is performed through the midplane in the shelf.

Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. For proper communication, both controllers must present a self-signed certificate to each other. This process happens automatically when the admin or security user logs in to each controller and opens the Certificates tile. Figure 31 shows the dialog box that is displayed the first time the tile is opened.

Figure 31) Initial step required to set up web server certificates.



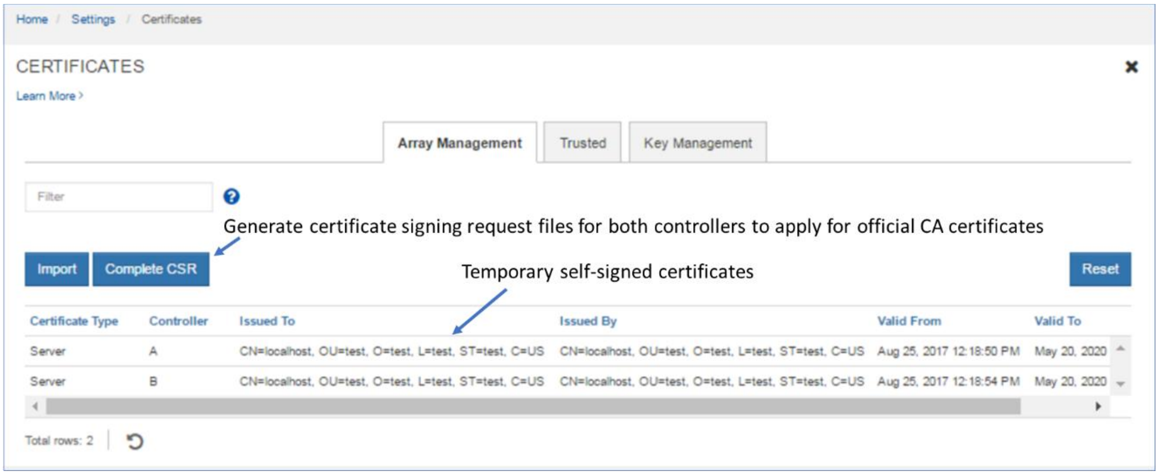
Cannot Access Other Controller

Acceptance of Self-Signed Certificate Is Required

To perform CA certificate related operations, we must communicate with both controllers in the storage array. To do so, you must initially accept the self-signed certificate for the other controller. Once you have accepted the certificate, then you will be able to perform the necessary certificate operations.

You must accept the self-signed certificate to continue setting up certificates. The process takes you to another webpage, where the certificate is created in the background. Follow the prompts to complete the process. When the process is complete, the array requires the admin user or a user with security permissions to log in again. Both controllers are then displayed with valid local host certificates, as shown in Figure 32.

Figure 32) Expanded SANtricity System Manager Certificates tile.



Home / Settings / Certificates
CERTIFICATES
Learn More ›
Array Management
Trusted
Key Management
Filter
Generate certificate signing request files for both controllers to apply for official CA certificates
Import
Complete CSR
Temporary self-signed certificates
Reset

Certificate Type	Controller	Issued To	Issued By	Valid From	Valid To
Server	A	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	Aug 25, 2017 12:18:50 PM	May 20, 2020
Server	B	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	Aug 25, 2017 12:18:54 PM	May 20, 2020

Total rows: 2

To enable the E-Series onboard web servers to validate certificates from external client browsers, the controllers are preloaded with industry-standard CA root certificates. To view the standard root certificates, select the Trusted tab in the Certificates tile window shown in Figure 32 and then select Show Preinstalled Certificates from the drop-down menu.

Multifactor authentication

Feature overview

Multifactor authentication (MFA) includes several functional areas on EF600 arrays:

- **Authentication with Security Assertion Markup Language (SAML) 2.0 to support MFA.** You can manage authentication through an identity provider (IdP) by using SAML 2.0. An administrator establishes communication between the IdP system and the storage array and then maps IdP users to the local user roles embedded in the storage array. Using IdP allows the administrator to configure MFA.

- **Digitally signed firmware.** The controller firmware verifies the authenticity of any downloadable SANtricity firmware. Digitally signed firmware is required in controller firmware version 8.42 (SANtricity 11.40.2) and later. If you attempt to download unsigned firmware during the controller upgrade process, an error is displayed, and the download is aborted.
- **Certificate revocation checking by using Online Certificate Status Protocol (OCSP).** Certificate management includes certificate revocation checking through an OCSP server. The OCSP server determines whether the CA has revoked any certificates before the scheduled expiration date. The OCSP server then blocks the user from accessing a server if the certificate is revoked. Revocation checking is performed whenever the storage array connects to an AutoSupport server, external key management server, LDAPS server, or syslog server. Configuration tasks are available from Settings > Certificates and require security admin permissions.
- **Syslog server configuration for audit log archiving.** In access management, you can configure a syslog server to archive audit logs. After configuration, all new audit logs are sent to the syslog server; however, previous logs are not transferred. Configuration tasks are available from Settings > Access Management and require security admin permissions.

How MFA works

MFA is provided through the industry standard SAML protocol. SAML does not directly provide the MFA functionality; instead, it allows the web service to send a request to an external system. The external system requests credentials from the user and verifies those credentials. Information about the authenticated user is then returned to the web service to allow the user to be assigned appropriate roles. With the previous E-Series authentication methods, the web service was responsible for requesting the user credentials and authenticating the user. With SAML, an external system provides all authentication activity. The external system can be configured to require any amount and types of user authentication factors.

SAML identifies two types of systems that cooperate to provide authentication of users:

- **Identity provider.** The identity provider (IdP) is the external system that does the actual authentication of users by requesting the user credentials and verifying their validity. Maintenance and configuration of the IdP is your responsibility.
- **Service provider.** The service provider (SP) is the system that sends a request to the IdP to have a user authenticated. For E-Series storage arrays, the controllers are the service providers; each controller is a separate SP.

Using SAML to provide MFA also enables single sign-on (SSO) capabilities. If multiple applications are configured to use the same IdP, SSO enables them to accept the same user credentials without requiring users to reenter them. The SSO feature is available only if the user is accessing these applications with the same browser.

Note: When SAML is enabled, SANtricity System Manager is the only management access point. There is therefore no access through the SANtricity CLI, the SANtricity Web Services REST API, in-band management (I/O path that uses a host agent), or native SYMbol interface. The lack of SYMbol access means that you cannot use the Storage Manager EMW or other SYMbol-based tools such as the NetApp Storage Management Initiative Specification (SMI-S) provider.

For more information about MFA, see the E-Series online help center and the E-Series Documentation Center. For detailed explanations about the full set of SANtricity management security features and settings, see TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide.

SANtricity storage features

SANtricity offers several layers of storage features, including security for data at rest, features that manage host paths, features to manage large-capacity drives that ensure data integrity and efficiently manage drive faults, and features that provide data protection. The following sections describe many of the features and provide links to additional information resources.

Drive encryption

When external key management is enabled from the Settings tile, use the Key Management tab to generate a certificate signing request (CSR) file. Use the CSR file on the key management server to generate a client certificate. Import the client certificate from the Key Management tab to enable secure communication between the E-Series controllers and the external key management server. For more information about the SANtricity drive security feature, see the E-Series online help center and TR-4474: SANtricity Drive Security.

SANtricity host and path management features

When considering the elements of E-Series multipath functionality, you must understand two concepts. The first is controller-to-volume ownership and how path failover between controllers is managed through asymmetrical logical unit access (ALUA) for SCSI hosts or asymmetric namespace access (ANA) for NVMe-oF hosts. This scenario occurs when the primary paths to an E-Series volume (I/O paths through the owning controller) are lost. The second concept concerns how the multipath driver on the host interacts with multiple ports on each E-Series controller (target port group support, or TPGS for SCSI hosts, or ANA for NVMe-oF hosts) to spread I/O across the interfaces and maximize performance. For a deep explanation of E-Series multipath behavior, see TR-4604: Clustered File Systems with E-Series Products: BPG for Media.

The design of the E-Series multipath behavior has evolved from a host multipath driver–managed scenario (explicit failover) to the new E-Series–led path management model (implicit failover). However, the E-Series fundamentals have not changed. For example, E-Series systems have asymmetric dual active controllers with the following characteristics:

- Volume ownership alternates as volumes are provisioned.
- Write I/O is mirrored to the peer controller.
- Both controllers have access to every volume on the array.
- Both controllers have multiple host ports.
- If one E-Series controller fails, the other controller takes control of all the volumes and continues to process I/O.

These attributes allow host multipath drivers to spread I/O across each controller's ports that are associated to the volumes owned by that controller. The drivers use path policies such as least queue depth and round robin. Depending on the host operating system, the default path policy is one of these two methods.

When all the paths from a host to one E-Series controller are lost, I/O from that host to the volumes owned by that controller is routed to ports on the other E-Series controller, which performs I/O shipping across the shelf midplane to the controller that owns the volumes. In parallel, a volume-ownership timer is set, and changes in controller-to-volume ownership are delayed until the timer expires. This delay time is long enough for links to reset and return to service (the default is 5 minutes). After the timer expires, the array decides whether to initiate a change of volume ownership to the peer controller. The decision is based on whether the non-owning controller is still receiving more than 75% of the I/O.

Table 4 provides a list of SANtricity host types and the associated support for implicit failover/failback.

Table 4) SANtricity host types and associated failover behavior.

Host type	ALUA/AVT status	Implicit failover	Implicit failback	Automatic load balance
Linux DM-Multipath (kernel 3.10 or later)	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported
Windows	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all operating systems)	Enabled	Supported	Not supported	Not supported

Note: Several uncommon host types also exist as well as host types that are only to be used if instructed to by support. Appearance on the host type list does not imply the option is fully supported; for more information, see the NetApp Interoperability Matrix Tool (IMT) as well as the SANtricity online help.

SANtricity reliability features

Table 5 provides a list of SANtricity reliability features and a brief explanation of each with references to additional information.

Table 5) SANtricity features for long-term reliability.

Reliability features with SANtricity
Media scan with redundancy check. A background scan of media is run on a set schedule and detects data integrity issues. This feature is critically important to turn on by default when you provision new volumes. **Note:** If you have been running I/O to an array with media scan turned off, consult with NetApp Technical Support before you turn it on.
Data assurance (T10 PI). This feature confirms data integrity from the HIC to the drive (end-to-end in the storage array). This data integrity is especially important with large-capacity drives.
Cache mirroring. Each E-Series controller owns a set of volumes and is responsible for processing I/O to and from those volumes. Both controllers have access to all volumes, and by default, all incoming writes are cached in memory on the peer controller. This mechanism enables a second level of data integrity checking and enables E-Series and EF-Series arrays to handle controller failover scenarios gracefully.
Nondisruptive controller firmware upgrade. Using the ALUA or ANA host types with multiple paths to hosts and an upgrade wizard that activates one controller at a time, this feature prevents upgrades from affecting host-to-volume access. **Note:** Not all host operating systems support the ALUA or ANA host type.
Proactive drive monitor and data evacuator. Nonresponsive drives are automatically power-cycled to see if the fault condition can be cleared. If the condition cannot be cleared, the drive is flagged as failed. For predictive failure events, the evacuator feature starts to remove data from the affected drive to move the data before the drive fails. If the drive fails, rebuild resumes where the evacuator was disrupted, reducing the rebuild time.
Automatic drive fault detection, failover, and rebuild. You can perform these tasks by using global hot spare drives for standard RAID and spare pool capacity for DDP.
SSD wear-life tracking and reporting. This metric is found in the Hardware tab's Drive Settings dialog box. It indicates the wear life of SSDs and replaces two SSD wear-life metrics (average erase count and spare blocks remaining) that were in previous versions of SANtricity. The metric is Percent Endurance Used; to access it, select a drive from the hardware view and then select Settings.

Reliability features with SANtricity
Online drive firmware upgrade. This feature upgrades one drive at a time and tracks writes to the affected drives during the upgrade window; it should be used only during low write I/O periods. **Note:** Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.
Automatic load balancing. This feature provides automated I/O workload balancing and confirms that incoming I/O traffic from hosts is dynamically managed and balanced across both controllers. The workload of each controller is continually monitored and analyzed in the background. When I/O on one controller significantly exceeds the I/O on the other controller for a prolonged, predictable period, SANtricity can change volume ownership from the busy controller to the less busy controller. The feature does not react to short-term changes in I/O patterns. However, when a change of ownership is needed, SANtricity interacts with the affected host multipath driver to initiate an implicit path failover. Most current server operating systems and associated multipath drivers support implicit failover. For more information, search for “What is automatic load balancing?” in the System Manager online help.
Embedded SNMP agent. For the EF600 controller, SNMP is supported natively. The embedded SNMP agent complies with the SNMP V2C standard and RFC 1213 (MIB-II). For more information, search for “manage SNMP alerts” in the System Manager online help.
Automatic alerts. This feature sends email alerts to notify data center support staff about events on the storage array.
Event Monitor and system log. The SANtricity Storage Manager Event Monitor automatically records events that occur on the storage array. Syslog enables a second level of activity tracking that allows you to connect events with associated changes recorded in the system log.
AutoSupport. E-Series products have supported AutoSupport for several releases.
Ability to enable or disable AutoSupport maintenance window. AutoSupport includes an option for enabling or suppressing automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a support case if there is an issue. To enable or disable the AutoSupport maintenance window, select Support > Access Management > AutoSupport.

SANtricity storage management features

E-Series EF600 systems ship with significant storage management features that can be activated from SANtricity System Manager. Table 6 lists standard features included with SANtricity OS.

Table 6) Standard features that are included with SANtricity.

Standard features with SANtricity
SANtricity System Manager (embedded single-array management). The browser-based, on-box SANtricity System Manager is used to manage individual new-generation storage arrays. • Access all array setup, storage provisioning, and array monitoring features from one UI. • System Manager includes an embedded RESTful API that can be used for management.
Volume workload tags. SANtricity System Manager provides a built-in volume tagging feature that allows administrators to organize the volumes in their arrays by workload type. Usually, the tag is only for organization purposes. In some cases, the Volume Creation wizard provides suggested configuration or volume segment size settings associated with the workload type. You do not have to accept the recommendations. The configurations are suggestions for saving time when you provision volumes for common applications.
Storage partitions. Partitions can consist of an individual host without shared volumes, host groups with shared volumes, or a combination of both. This concept has been abstracted in the new System Manager, but you can view the partitions by using a CLI.
Changing host protocol. This capability is supported through new feature pack keys. To obtain free activation codes and detailed instructions for each starting and ending protocol, go to the E-Series and SANtricity 11 Resources page (Maintain E-Series hardware).

SANtricity Remote Storage Volumes

The Remote Storage Volumes feature enables customers to import data through iSCSI from an existing remote storage device onto an E-Series volume with minimal downtime. It can be used to help streamline the process for equipment upgrades and/or provide data migration capabilities to move data from non-E-Series devices to E-Series systems.

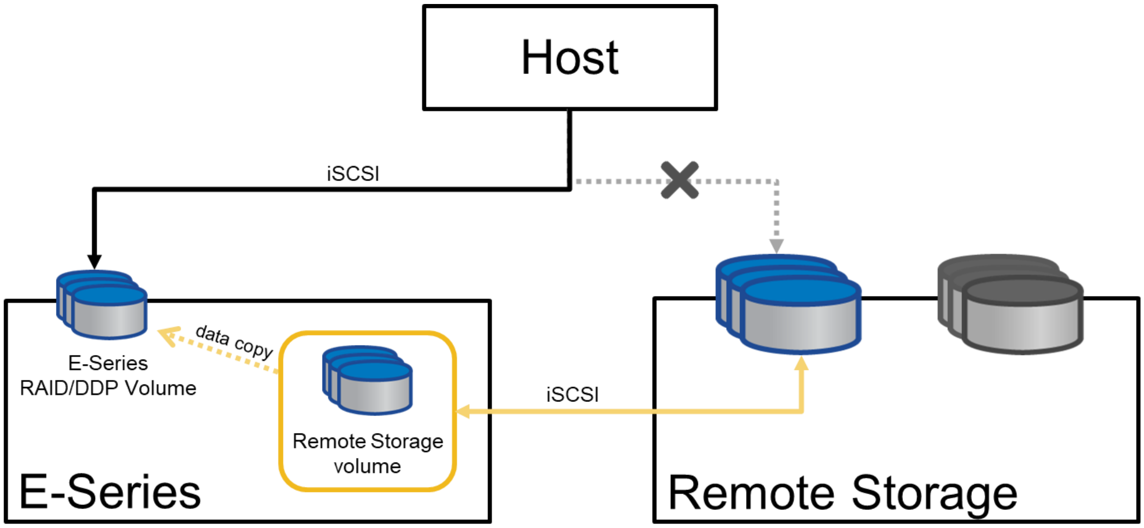
The base function for this feature is to support importing data from a remote storage device directly to a local E-Series volume. To use this feature, an iSCSI connection must first be manually established between the remote storage device and the E-Series system. The remote storage then needs to be configured to have one or more IP addresses where the iSCSI IQNs of the remote storage devices can be discovered.

With the iSCSI connection in place, the remote storage device can then be mapped to the E-Series system. After the mapping is in place, you can then use SANtricity System Manager or REST API commands for the E-Series system to initiate and manage the import operation.

During the import operation, the target volume can be set up to process the I/O operations that the remote storage device was originally processing. Any I/O operations going to the target volume are then propagated back to the remote storage device until the import operation has completed and the import has been disconnected.

Figure 33 shows the technical components of the solution.

Figure 33) Remote Storage Volumes solution architecture overview.



Information that you must provide to initiate the import operation includes:

- Remote storage iSCSI IQN
- Remote storage iSCSI IP addresses
- LUN number where the remote device is mapped

The provided information must persist on the E-Series system so that it can remain accessible after reboots, power cycles, and so on.

After it is configured, you can update the remote storage iSCSI IQN and/or iSCSI IP addresses, if needed, through either SANtricity System Manager or REST API commands.

For more information about remote storage volumes, see TR-4893-DEPLOY: SANtricity Remote Storage Volumes.

SANtricity copy services features

Table 7 lists standard copy services features with EF600 storage arrays.

Table 7) SANtricity copy services features.

Standard SANtricity copy services features
SANtricity Snapshot copies. Point-in-time NetApp Snapshot™ copies.
Asynchronous mirroring. Mirroring to a remote site where RPO = 0 is not a requirement.
Volume copy. Used to clone volumes for testing/development or analytics purposes.

For additional details and use case information about SANtricity copy services features, see TR-4458: Deploying NetApp E-Series and EF-Series Copy Services with Oracle and SQL Server Databases.

For details on using SANtricity Snapshots see TR-4747: SANtricity Snapshot Feature Overview and Deployment Guide.

Starting with SANtricity 11.62 the Unified Manager is used to create mirror relationships. See TR-4839: SANtricity Synchronous and Asynchronous Mirroring Feature Descriptions and Deployment Guide (11.62 and Later) or the Online Help in SANtricity Unified Manager for a complete description. SANtricity Unified Manager must be version 4.2 or later and SANtricity System Manager must be OS version 11.62 or later.

Prior to SANtricity 11.62, for a description of mirroring between two new generation E-Series arrays or between a new generation E-Series array and a legacy E-Series array, see TR-4656: SANtricity Synchronous and Asynchronous Mirroring Feature Descriptions and Deployment Guide (11.61 and Earlier).

SANtricity management integration

Starting with SANtricity 11.40 and continuing with SANtricity 11.70.x, the E-Series SANtricity integration model changed focus. To support today's modernized data center operations and partner appliances, NetApp is deemphasizing legacy plug-ins and emphasizing API integration.

Table 8 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. To download the latest version of the E-Series SANtricity Web Services (REST API) visit NetApp Support at http://mysupport.netapp.com/. Information for how to use Ansible with E-Series for managing your storage can be in TR-4574: Deploying NetApp E-Series with Ansible (Automating E-Series). For the Windows PowerShell toolkit, go to the NetApp PowerShell Toolkit page of the NetApp Support Site.

Table 8) SANtricity APIs and toolkits.

APIs and toolkits	Description
SANtricity Web Services Proxy **Note:** You can use either the proxy or the embedded REST API for new-generation systems.	These web APIs provide a collection of REST interfaces to configure, manage, and monitor E-Series systems.
NetApp E-Series and Ansible	Ansible is a simple yet powerful orchestration tool. NetApp E-Series has joined the Ansible community to provide you with a high-quality solution for managing your E-Series storage systems, regardless of scale.
NetApp PowerShell Toolkit	The unified toolkit provides end-to-end automation and storage management across NetApp storage systems.

APIs and toolkits	Description
SANtricity Secure CLI	New in SANtricity 11.60.2 is the ability to download the SANtricity Secure CLI (SMcli) from System Manager.

Table 9 provides a list of third platform plug-ins that use E-Series storage systems as building blocks. Usually, the plug-ins listed are available on the various provider websites. For more information about third platform integration with EF-Series storage systems, contact your NetApp sales representative.

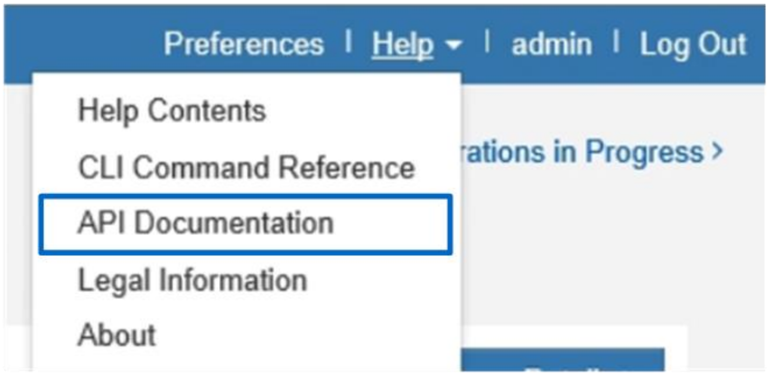
Table 9) Third platform plug-ins that use the SANtricity Web Services Proxy.

Software package	Use
NetApp SANtricity Performance App for Splunk Enterprise https://splunkbase.splunk.com/app/1932/ Technology Add-On for NetApp SANtricity https://splunkbase.splunk.com/app/1933/	A display and monitor tool to report configuration and performance details of multiple E-Series systems in one interface. Requires both application and technology add-on.
NetApp E-Series + Grafana: Performance Monitoring https://github.com/netapp/eseries-perf-analyzer	The E-Series Performance Analyzer is a powerful and easy-to-use tool to monitor the performance of your E-Series storage system.

SANtricity Web Services native REST API

The SANtricity Web Services REST API is an embedded API for experienced developers. Actions performed through the REST API are applied on execution and without user prompts or confirmation dialog boxes. The REST API is URL based, and the accompanying API documentation is completely interactive. Each URL contains a description of the corresponding operation and enables you to perform the action directly through the API documentation. To access the documentation, select API Documentation in the Help drop-down menu from any page in System Manager, as shown in Figure 34.

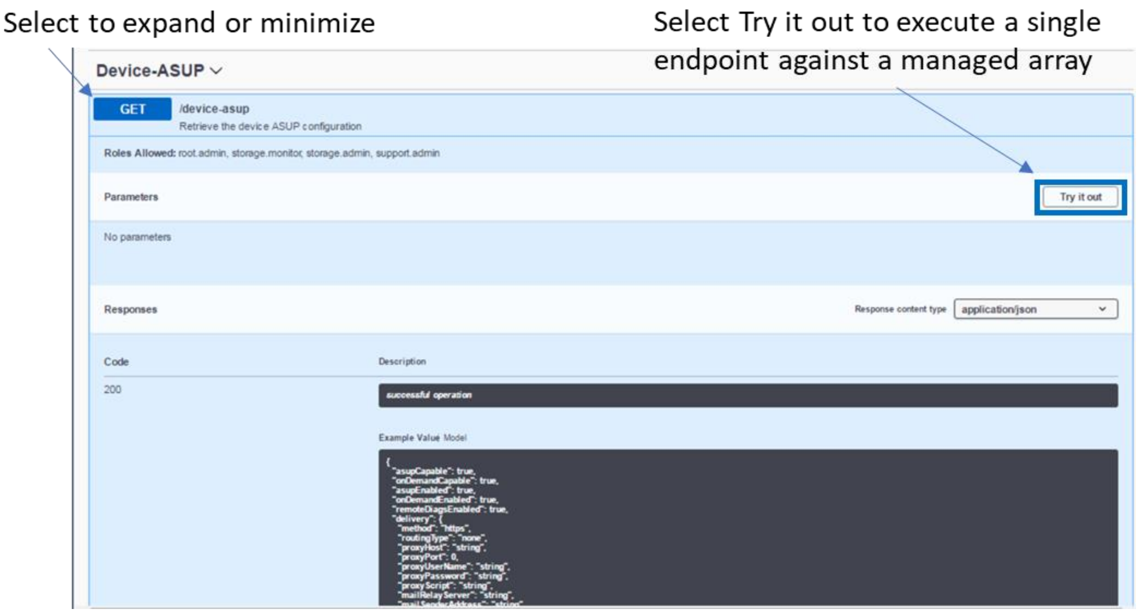
Figure 34) Opening the API documentation.



Each URL endpoint presented in the API documentation has a corresponding POST, DELETE, or GET option. These URL endpoint options, known as HTTP verbs, are the actions available through the API documentation. A sample from the REST API documentation is shown in Figure 35. You can expand or hide operations by selecting the drop-down beside the topic name or clicking the individual endpoints. Click Try It Out to execute the endpoint. You must click Execute to run an endpoint (Figure 36).

Note: To execute successfully, some endpoints require additional input parameters in the Try It Out dialog box. No additional input is required for this example.

Figure 35) Example of expanding the Device-ASUP endpoint.


Select to expand or minimize

Select Try it out to execute a single endpoint against a managed array

Retrieve the device ASUP configuration

Roles Allowed: root.admin, storage.monitor, storage.admin, support.admin

No parameters

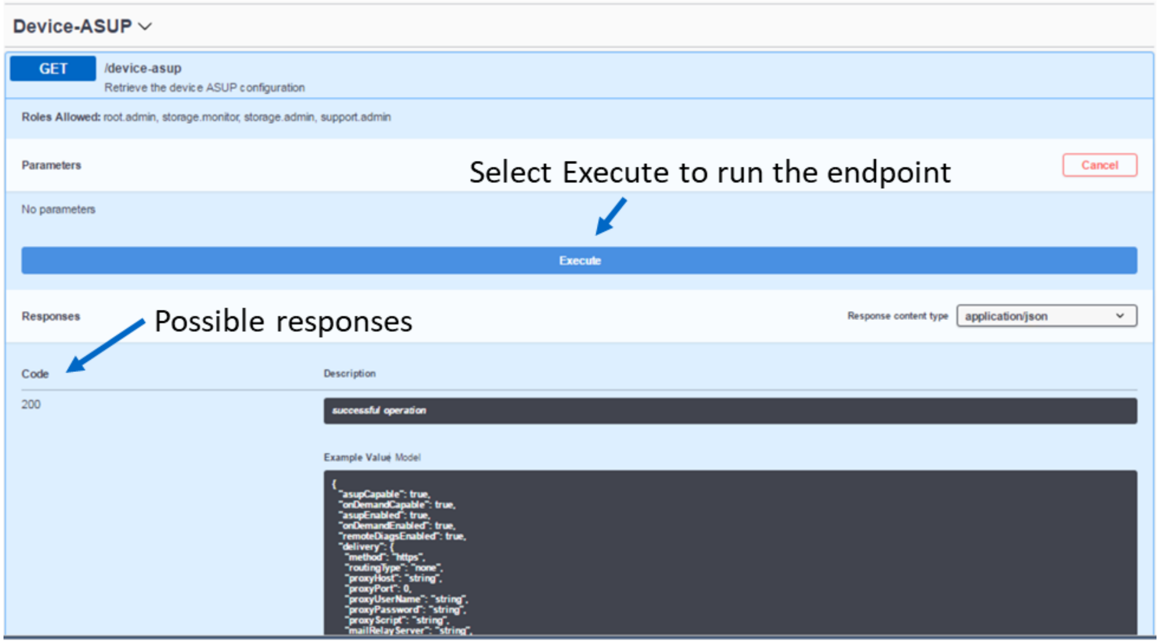
Response content type: application/json

Code	Description
200	successful operation

Example Value Model

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
    "mailSenderAddress": "string"
```

Figure 36) REST API documentation sample.



Retrieve the device ASUP configuration

Roles Allowed: root.admin, storage.monitor, storage.admin, support.admin

Select Execute to run the endpoint

No parameters

Possible responses

Response content type: application/json

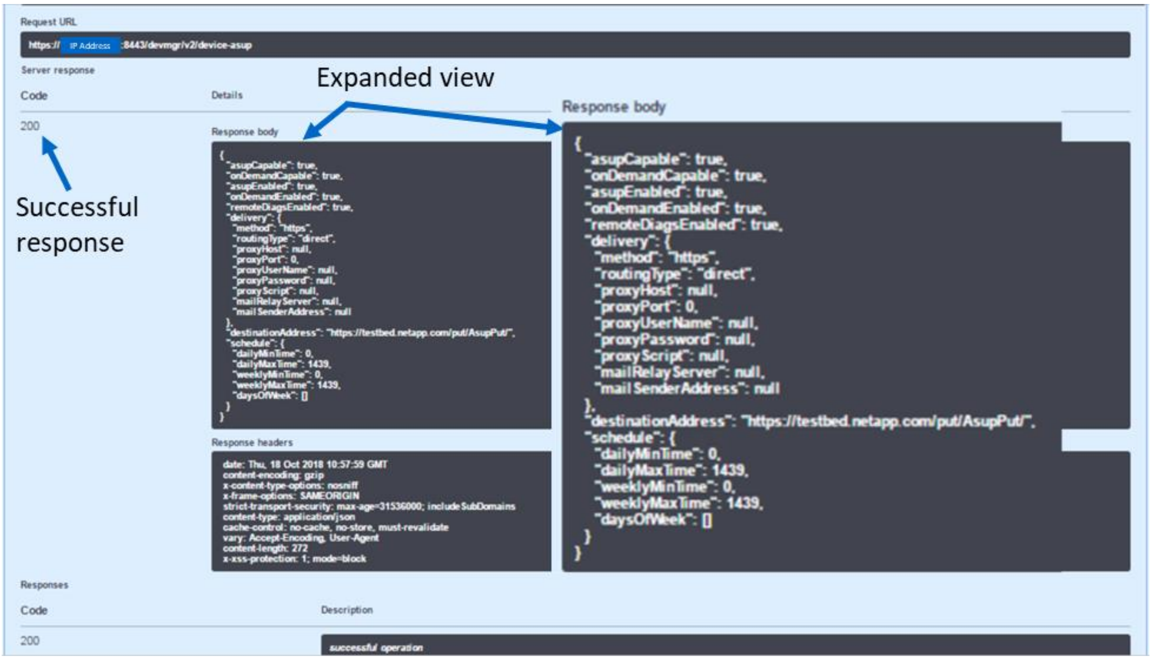
Code	Description
200	successful operation

Example Value Model

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
```

The corresponding output for the GET device-asup verb is shown in Figure 37 and Figure 38.

Figure 37) Sample output from the Try It Out button.

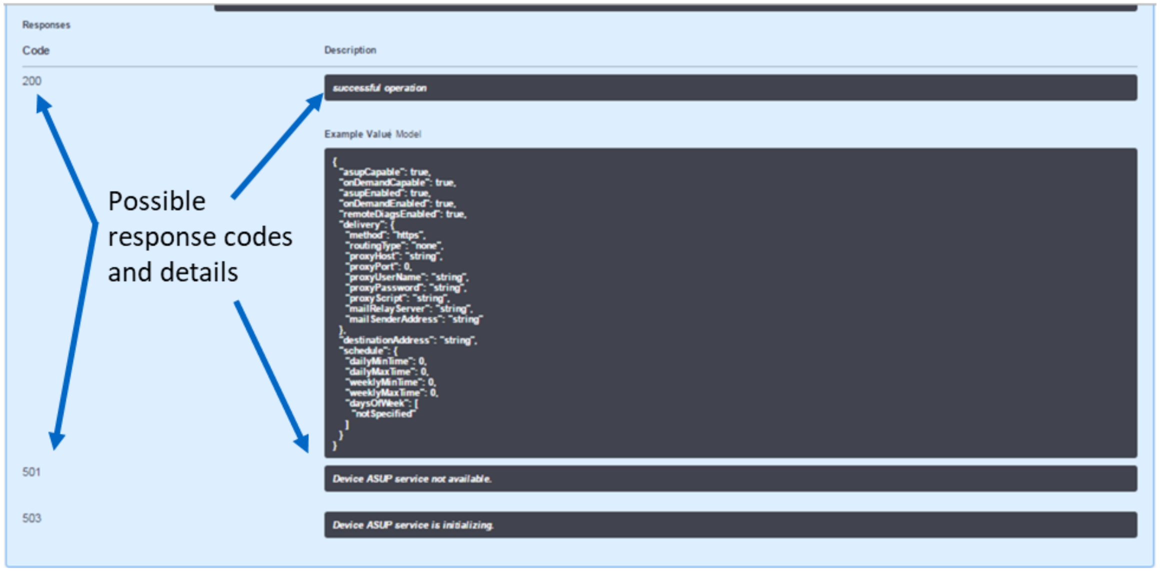


```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "direct",
    "proxyHost": null,
    "proxyPort": 0,
    "proxyUserName": null,
    "proxyPassword": null,
    "proxyScript": null,
    "mailRelayServer": null,
    "mailSenderAddress": null
  },
  "destinationAddress": "https://testbed.netapp.com/put/AsupPut/",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 1439,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 1439,
    "daysOfWeek": []
  }
}
```

```
date: Thu, 18 Oct 2018 10:57:59 GMT
content-encoding: gzip
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; include SubDomains
content-type: application/json
cache-control: no-cache, no-store, must-revalidate
vary: Accept-Encoding, User-Agent
content-length: 272
x-xss-protection: 1; mode=block
```

successful operation

Figure 38) Device-asup endpoint possible response codes and details.



successful operation

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
    "mailSenderAddress": "string"
  },
  "destinationAddress": "string",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 0,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 0,
    "daysOfWeek": [
      "notSpecified"
    ]
  }
}
```

Device ASUP service not available.

Device ASUP service is initializing.

Data in the REST API is encoded through JSON. The structured JSON data from the REST API can be easily parsed by programming languages (C, C++, cURL, Java, Python, Perl, and so on). JSON is simple encoding based on key-value pairs with support for list and subject objects. Objects start and end with curly braces (that is, { }), whereas lists start and end with brackets (that is, [ ]). JSON understands values that are strings, numbers, and Booleans. Numbers are floating-point values. The API documentation provides a JSON template for each applicable URL operation, allowing the developer to simply enter parameters under a properly formatted JSON command.

For more information, see the E-Series Documentation Center.

SANtricity Secure CLI

The SANtricity Secure CLI is an embedded API for experienced developers. From System Manager you can download the CLI package. The CLI provides a text-based method for configuring and monitoring storage arrays. It communicates via HTTPS and uses the same syntax as the CLI available in the externally installed management software package. No key is required to download the CLI.

A Java Runtime Environment (JRE), version 8 and above, must be available on the management system where you plan to run the CLI commands.

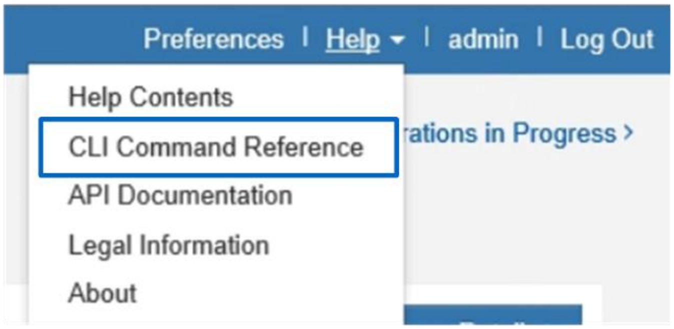
Downloading the CLI

- Select the Settings view > System.
- Under Add-ons, select Command Line Interface. The ZIP package downloads to the browser.
- Save the ZIP file to the management system where you plan to run CLI commands for the storage array, and then extract the file.

You can now run CLI commands from an operating system prompt, such as the DOS C: prompt.

To access the documentation, select CLI Command Reference in the Help drop-down menu from any page in System Manager A CLI, as shown in Figure 39.

Figure 39) Opening the CLI Command Reference.



SANtricity Storage Plugin for vCenter

The vSphere Client is a single management interface that you can use to manage the VMware infrastructure and all your day-to-day storage needs. The following functions are available in the NetApp SANtricity Storage 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 operating system.
- 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.

  Note: The plugin is not a direct replacement for the 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 web server.

You can download the plugin from the NetApp Support Site, NetApp Support Site > Downloads > All Downloads.

You can find installation and configuration documentation on the NetApp Documentation site, E-Series and SANtricity Documentation Center.

SANtricity OS specifications for EF600 hardware

Table 10 lists the NetApp SANtricity OS specifications for NetApp EF600-based storage systems.

Table 10) SANtricity OS boundaries for EF600-based storage systems.

Components	Maximum
Storage hardware components	
Shelves (controller and expansion)	8 (1 controller plus 7 expansion shelves) **Note:** If only DE212C shelves are present, then 8 expansion shelves are permitted.
Maximum drives—drive slot count	24 NVMe SSDs plus 96 SAS SSDs or 420 NL-SAS HDD
SSD cache capacity	8TB
Logical components	
Host partitions	1024
Volumes per partition	256
Volumes per system	2,048
Disk pools per system	20
Volumes per disk pool	2,048
Total DDP capacity in an array (maximum capacity includes RAID overhead, DDP reserve capacity, and a small DDP-specific overhead based on the number of drives in the pool and other factors)	12PiB maximum DDP capacity per EF600 array
Maximum DDP single volume capacity	4PiB
Maximum standard RAID capacity limits	Limits for standard RAID based on maximum supported drives per RAID type: • 30 drives of any supported capacity for RAID 5 and RAID 6 (only 24 NVMe drives supported with EF600) • All drives of any supported capacity for RAID 10
Maximum single volume capacity for standard RAID	4PiB
Maximum standard RAID volumes per volume group	256
Maximum standard RAID single volume capacity	15EiB (theoretical maximum limit—actual limit based on RAID type, number of data drives per volume group, and the capacity of the drives used)
Consistency groups	
Volumes per consistency groups	64
Consistency groups per system	32
Snapshot copies	
Per Snapshot group	32
Per volume	128
Per storage system	2,048

Components	Maximum
Snapshot volumes	
Per Snapshot copy	4
Per system	1,024
Snapshot groups	
Per volume	4
Per system	1,024
Asynchronous mirrors	
Mirrors per system	256
Mirrors per volume	1
Mirrors per asynchronous mirror group	64
Asynchronous mirror groups per system	4

For additional software limits and specifications, see the Hardware Universe.

Note: EF600 does not require NVMe drives in the controller shelf.

Note: EF600 does not support thin provisioning.

Note: EF600 does not support synchronous mirroring.

EF600 hardware configurations

NetApp EF600 storage systems, like all NetApp E-Series arrays, use a modular approach to hardware configuration. This approach can meet most customer SAN storage requirements for flexible host interfaces and versatile drive choices without sacrificing supportability, ease of implementation, and long-term stability. The E-Series has a proven record of accomplishment for reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers that provide mission-critical infrastructure.

Controller shelf configurations

The following sections provide detailed information about the EF600 shelf configuration.

EF600 controller shelf

The EF600 is a two-rack-unit-high (2U) shelf that holds up to 24 2.5" NVMe SSDs. It features two RAID controllers and two ENERGY STAR Platinum certified high-efficiency power supplies (1600W) with integrated fans.

Figure 40, Figure 41, Figure 42, and Figure 43 show the front and rear views of the EF600 controller shelf.

Figure 40) EF600 front view with bezel.

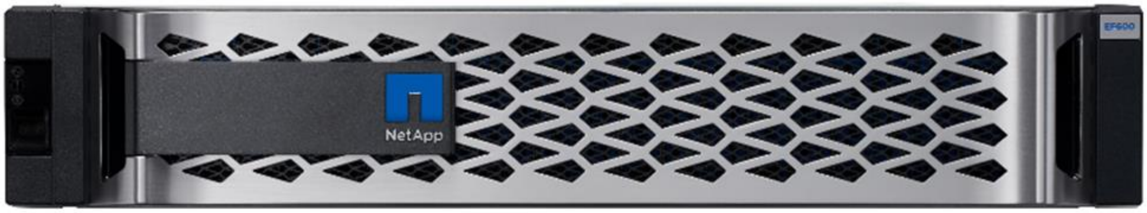


Figure 41) EF600 front view (open).

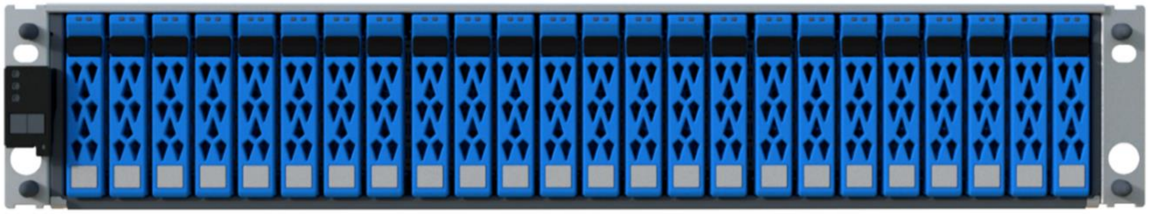


Figure 42) EF600 rear view with HICs in slots 1 and 2 shown.

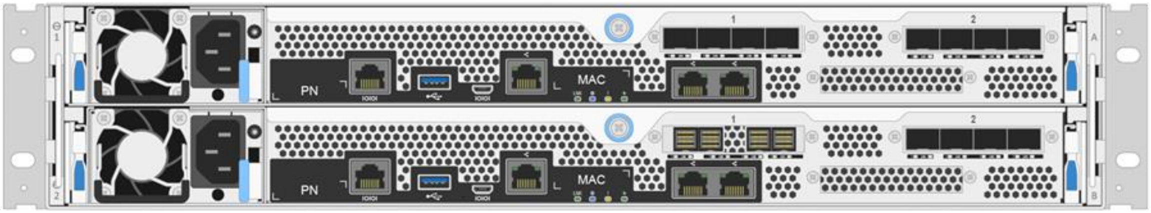
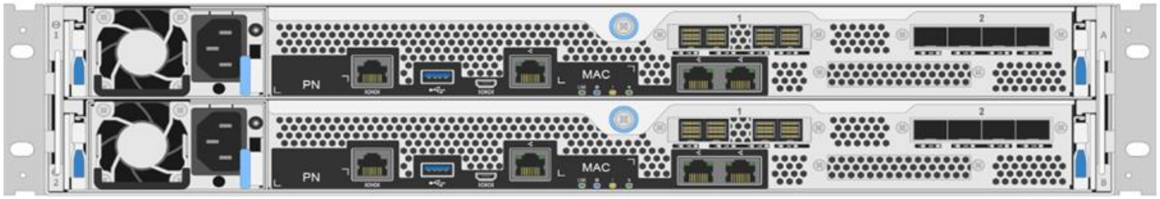


Figure 43) EF600 rear view with optional drive shelf expansion card in slot 1 and HIC in slot 2 shown.



EF600 hardware specifications

The EF600 controller has the following base hardware features:

- Ethernet port for management-related activities
- Dual 10GbE ports for future development
- Optional Quad 12Gb SAS drive expansion ports to attach expansion drive shelves
- Type-A USB port for factory use only is disabled if using SANtricity OS 11.80 or newer

Table 11 lists the technical specifications for the EF600-based storage systems.

Table 11) EF600 technical specifications.

Specification	EF600
Maximum raw system capacity without expansion shelves (assumes 24 SSDs)	367TB (24 x 15.3TB SSDs)
Maximum number of NVMe drives per system	24 NVMe SSDs maximum
NE224 shelf form factor	2U, 24 drives
Memory	32GB or 128GB per controller
	64GB or 256GB per duplex system
• Single HIC per controller • Controllers must match. • A software feature pack* can be applied to convert between host protocols.	2-port 200Gb IB (2 ports per controller) – supports NVMe/IB, NVMe/RoCE, or iSER/IB **Note:** Cannot use expansion card with the single 200Gb HIC.

Specification	EF600
• Cannot mix protocols.	
• Single HIC per controller • Controllers must match. • A software feature pack* can be applied to convert between the various protocols available on each HIC. • Cannot mix protocols. • Must have expansion card installed in HIC slot 1	• 1x 100Gb IB (2 ports per controller) – supports NVMe/IB, NVMe/RoCE, SRP/IB, and iSER/IB according to feature pack installed* • 1x 25Gb iSCSI (4 ports per controller) • 1x 32Gb FC (4 ports per controller) – supports traditional FC as well as NVMe/FC according to feature pack installed*
• Two HICs per controller • Controllers must match. • A software feature pack* can be applied to convert between the various protocols available on each HIC. • Cannot mix protocols.	• 2x 2-port 100Gb IB (4 ports per controller) – supports NVMe/IB, NVMe/RoCE, SRP/IB, or iSER/IB according to feature pack installed* • 2x 4-port 32Gb FC (8 ports per controller) – supports traditional FC as well as NVMe/FC according to feature pack installed*; see the Hardware Universe for SFP details • 2x 4-port 25Gb iSCSI (8 ports per controller); see Hardware Universe for SFP details
Maximum raw system capacity with expansion shelves (assumes 24 NVMe SSDs and 420 NL-SAS drives)	7.9PB equals 7,560TB (420x 18TB NL-SAS) plus 367TB (24x 15.3TB SSDs)
Optional drive shelf expansion	• 12Gb SAS in slot 1 only (4 ports per controller) • Maximum NL-SAS drive expansion supported: Any mixture of DE212C and DE460C shelves not to exceed a total of 420 NL-SAS drive slots and 7 expansion shelves unless only DE212C shelves are used, then 8 DE212C shelves are allowed. For example, 7 DE460C shelves, or 8 DE212C shelves, or 5 DE460C shelves plus 2 DE212 shelves. • Maximum SAS SSD drive expansion supported: Any mixture of DE212C, DE224C, and DE460C shelves not to exceed a total of 96 SAS SSD drive slots and 7 expansion shelves unless only DE212C shelves are used, then 8 DE212C shelves are allowed. For example, 1 DE460C shelf plus 1 DE224C shelf plus 1 DE212C shelf, or 4 DE224C shelves, or 8 DE212C shelves. **Note:** There is no support for 10k SAS drives. **Note:** There is no support for expansion to a second enclosure containing NVMe drives. **Note:** NVMe drives in the controller shelf are not required for addition of expansion shelves.
SAS3 drive shelves supported for expansion drive offerings	DE212C (2RU, 12 drives): 8 expansion shelves maximum.
	DE224C (2RU, 24 drives): 7 expansion shelves maximum.
	DE460C (4RU, 60 drives): 7 expansion shelves maximum.
High-availability (HA) features	Dual active controllers with automated I/O path failover
	Support for RAID 0, 1 (10 for 4 drives or more), 5, 6, and DDP **Note:** It is only possible to create RAID 3 volumes through the CLI. For more information, search for “using the create volume group wizard” in SANtricity System Manager online help.

Specification	EF600
	Redundant, hot-swappable storage controllers, disks, and power supplies. Fans require that you remove the controller to do a replacement.
	Mirrored data cache with battery-backed destage to flash

*For details about the available feature pack submodel IDs (SMIDs) for the EF600 storage controllers, see the section, “Controller host interface features“.

Note: For current supported drive availability information and encryption capability by drive capacity (full disk encryption [FDE] and FIPS), see the Hardware Universe.

Controller host interface features

By default, the EF600 controller includes an Ethernet management port that provides out-of-band system management access.

The management port defaults to the Dynamic Host Configuration Protocol (DHCP). If you want to use static addresses to manage the EF600, simply leave the management ports disconnected for approximately 5 minutes after powering on, to allow the DHCP feature to time out. Then, you can connect with a local PC to the default IP addresses:

- Controller A Management Port = 169.254.128.101
- Controller B Management Port = 169.254.128.102

Host interface ports can be added, as indicated in Table 12. Each HIC supports multiple protocols.

Table 12) Available feature pack submodel IDs (FP-SMIDs) for EF600 controllers.

FP-SMID	HIC protocol
443	NVMe/FC, NVMe/RoCE, or iSCSI
444	NVMe/FC or NVMe/IB
448	FC (not NVMe)
465	FC PTL (not NVMe)
491	iSER/IB
492	SRP/IB (100Gb HIC only)

For instructions on how to obtain and apply a software feature, see the E-Series and EF-Series Systems Documentation Center. Locate the Upgrading > Hardware Upgrade section of the page, select Change or Add Host Protocols, and download the Converting EF600 Host Protocol document.

Table 13 provides port speed details for the NVMe/FC and FC options.

Table 13) FC host interface protocol and supported speeds.

HIC protocol	Supported speeds
32Gbps FC	32Gbps, 16Gbps, 8Gbps
32Gbps NVMe/FC	32Gbps, 16Gbps, 8Gbps

Table 14 provides port speed details for the iSCSI options.

Table 14) iSCSI host interface protocol and supported speeds.

HIC protocol	Supported speeds
25Gbps iSCSI	25Gbps, 10Gbps

Table 15 provides the port speed details for the 200Gbps IB HIC and the 100Gbps IB HIC. The HIC uses autonegotiation to determine the link speed according to the cables and HCAs used on the host.

Table 15) IB host interface protocol and supported speeds.

HIC protocol	Supported speeds
200Gbps NVMe/IB	200Gbps, 100Gbps, 56Gbps
200Gbps NVMe/RoCE	200Gbps, 100Gbps, 50Gbps, 40Gbps, 25Gbps, 10Gbps
200Gbps iSER/IB	200Gbps, 100Gbps, 56Gbps
100Gbps NVMe/IB	100Gbps, 56Gbps, 40Gbps
100Gbps NVMe/RoCE	100Gbps, 50Gbps, 40Gbps, 25Gbps, 10Gbps
100Gbps SRP/IB or iSER/IB	100Gbps, 56Gbps, 40Gbps

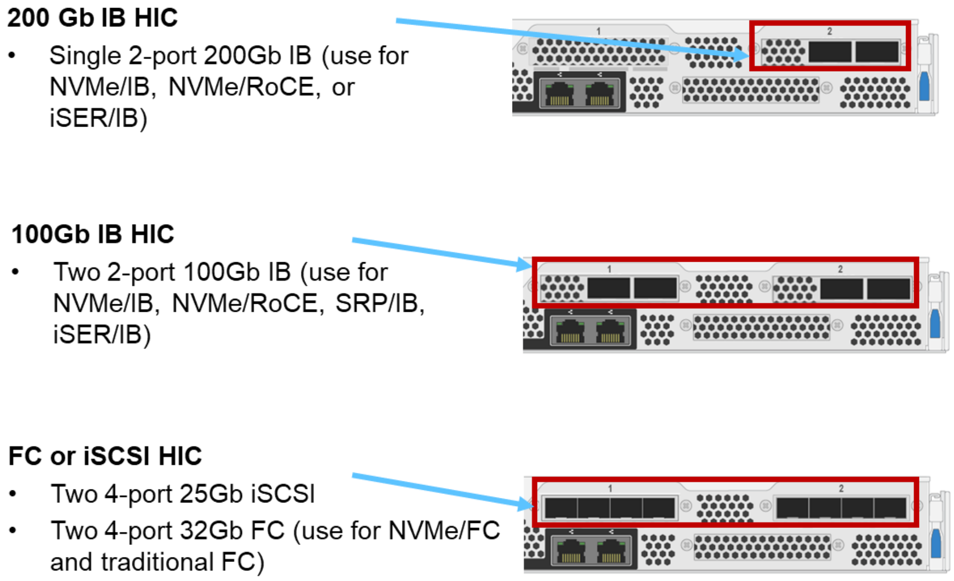
Note: NetApp does not sell IB cables for either port speed; however, cables are readily available from suppliers such as NVIDIA Mellanox and QLogic.

For optical connections, the appropriate SFPs must be ordered for the specific implementation. Consult the Hardware Universe for a full listing of available host interface equipment. All EF600 optical connections use OM4 optical cable.

Note: Both controllers in a duplex configuration must be configured identically.

The HIC options are shown in Figure 44.

Figure 44) EF600 controller HIC options.



200 Gb IB HIC

- Single 2-port 200Gb IB (use for NVMe/IB, NVMe/RoCE, or iSER/IB)

100Gb IB HIC

- Two 2-port 100Gb IB (use for NVMe/IB, NVMe/RoCE, SRP/IB, iSER/IB)

FC or iSCSI HIC

- Two 4-port 25Gb iSCSI
- Two 4-port 32Gb FC (use for NVMe/FC and traditional FC)

Hardware LED definitions

EF600 controller shelf LEDs

The EF600 controller shelf has LED status indicators on the front of the shelf, the operator display panel (ODP), the rear of the shelf, the power supply, and the controller canisters. The LEDs on the ODP indicate systemwide conditions, and the LEDs on the power-fan canisters and controller canisters indicate the status of the individual units.

Figure 45 shows the ODP of the EF600 controller shelf.

Figure 45) ODP on front panel of EF600 controller shelf.

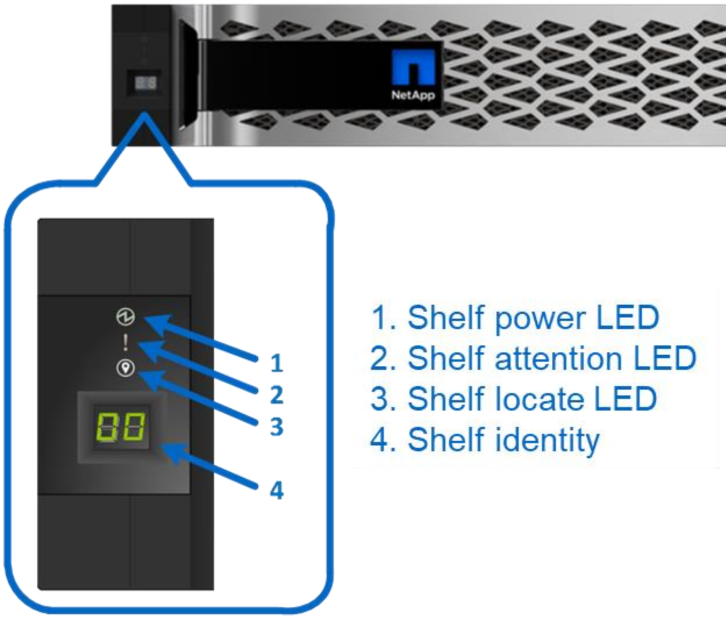


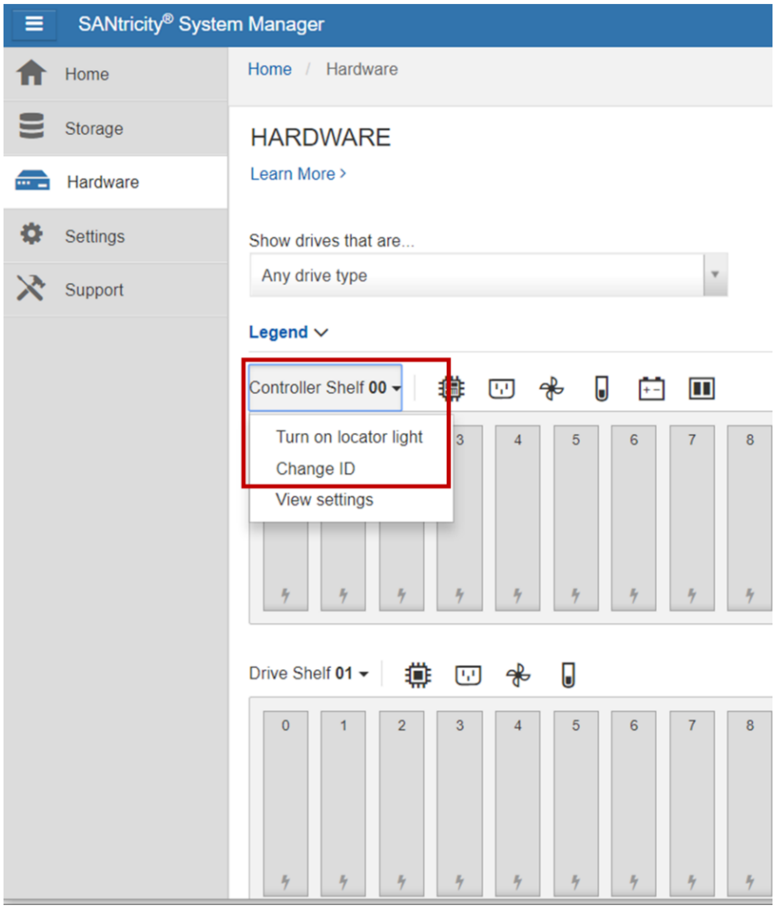
Table 16 defines the ODP LEDs on the EF600 controller shelf.

Table 16) EF600 controller shelf LED definitions (front panel).

LED name	Color	LED on	LED off
Power	Green	Power is present	Power is not present
Attention	Amber	A component in the controller shelf requires attention	Normal status
Locate	Blue	There is an active request to physically locate the shelf	Normal status

The shelf-identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99 that can be set from the NetApp SANtricity System Manager Hardware tab shown in Figure 46.

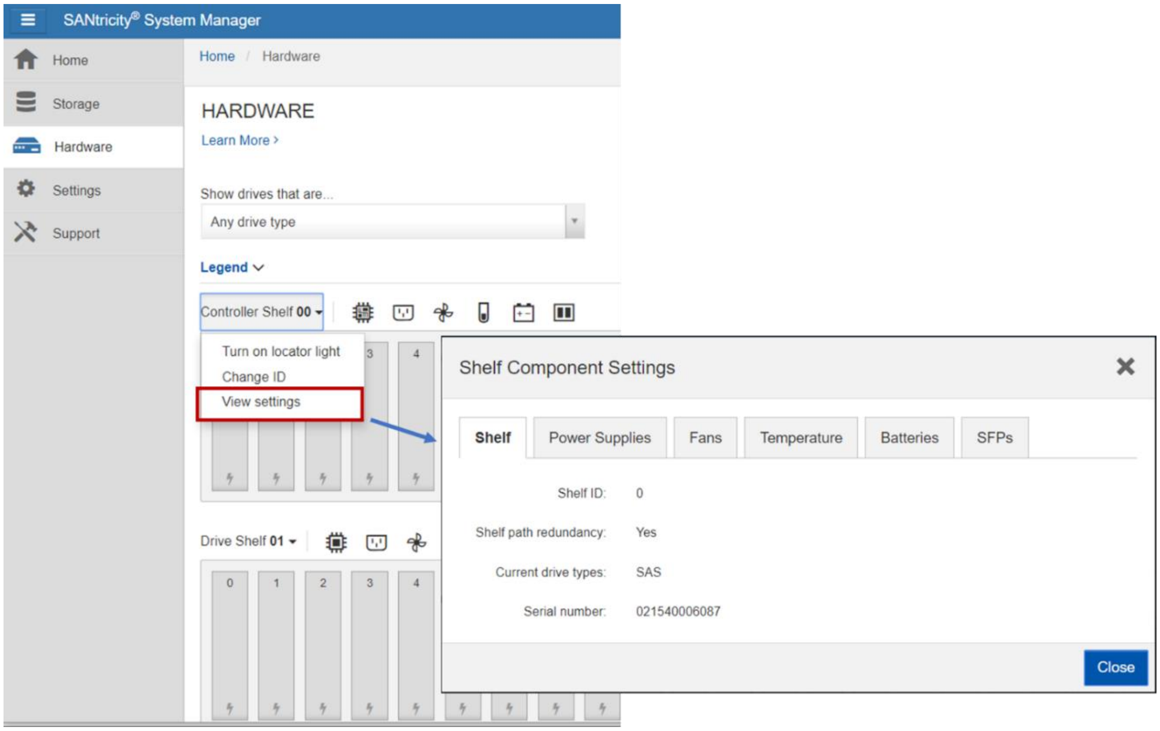
Figure 46) Setting the shelf ID by using SANtricity System Manager.



EF600 controller canister LEDs

The EF600 controller canister has several LED status indicators. You can verify host port status and other system-level status information by directly checking the port LEDs or by using the SANtricity System Manager UI. For example, systemwide status information is displayed on the View Settings page, as shown in Figure 47.

Figure 47) Viewing system status information by using SANtricity System Manager.



Show drives that are...
Any drive type

Shelf ID: 0

Shelf path redundancy: Yes

Current drive types: SAS

Serial number: 021540006087

LED definitions with 2-Port 200Gb IB HIC installed

The EF600 controller supports a single 2-port 200Gbps IB HIC. This HIC supports NVMe/IB, NVMe/RoCE, and iSER/IB according to the feature pack installed. Figure 48 shows the 2-port 200Gb IB HIC.

Figure 48) LEDs on the EF600 with 2-port 200Gb IB HIC.

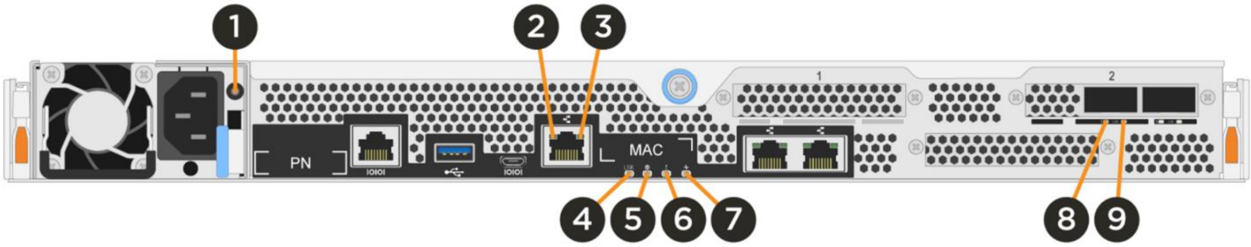


Table 17 defines the LEDs on the 2-port 200Gb IB HIC.

Table 17) EF600 with 2-port 200Gb IB HIC LED definitions.

Call-out	LED name	Color	LED description
1	PSU	Green/red	• LED off: No AC power • Green: AC present and DC output OK • Red: AC cord unplugged or power supply failure
2	Link	Green	• LED on: Link is up • LED off: Link is down
3	Activity	Green	• Blinking: Indicates activity for the Ethernet port

Call-out	LED name	Color	LED description
4	NV LED	Green	Defaults to on at power on. Software turns off this LED during boot. On indicates that battery backup has been enabled to support caching activity.
5	Locate LED	Blue	• On: Identifies enclosure • Off: Not locating enclosure **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete.
6	Attention LED	Amber	• On: Direct attention to the controller for service event • Off: No issues on controller **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete (if no issues are indicated).
7	Activity LED	Green	• Blinking: Activity on controller
8	Attention LED	Amber	• On: A condition that requires attention • Off: No special conditions
9	Link LED	Green	• On: Link up • Off: No link

LED definitions with 2-Port 100Gb IB HICs installed

The EF600 controller supports two 2-port 100Gbps IB HICs. These HICs support NVMe/IB, NVMe/RoCE, SRP/IB, and iSER/IB according to the feature pack installed. Figure 49 shows the 2-port 100Gb IB HIC.

Figure 49) LEDs on the EF600 with 2-port 100Gb IB HICs.

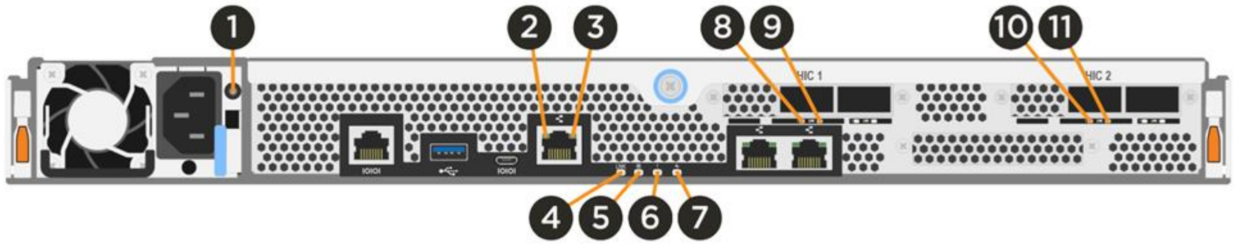


Table 18 defines the LEDs on the 2-port 100Gb IB HIC.

Table 18) EF600 with 2-port 100Gb IB HIC LED definitions.

Call-out	LED name	Color	LED description
1	PSU	Green/red	• LED off: No AC power • Green: AC present and DC output OK • Red: AC cord unplugged or power supply failure
2	Link	Green	• LED on: Link is up • LED off: Link is down
3	Activity	Green	• Blinking: Indicates activity for the Ethernet port
4	NV LED	Green	Defaults to on at power on. Software turns off this LED during boot. On indicates that battery backup has been enabled to support caching activity.
5	Locate LED	Blue	• On: Identifies enclosure

Call-out	LED name	Color	LED description
			• Off: Not locating enclosure **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete.
6	Attention LED	Amber	• On: Direct attention to the controller for service event • Off: No issues on controller **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete (if no issues are indicated).
7	Activity LED	Green	• Blinking: Activity on controller
8	Attention LED	Amber	• On: A condition that requires attention • Off: No special conditions
9	Link LED	Green	• On: Link up • Off: No link
10	Attention LED	Amber	• On: A condition that requires attention • Off: No special conditions
11	Link LED	Green	• On: Link up • Off: No link

LED definitions with 4-Port 32Gb FC HICs installed

The EF600 controller supports two 4-port 32Gbps FC HICs that offer the ability to autonegotiate down to 16Gbps with the 32Gbps SFP and down to 8Gbps with the 16Gbps SFP. The new 32Gbps FC HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 50 shows the LEDs for the 4-port 32Gbps FC HICs.

Figure 50) LEDs on the EF600 with 4-port 32Gb FC HICs.

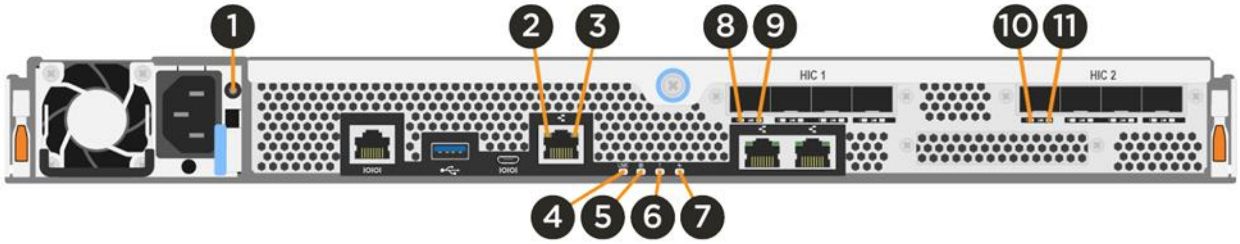


Table 19 defines the LEDs on the 4-port 32Gbps optical HIC.

Table 19) EF600 with 4-port 32Gb FC HIC LED definitions.

Call-out	LED Name	Color	LED description
1	PSU	Green/Red	• LED off: no AC power • Green: AC present and DC output OK • Red: AC cord unplugged or power supply failure
2	Link	Green	• LED on: link is up • LED off: link is down
3	Activity	Green	• Blinking: indicates activity for the Ethernet port

Call-out	LED Name	Color	LED description
4	NV LED	Green	Defaults to on at power on. Software turns off this LED during boot. On indicates that battery backup has been enabled to support caching activity.
5	Locate LED	Blue	• On: identifies enclosure • Off: not locating enclosure **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete.
6	Attention LED	Amber	• On: direct attention to the controller for service event • Off: no issues on controller **Note:** During power on, this LED is on initially, but it will turn off after boot process is complete (if no issues are indicated).
7	Activity LED	Green	• Blinking: activity on controller
8	Attention LED	Amber	• On: a condition that requires attention • Off: no special conditions
9	Link LED	Green	• On: link up • Off: no link
10	Attention LED	Amber	• On: a condition that requires attention • Off: no special conditions
11	Link LED	Green	• On: link up • Off: no link

LED definitions with four-port iSCSI HIC and SAS expansion card installed

The EF600 controller supports an optical 4-port 25Gbps. Figure 51 shows the LEDs for the 4-port HIC and SAS expansion option.

Figure 51) LEDs on the EF600 (4-port HIC and SAS expander shown).

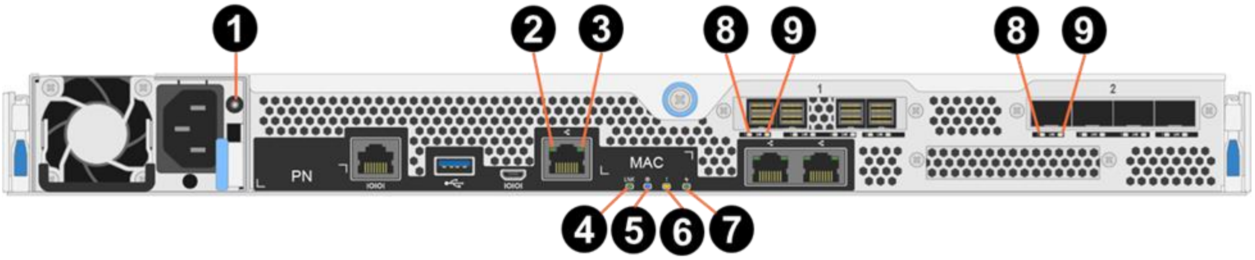


Table 20 defines the LEDs for the 4-port iSCSI HIC and SAS expansion options.

Table 20) EF600 controller LEDs with 4-port or 2-port HIC options definitions.

Call-out	LED name	Color	LED description
1	PSU	Green/Red	• LED off: no AC power • Green: AC present and DC output OK • Red: AC cord unplugged or power supply failure

Call-out	LED name	Color	LED description
2	Link	Green	• LED on: link up • LED off: link down
3	Activity	Green	• Blinking: indicates activity for the Ethernet port
4	NV LED	Green	Defaults to on at power-up. Software turns off this LED during boot. On indicates that battery backup has been enabled to support caching activity.
5	Locate LED	Blue	• On: identifies enclosure • Off: not locating enclosure **Note:** During power-up, this LED is on initially, but it will turn off after boot-up process is complete
6	Attention LED	Amber	• On: direct attention to the controller for service event • Off: no issues on controller **Note:** During power-up, this LED is on initially, but it will turn off after boot-up process is complete (if no issues are indicated).
7	Activity LED	Green	• Blinking: activity on controller
8	Attention LED	Amber	• On: a condition that requires attention • Off: no special conditions
9	Link LED	Green	• On: link up • Off: no link

Note: The LED definitions for port 0c repeat for ports 0d, 0e, and 0f.

For more information about the EF600 storage systems and related hardware, see the E-Series and SANtricity 11 Resources page.

Drive LED definitions

Figure 52 shows the LEDs on the drive carriers for the EF600 SSDs. The NE224C shelf in the EF600 architecture supports only 2.5-inch form-factor SSDs.

Figure 52) EF600 drive carrier LEDs.

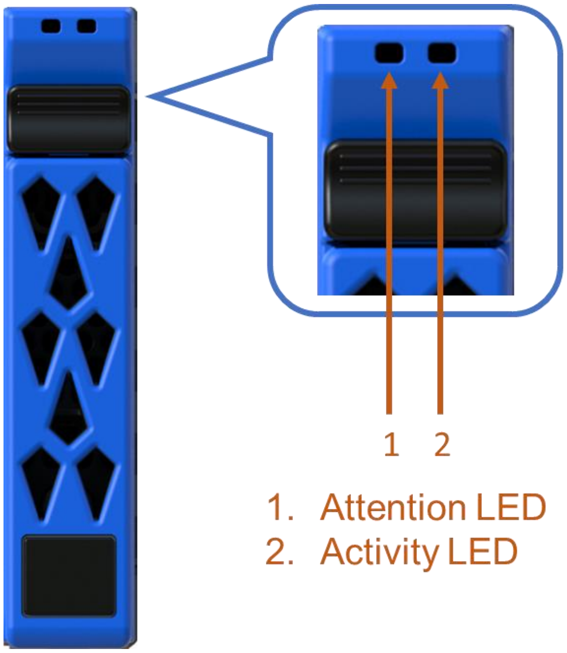


Table 21 defines the LEDs for the drives.

Table 21) EF600 drive LED definitions.

LED Name	Color	LED On	LED Off
Activity	Green	Drive has power	Drive does not have power
	Blinking green	The drive has power, and I/O is in process	No I/O is in process
Attention	Amber	An error occurred with the functioning of the drive	Normal status
	Blinking amber	Drive locate turned on	Normal status

Drive shelves

The EF600 controller shelf supports 24 NVMe SSD drives in the NE224 shelf, but you can further expand the system capacity by adding additional expansion drive shelves to the controller shelf. The EF600 supports up to 420 additional NL-SAS HDD drives or 96 additional SAS SSD drives, the controller shelf plus seven expansion drive shelves, for a maximum of 420 HDDs (120 SSDs). Table 22 shows the drive shelf options.

Table 22) Drive shelf options for EF600.

Property	NE224	DE212C	DE224C	DE460C*
Form factor	2RU	2RU	2RU	4RU
Drive size	2.5"	3.5" 2.5" (with bracket)	2.5"	3.5" 2.5" (with bracket)
Drive types	NVMe SSD	NL-SAS	SAS SSD	NL-SAS

Property	NE224	DE212C	DE224C	DE460C*
		SAS SSD		SAS SSD
Total drives	24	12	24	60
Drive interface	NVMe	12Gb SAS	12Gb SAS	12Gb SAS
Maximum shelves	1	8	7	7

*Each slot is limited to 16.3W in DE460C shelf.

Note: You can mix SAS expansion shelves to achieve a total of 420 NL-SAS drives or 96 SAS SSDs.

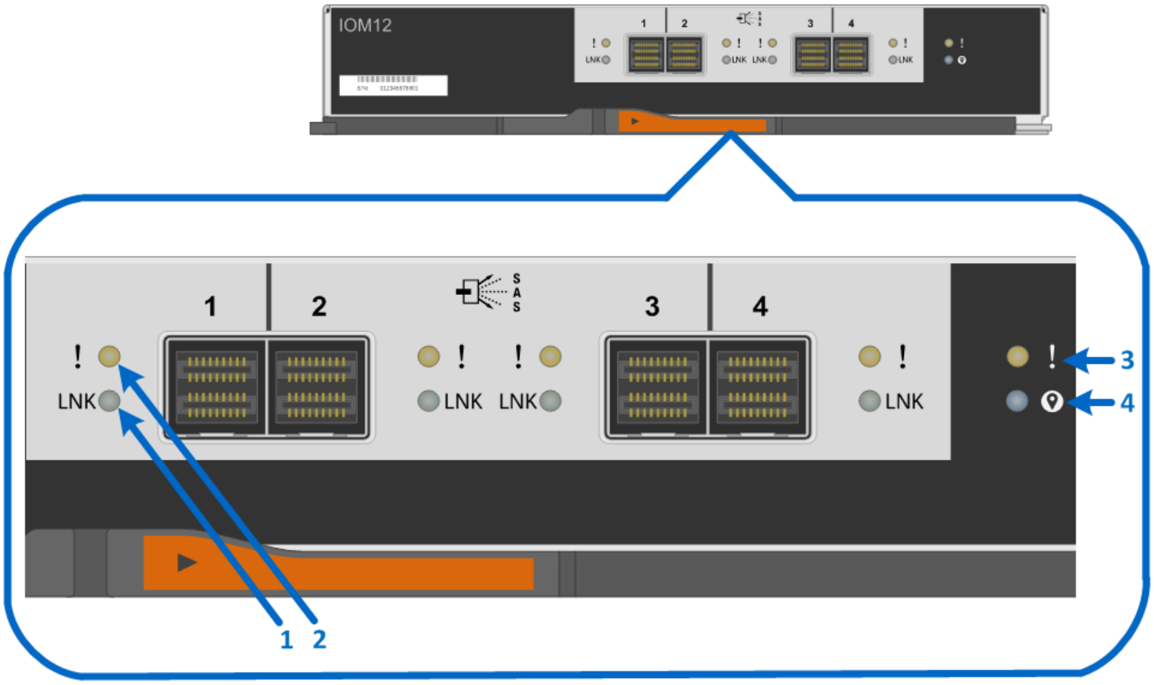
Drive shelf configurations

You can pair EF600 controllers with the 12Gb SAS 3 drive shelves (DE212C, DE224C and DE460C). These shelves are not covered in detail in this document. For more information, see the E-Series Disk Shelves documentation.

IOM LED definitions

Figure 53 shows the LEDs for the 4-port 12Gb SAS 3 IOM. LEDs are highlighted only for SAS expansion port 1 and for the IOM. SAS expansion ports 2 through 4 have the same LEDs.

Figure 53) LEDs for IOM.



1. Drive Expansion Port 1 Link LED
2. Drive Expansion Port 1 Fault LED
3. Attention LED
4. Locate LED

Table 23 defines the LEDs for the IOM.

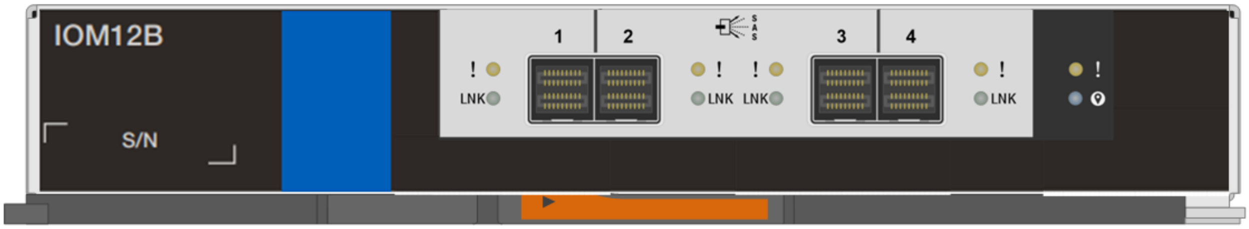
Table 23) IOM LED definitions.

LED name	Color	LED on	LED off
Drive expansion link	Green	Link is up.	Link is down.
Drive expansion fault	Amber	At least one of the four PHYs in the output port is working, but another PHY cannot establish the same link to the expansion output connector.	Port is optimal (all PHYs in the port are up).
Attention	Amber	Some fault exists in the IOM.	Normal status.
Locate	Blue	Request to locate the enclosure is active.	Normal status.

IOM12B

A new IOM the IOM12B has been added for disk expansion shelves. The IOM12B is only supported with SANtricity 11.70.2 and newer SANtricity versions. IOM12 and IOM12B are not supported in the same shelf but can exist in the same stack. Figure 54 shows the new IOM12B.

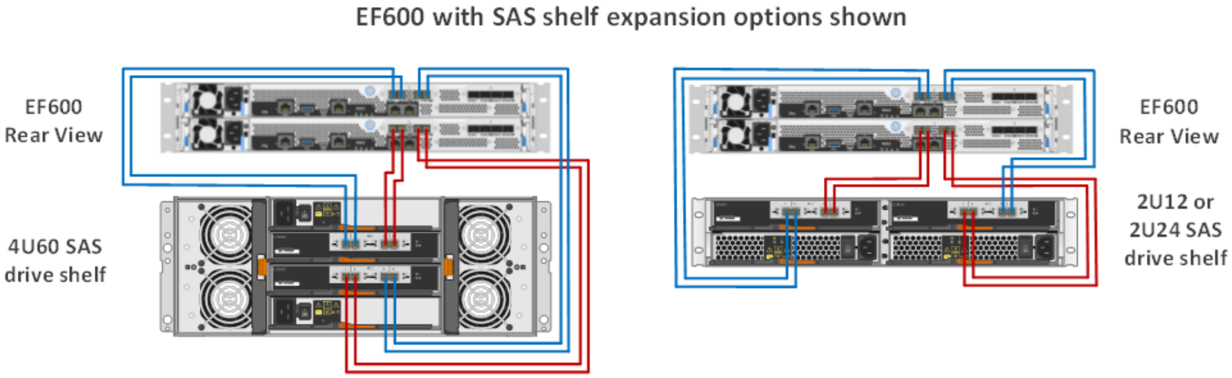
Figure 54) IOM12B.



Greenfield installation

EF600 storage systems make use of an optional four-port SAS HIC in slot 1 of each controller to provide expansion capability, as shown in Figure 3. This new architecture, bringing together NVMe and SAS shelves, results in a modification of the traditional EF-Series cabling, as shown in Figure 55.

Figure 55) EF600 with SAS expansion configuration.



Drive shelf hot add

EF600 storage systems support the addition of expansion drive shelves and drive capacity to running storage systems. To prevent the loss of data availability to existing drive shelves when new drive shelves are added, you must cable the storage system according to the cabling best practices recommended by

NetApp. Two independent SAS channel paths must be available to the drive shelves so that one path can be interrupted when a drive shelf is added to the storage system while the other path maintains data availability to existing shelves.

After additional drive shelves have been successfully added to a storage system, you can use SANtricity to add capacity to existing volume groups and disk pools or to create new volume groups and disk pools.

When adding a drive shelf to an existing EF600 storage system, it is critical to follow the specific hot-add installation steps in the order specified by the E-Series Hardware Cabling Guide.

Note: For more information and assistance with adding a drive shelf to an existing production E-Series system, go to http://mysupport.netapp.com/eseries and click the Cable the Hardware link or contact NetApp Customer Support Delivery.

Figure 56 and Figure 57 show the hot-add connectivity when a drive shelf is added as the last shelf in the system. The DE212C and DE224C are shown; the cabling for DE460C is similar.

Figure 56) Drive shelf hot-add A-side cabling.

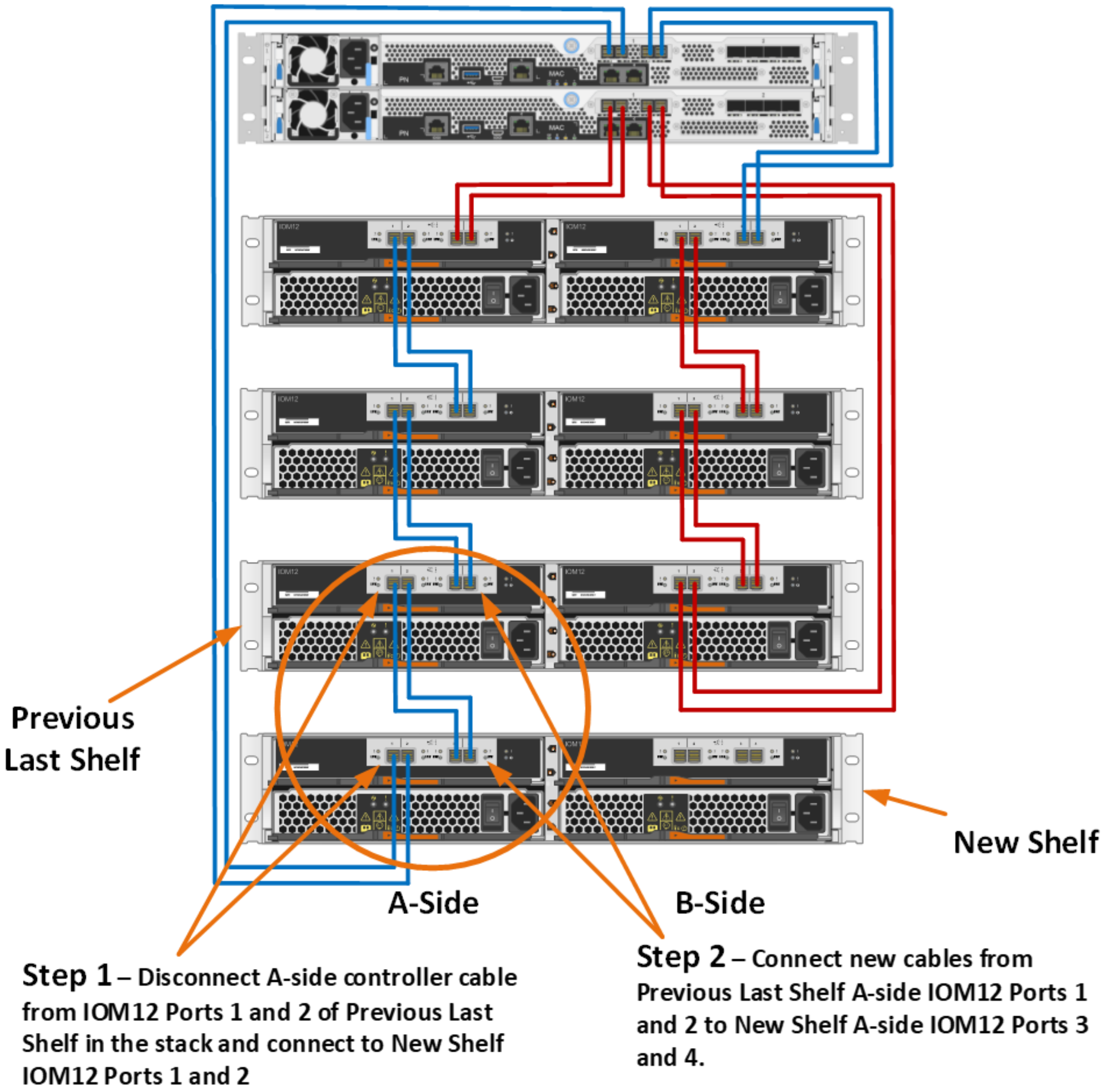
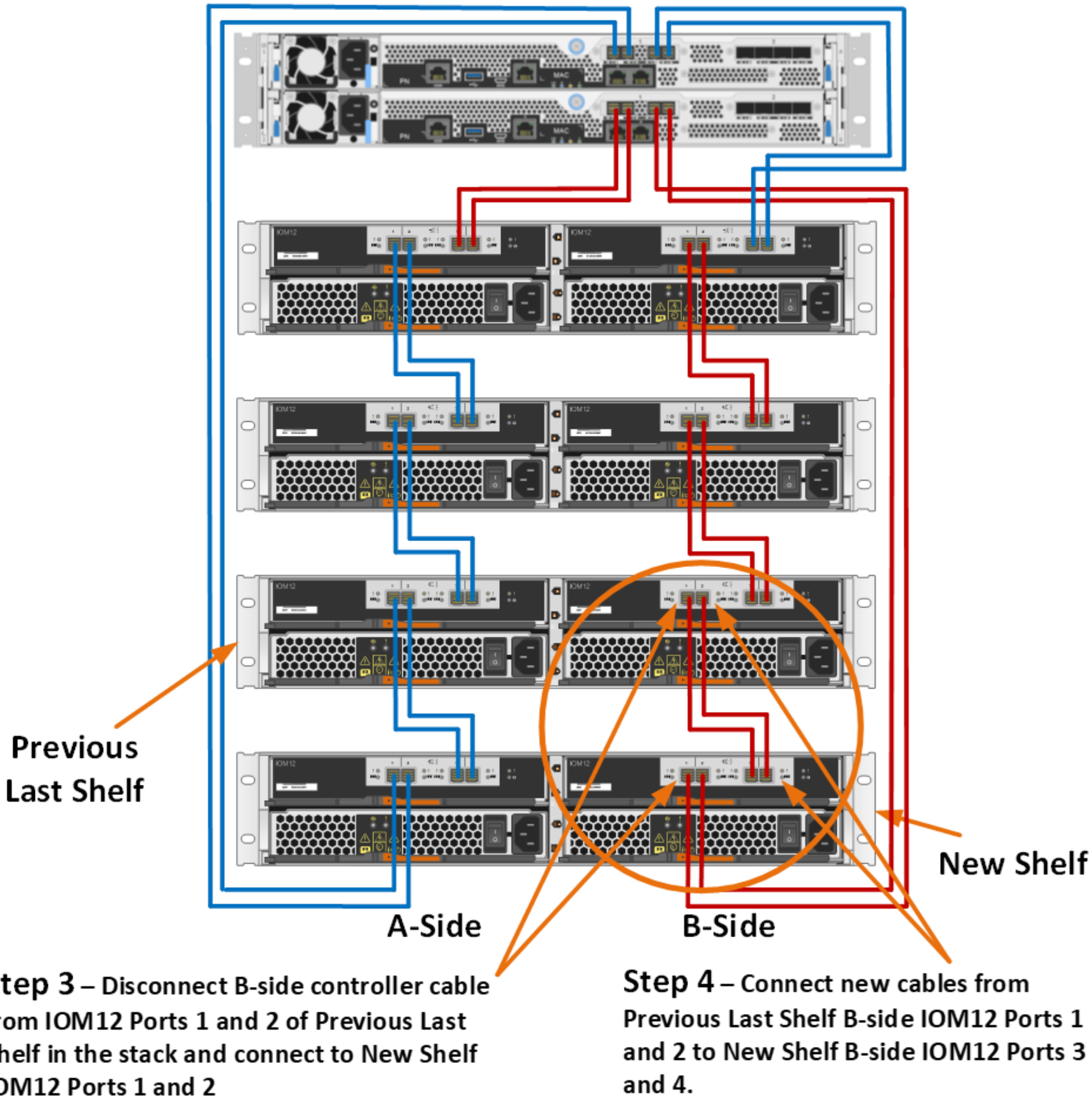

Previous
Last Shelf
New Shelf
A-Side
B-Side
Step 1 – Disconnect A-side controller cable from IOM12 Ports 1 and 2 of Previous Last Shelf in the stack and connect to New Shelf IOM12 Ports 1 and 2
Step 2 – Connect new cables from Previous Last Shelf A-side IOM12 Ports 1 and 2 to New Shelf A-side IOM12 Ports 3 and 4.

Figure 57) Drive shelf hot-add B-side cabling.


Previous
Last Shelf
New Shelf
A-Side
B-Side
Step 3 – Disconnect B-side controller cable from IOM12 Ports 1 and 2 of Previous Last Shelf in the stack and connect to New Shelf IOM12 Ports 1 and 2
Step 4 – Connect new cables from Previous Last Shelf B-side IOM12 Ports 1 and 2 to New Shelf B-side IOM12 Ports 3 and 4.

Best practice

Plan carefully for any drive shelf hot-add activity on production storage systems. Verify that the following conditions are met:

- The existing power infrastructure can support the additional hardware.
- The cabling plan for the new shelf does not simultaneously interrupt the SAS expansion paths for controller A and controller B.
- The new expansion port 1 path is confirmed to be valid, and the new shelf is visible in the SANtricity management software before the expansion path 2 is disconnected and moved to the new shelf.

Best practice

Note: Failure to preserve one active path to existing drive shelves during the procedure could potentially result in degradation/failure of LUNs during I/O activity.

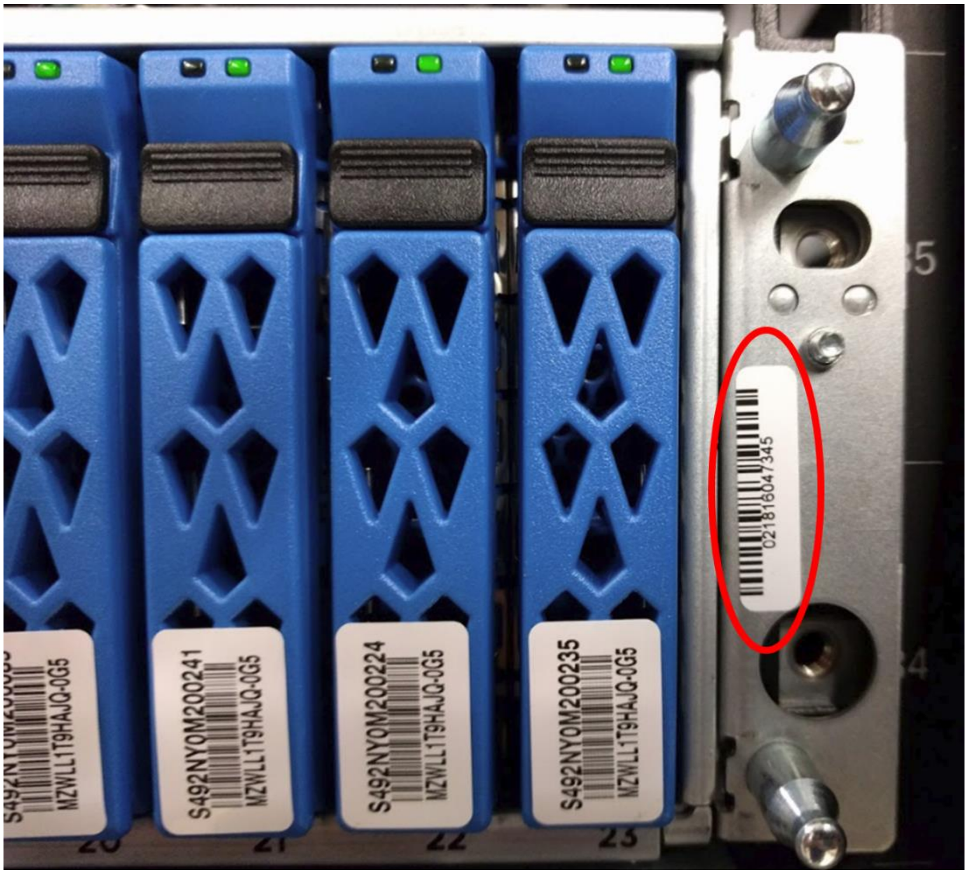
E-Series product support

NetApp E-Series storage systems are identified by the chassis serial number (SN) of the E-Series system shelf, not the SNs of the individual controllers in the system shelf. You must register the E-Series system shelf SN, because only that SN can be used to log a support case with NetApp.

Controller shelf serial number

NetApp EF600 storage systems are shipped preconfigured from the factory (controllers have HICs and batteries installed, and controllers are installed in the controller shelf). The chassis serial number is printed on a white label that is affixed to the controller shelf behind the right end cap on the front of the chassis. The SN is circled in red on Figure 58.

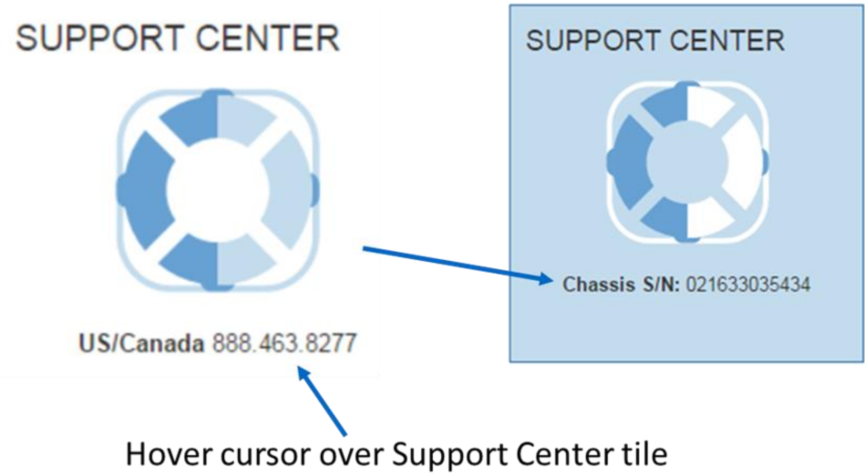
Figure 58) Controller shelf SN.



The SN is also included on the shelf UL sticker. However, this sticker is often not visible after the shelves are installed in a rack.

On a running storage system, you can also find the chassis serial number through NetApp SANtricity System Manager by selecting the Support tab and positioning your cursor over the Support Center tile, as shown in Figure 59.

Figure 59) SANtricity System Manager Support Center tile showing chassis serial number.


SUPPORT CENTER
US/Canada 888.463.8277
SUPPORT CENTER
Chassis S/N: 021633035434
Hover cursor over Support Center tile

License keys

E-Series storage arrays use two types of license keys. One type of key file is for premium features, and the other type of key file is used to change the storage system feature pack (which changes the host interface protocol).

For the EF600 system, there are currently no premium features. All features are enabled out of the box.

Note: The encryption feature is disabled for systems sold in export-limited countries.

The feature pack keys are used to change the protocol on IB HICs between NVMe/IB and NVMe/RoCE and between FC and NVMe/FC on FC HICs. The process to generate a new feature pack key for your storage array is almost the same as the process to generate a premium feature key. The difference is that the 11-digit key activation code for each package is available at no additional cost and is listed in the hardware upgrade instructions per controller type, available on the E-Series and SANtricity 11 Resources page.

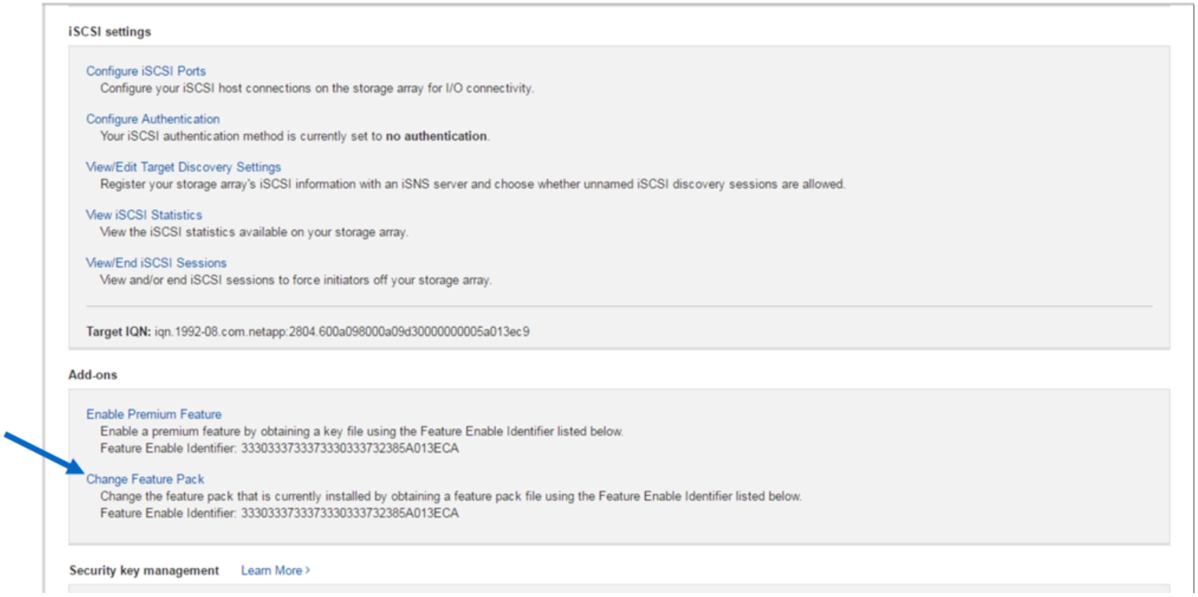
The following information is required to generate a feature pack key file:

- 11-digit key activation code
- Array serial number shown in System Manager by selecting Support, then Support Center

Select the feature enable identifier shown in System Manager by selecting Settings > System, then reference the identifier in the Add-Ons section.

After the feature pack file is downloaded to the host server, click Change Feature Pack, as shown in Figure 60. Follow the prompts, beginning with browsing to the feature pack file, as shown in Figure 61.

Figure 60) Changing the feature pack from Settings > System view.



iSCSI settings

Configure iSCSI Ports
Configure your iSCSI host connections on the storage array for I/O connectivity.

Configure Authentication
Your iSCSI authentication method is currently set to **no authentication**.

View/Edit Target Discovery Settings
Register your storage array's iSCSI information with an iSNS server and choose whether unnamed iSCSI discovery sessions are allowed.

View iSCSI Statistics
View the iSCSI statistics available on your storage array.

View/End iSCSI Sessions
View and/or end iSCSI sessions to force initiators off your storage array.

Target IQN: iqn.1992-08.com.netapp:2804.600a098000a09d30000000005a013ec9

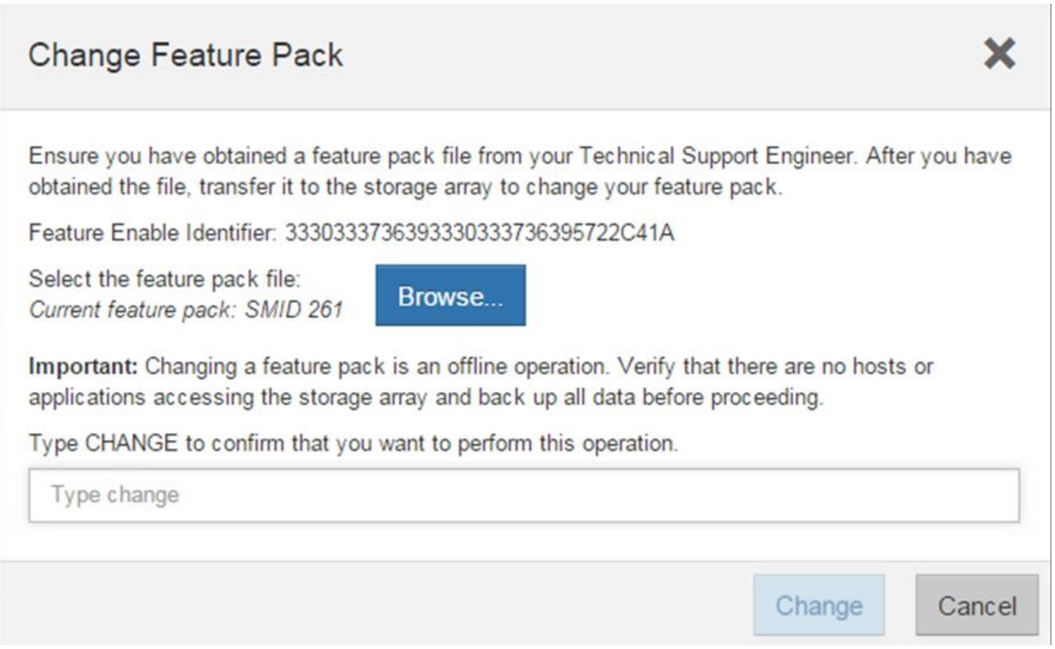
Add-ons

Enable Premium Feature
Enable a premium feature by obtaining a key file using the Feature Enable Identifier listed below.
Feature Enable Identifier: 333033373337333033373238 5A013ECA

Change Feature Pack
Change the feature pack that is currently installed by obtaining a feature pack file using the Feature Enable Identifier listed below.
Feature Enable Identifier: 333033373337333033373238 5A013ECA

Security key management Learn More ›

Figure 61) Change Feature Pack option.



Change Feature Pack ✕

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: 333033373639333033373639 5722C41A

Select the feature pack file:
Current feature pack: SMID 261 Browse...

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.

Type change

Change Cancel

Note: Changing the feature pack causes the storage array to reboot. The new protocol will be active after the system is back online.

For issues with accessing license key files, open a support ticket with NetApp Support by using the serial number of the registered controller shelf for the associated storage system. This process requires a NetApp Support login.

Conclusion

NetApp EF600 with SAS expansion shelves supporting NL-SAS HDD drives and SAS SSD drives broadens the abilities of the array to manage more use cases. The additional capacity enables the EF600 array to store an application backup or provide a cold tier for an application such as Splunk.

NetApp EF600 storage systems provide extreme throughput performance with fast host interfaces and can offer up to 367TB of raw NVMe SSD capacity to support fast, large-capacity applications. It is also capable of delivering sub-150µsec response times for critical path transactional environments that require consistently low latency. For high-random IOPS environments, the EF600 supports up to two million 4KB read IOPS. For high-bandwidth workloads, the EF600 supports approximately 12.5GBps cache-mirrored sequential writes and up to 44GBps sequential reads.

With its extreme versatility—including multiple host interface choices, multiple RAID choices, and a range of entry-level-capacity to enterprise-capacity drive choices—the EF600 is a modern, ready-to-work, NVMe all-flash storage system. The addition of NVMe/IB, NVMe/RoCE, and NVMe/FC makes the EF600 a truly new-generation NVMe all-flash array. The EF600 system delivers industry-leading price/performance, excellent interface and configuration flexibility, and the extended RAS value that enterprise customers can trust with their highest-value workloads.

Appendix A: Understanding SSD endurance and overprovisioning

This appendix describes how to increase SSD endurance and maximize steady-state write performance for write-intensive workloads by configuring volume groups and DDPs to have free capacity. The topics of endurance, overprovisioning, write amplification factor, and workload conditioning will be explored to provide a basis for understanding how leaving free capacity effectively increases the level of overprovisioning in the drives in each group or pool. Increasing overprovisioning can be expected to increase both SSD endurance and maximum sustained write performance, especially for lower-capacity drives.

SSD endurance

SSD endurance is typically specified in terms of drive writes per day (DWPD), which is just a convenient way to specify an amount of data. The NVMe SSDs used in the EF600 are rated for 1 DWPD. That means that you could nominally write an amount of data equal to the capacity of each SSD once per day without exceeding its rated endurance during the warranty period. Because endurance is a measure of the amount of data that can be written, the rated endurance for a 3.84TB SSD expressed as terabytes written is twice that of a 1.92TB SSD because it has twice the capacity. Similarly, the endurance for a 15.3TB SSD is twice that of a 7.68TB SSD.

There is an endurance limit specified for SSDs because solid-state memory can wear out. The NAND flash memory in an SSD is repeatedly programmed and erased over time as data is written to the drive. NAND flash memory can only be programmed and erased a limited number of times before wearing out, which means that there is an upper limit on how much data can be written to each SSD during its lifetime.

The smallest amount of data that can be written from the perspective of the array (and from the attached hosts) is one logical block, which is 4096 bytes for the NVMe drives used in an EF600. Inside the SSD, the smallest amount of data that can be written is a NAND flash memory page, which may be larger than a logical block. The smallest amount of data that can be erased is a NAND block, which can contain hundreds of pages. After a page is written, it cannot be overwritten until the entire NAND block is erased. The exact page and NAND block sizes vary between SSD models. In general, the NAND block size increases as NAND flash memory density and capacity increases.

Overprovisioning

All SSDs have more internal solid-state storage than the amount specified as the usable capacity. The extra capacity is referred to as overprovisioning (OP). The rated endurance is directly related to the amount of overprovisioning, which is expressed as the percentage increase of the usable capacity. OP values of 7%, 28%, and 100% typically correspond to rated endurances of 1 DWPD, 3 DWPD, and 10 DWPD, respectively. The exact amount of OP required for the rated endurance is an implementation detail, however, and can vary between vendors or between generations of drives.

So, the amount of solid-state storage in a drive that has a stated usable capacity of Ux with 7% OP has internal storage in the amount of R = Ux + 0.07*Ux or R = 1.07*Ux. If the same drive of raw capacity R were instead configured for an OP of 28%, the usable capacity would be Uy = (1.07*Ux)/1.28. If the drive were configured for an OP of 100%, the usable capacity would be Uz = (1.07*Ux)/2.

As an example, a drive with a stated usable capacity of 3.84TB when configured for 7% OP to support an endurance of 1 DWPD would have a usable capacity of 3.2TB when configured for an OP of 28% to support an endurance of 3 DWPD. If it were configured with an OP of 100% to support 10 DWPD, it would have a usable capacity of 2.1TB.

As the capacity of SSDs has increased, the amount of raw capacity needed to configure a given amount of OP has also increased because OP is specified as the percent of additional memory needed to support a given endurance. For example, an 800GB SSD rated for 3 DWPD needs a raw capacity of approximately 1024GB, or 224GB more than the usable capacity. By comparison, a 3.84TB SSD configured for an endurance of 3 DWPD would require approximately 1.1TB of additional capacity as opposed to only about 270GB of additional capacity to support an endurance of 1 DWPD. The difference in raw capacity required is over 800GB, which is not directly visible to the end user and increases the cost of the drive as a percentage of usable capacity.

Write amplification factor

SSD endurance is specified as an amount of data that can be written to each drive during its lifetime. It is not really that simple, however, because the endurance rating is based on a random write workload assuming a certain write amplification factor (WAF). Recall that the data can be written to the NAND flash memory with page granularity, but can only be erased as a NAND block, which may contain hundreds of pages. To ensure even wear on all NAND blocks, the SSD performs both garbage collection and wear leveling in the background.

- Garbage collection happens when the contents of a logical block are overwritten with new data. The SSD writes the data to a page that is currently erased. The old data for that logical block are no longer needed and can be discarded. After a large enough percentage of pages in a block no longer contains valid data, the SSD copies pages with valid data into erased pages in another NAND block so that it can erase the entire NAND block.
- Wear leveling happens when a NAND block contains data that is never overwritten, the SSD periodically copy the data to another block so that all blocks can be used (in other words, programmed and erased) evenly throughout the life of the drive.

All of this means that the amount of data written to the NAND flash memory exceeds the amount of data written to the SSD by the array (which is the host, as viewed by the SSD). The ratio of NAND writes to host writes is referred to as the write amplification factor or WAF.

Note: In general, increasing the OP lowers the WAF, especially for random write workloads. Lowering the WAF in turn increases endurance and can also increase steady-state performance for write-intensive workloads.

Steady-state performance

The maximum achievable write performance for an SSD eventually reaches a steady-state level. For most workloads, the maximum obtainable write performance can be expected to decrease from the peak values that can be obtained when the drive is mostly erased. As the host continues to write data to the drive, the SSD must perform garbage collection in the background to free space as logical blocks are overwritten. Over time, the drive must also perform background wear leveling. The maximum obtainable write performance starts to decrease as data is written to the drive but can be expected to stabilize to a steady-state value for a given workload. When the maximum obtainable performance stabilizes, the drive is said to be conditioned for that workload.

The amount of data that must be written before the maximum write performance stabilizes varies with the workload and the amount of overprovisioning. As a rule, maximum write performance can be expected to stabilize after an amount of data two to three times the capacity of the drive has been written to the drive. There is a correlation between maximum steady state write performance and overprovisioning. As a rule, maximum write performance increases with higher levels of overprovisioning.

Note: Write performance for a given workload does not necessarily drop after the SSD has been conditioned to that workload if the write rate is at or lower than the maximum steady state write performance.

Reserving free capacity

When creating volume groups and DDPs, consider leaving some free capacity in the group or pool rather than allocating all available capacity to volumes. The EF600 automatically unmaps free capacity. Therefore, free capacity effectively increases the OP level for the constituent drives in that group or pool, which can result in lower WAF for both random write and multi-stream sequential write workloads. Lowering the WAF for a given workload inherently increases endurance and can improve steady-state performance for write-intensive workloads, especially for lower capacity drives. With lower capacity drives, the maximum steady-state write performance is expected to be less than half that of the system throughput capability if there is no free space in the group or pool.

The maximum steady-state IOPS and bandwidth capability for each individual SSD in a group or pool increases as free capacity is increased in the group or pool. Equally important, increasing free capacity decreases the WAF for most workloads, increasing SSD endurance. The decrease in WAF should occur for most workloads even if the performance requirements of the workload are significantly lower than the maximum steady-state values.

Table 24 shows the effective OP for various amounts of free capacity held back as a percentage of the usable capacity of the drive. The usable capacity in a volume group varies considerably with the RAID level and group size, so the free capacity reserved in the volume group should be based on the total capacity of the drive. A holdback of 16.4% equates to an effective OP of 28%, which is the OP level nominally used to configure drives for 3 DWPD endurance.

Table 24) Per-drive capacity holdback (in GiB) required to reach effective OP.

% Holdback	Effective OP	1.92TB SSD	3.84TB SSD	7.68TB SSD	15.3TB SSD
0	7.0%	0	0	0	0
4	11.5%	71.54	143.08	286.16	572.32
8	16.3%	143.08	286.16	572.32	1144.63
12	21.6%	214.62	429.24	858.47	1716.95
16.4	28.0%	293.31	586.63	1173.25	2346.50
20	33.8%	357.70	715.40	1430.79	2861.58
24	40.8%	429.24	858.48	1716.95	3433.90
28	48.6%	500.78	1001.56	2003.11	4006.21

Where to find additional information

To learn more about the information that is described in this document, review the following documents and websites:

- E-Series EF600 datasheet
  https://www.netapp.com/us/media/ds-4002.pdf
- E-Series and SANtricity 11 Documentation Center
  https://docs.netapp.com/ess-11/index.jsp
- E-Series and SANtricity 11 Resource page
  https://mysupport.netapp.com/info/web/ECMP1658252.html
- NetApp Product Documentation
  https://www.netapp.com/us/documentation/index.aspx

Version history

Version	Date	Document version history
Version 1.0	September 2019	Initial release of EF600 array and SANtricity 11.60
Version 1.1	July 2020	Updated for SANtricity 11.60.2 release
Version 1.2	November 2020	Updated for SANtricity 11.70 release
Version 1.3	July 2021	Updated for SANtricity 11.70.1 release
Version 1.4	May 2022	Updated for addition of SAS expansion shelves, resource-provisioned volumes, and SANtricity 11.70.3.
Version 1.5	October 2022	Updated for IOM LED definitions and IOM12B
Version 2.0	July 2023	Updated for SANtricity 11.80.0 release.
Version 2.1	November 2024	Updated for SANtricity 11.90.0 release.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

TR-4800-1124

NetApp