FAQs

E-Series Systems

NetApp
December 30, 2022

Table of Contents

FAQs

What settings are imported?

The Import Settings feature is a batch operation that loads configurations from one storage array to multiple storage arrays.

The settings that are imported during this operation depend on how the source storage array is configured in System Manager. The following settings can be imported to multiple storage arrays:

- **Email alerts** — Settings include a mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — Settings include a syslog server address and a UDP port.
- **SNMP alerts** — Settings include a community name and IP address for the SNMP server.
- **AutoSupport** — Settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.
- **Directory services** — Configuration includes the domain name and URL of an LDAP (Lightweight Directory Access Protocol) server, along with the mappings for the LDAP server's user groups to the storage array's predefined roles.
- **Storage configuration** — Configurations include volumes (only thick and only non-repository volumes), volume groups, pools, and hot spare drive assignments.
- **System settings** — Configurations include media scan settings for a volume, SSD cache for controllers, and automatic load balancing (does not include host connectivity reporting).

Why do I not see all of my storage arrays?

During the Import Settings operation, some of your storage arrays might not be available in the target selection dialog box.

Storage arrays might not appear for the following reasons:

- The firmware version is below 8.50.
- The storage array is offline.
- The system cannot communicate with that array (for example, the array has certificate, password, or networking problems).

Why are these volumes not associated with a workload?

Volumes are not associated with a workload if they have been created using the command line interface (CLI) or if they have been migrated (imported/exported) from a different storage array.

How does my selected workload impact volume creation?

During volume creation, you are prompted for information about a workload's use. The system uses this information to create an optimal volume configuration for you, which can

be edited as needed. Optionally, you can skip this step in the volume creation sequence.

A workload is a storage object that supports an application. You can define one or more workloads, or instances, per application. For some applications, the system configures the workload to contain volumes with similar underlying volume characteristics. These volume characteristics are optimized based on the type of application the workload supports. For example, if you create a workload that supports a Microsoft SQL Server application and then subsequently create volumes for that workload, the underlying volume characteristics are optimized to support Microsoft SQL Server.

- **Application-specific** — When you are creating volumes using an application-specific workload, the system may recommend an optimized volume configuration to minimize contention between application workload I/O and other traffic from your application instance. Volume characteristics like I/O type, segment size, controller ownership, and read and write cache are automatically recommended and optimized for workloads that are created for the following application types.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Video surveillance applications
  - VMware ESXi (for volumes to be used with Virtual Machine File System)

    You can review the recommended volume configuration and edit, add, or delete the system-recommended volumes and characteristics using the Add/Edit Volumes dialog box.
- **Other (or applications without specific volume creation support)** — Other workloads use a volume configuration that you must manually specify when you want to create a workload that is not associated with a specific application, or if there is no built-in optimization for the application you intend to use on the storage array. You must manually specify the volume configuration using the Add/Edit Volumes dialog box.

Why do I not see all my volumes, hosts, or host clusters?

Snapshot volumes with a DA-enabled base volume are not eligible to be assigned to a host that is not Data Assurance (DA) capable. You must disable DA on the base volume before a snapshot volume can be assigned to a host that is not DA capable.

Consider the following guidelines for the host to which you are assigning the snapshot volume:

- A host is not DA capable if it is connected to the storage array through an I/O interface that is not DA capable.
- A host cluster is not DA capable if it has at least one host member that is not DA capable.

> You cannot disable DA on a volume that is associated with snapshots (consistency groups, snapshot groups, snapshot images, and snapshot volumes), volume copies, and mirrors. All associated reserved capacity and snapshot objects must be deleted before DA can be disabled on the base volume.

Why can I not delete the selected workload?

This workload consists of a group of volumes that were created using the command line interface (CLI) or migrated (imported/exported) from a different storage array. As a result, the volumes in this workload are not associated with an application-specific workload, so

the workload cannot be deleted.

How do application-specific workloads help me manage my storage array?

The volume characteristics of your application-specific workload dictate how the workload interacts with the components of your storage array and helps determine the performance of your environment under a given configuration.

An application is software such as SQL Server or Exchange. You define one or more workloads to support each application. For some applications, the system automatically recommends a volume configuration that optimizes storage. Characteristics such as I/O type, segment size, controller ownership, and read and write cache are included in the volume configuration.

What do I need to do to recognize the expanded capacity?

If you increase the capacity for a volume, the host might not immediately recognize the increase in volume capacity.

Most operating systems recognize the expanded volume capacity and automatically expand after the volume expansion is initiated. However, some might not. If your OS does not automatically recognize the expanded volume capacity, you might need to perform a disk rescan or reboot.

After you have expanded the volume capacity, you must manually increase the file system size to match. How you do this depends on the file system you are using.

Refer to your host operating system documentation for additional details.

When would I want to use the assign host later selection?

If you want to speed the process for creating volumes, you can skip the host assignment step so that newly created volumes are initialized offline.

Newly created volumes must be initialized. The system can initialize them using one of two modes – either an Immediate Available Format (IAF) background initialization process or an offline process.

When you map a volume to a host, it forces any initializing volumes in that group to transition to background initialization. This background initialization process allows for concurrent host I/O, which can sometimes be time-consuming.

When none of the volumes in a volume group are mapped, offline initialization is performed. The offline process is much faster than the background process.

What do I need to know about host block size requirements?

For EF300 and EF600 systems, a volume can be set to support a 512-byte or a 4KiB block size (also called "sector size"). You must set the correct value during volume creation. If possible, the system suggests the appropriate default value.

Before setting the volume block size, read the following limitations and guidelines.

- Some operating systems and virtual machines (notably VMware, at this time) require a 512-byte block size and do not support 4KiB, so make sure you know the host requirements before creating a volume. Typically, you can achieve the best performance by setting a volume to present a 4KiB block size; however, ensure that your host allows for 4KiB (or “4Kn”) blocks.
- The type of drives you select for your pool or volume group also determines what volume block sizes are supported, as follows:
  - If you create a volume group using drives that write to 512-byte blocks, then you can only create volumes with 512-byte blocks.
  - If you create a volume group using drives that write to 4KiB blocks, then you can create volumes with either 512-byte or 4KiB blocks.
- If the array has an iSCSI host interface card, all volumes are limited to 512-byte blocks (regardless of volume group block size). This is due to a specific hardware implementation.
- You cannot change a block size once it is set. If you need to change a block size, you must delete the volume and re-create it.

Why would I need to create a host cluster?

You need to create a host cluster if you want to have two or more hosts share access to the same set of volumes. Normally, the individual hosts have clustering software installed on them to coordinate volume access.

How do I know which host operating system type is correct?

The Host Operating System Type field contains the operating system of the host. You can select the recommended host type from the drop-down list or allow the Host Context Agent (HCA) to configure the host and appropriate host operating system type.

The host types that appear in the drop-down list depend on the storage array model and the firmware version. The most recent versions display the most common options first, which are the most likely to be appropriate. Appearance on this list does not imply the option is fully supported.

For more information about host support, refer to the NetApp Interoperability Matrix Tool.

Some of the following host types might appear in the list:

Host Operating System type	Operating System (OS) and multipath driver
Linux DM-MP (Kernel 3.10 or later)	Supports Linux operating systems using a Device Mapper multipath failover solution with a 3.10 or later Kernel.
VMware ESXi	Supports VMware ESXi operating systems running the Native Multipathing Plug-in (NMP) architecture using the VMware built-in Storage Array Type Policy module SATP_ALUA.

Host Operating System type	Operating System (OS) and multipath driver
Windows (clustered or non-clustered)	Supports Windows clustered or non-clustered configurations that are not running the ATTO multipathing driver.
ATTO Cluster (all operating systems)	Supports all cluster configurations using the ATTO Technology, Inc., multipathing driver.
Linux (Veritas DMP)	Supports Linux operating systems using a Veritas DMP multipathing solution.
Linux (ATTO)	Supports Linux operating systems using an ATTO Technology, Inc., multipathing driver.
Mac OS	Supports Mac OS versions using an ATTO Technology, Inc., multipathing driver.
Windows (ATTO)	Supports Windows operating systems using an ATTO Technology, Inc., multipathing driver.
FlexArray (ALUA)	Supports a NetApp FlexArray system using ALUA for multipathing.
IBM SVC	Supports an IBM SAN Volume Controller configuration.
Factory Default	Reserved for the initial start-up of the storage array. If your host operating system type is set to Factory Default, change it to match the host operating system and multipath driver running on the connected host.
Linux DM-MP (Kernal 3.9 or earlier)	Supports Linux operating systems using a Device Mapper multipath failover solution with a 3.9 or earlier Kernel.
Window Clustered (deprecated)	If your host operating system type is set to this value, use the Windows (clustered or non-clustered) setting instead.

After the HCA is installed and the storage is attached to the host, the HCA sends the host topology to the storage controllers through the I/O path. Based on the host topology, the storage controllers automatically define the host and the associated host ports, and then set the host type.

If the HCA does not select the recommended host type, you must manually set the host type.

How do I match the host ports to a host?

If you are manually creating a host, you first must use the appropriate host bus adapter (HBA) utility available on the host to determine the host port identifiers associated with each HBA installed in the host.

When you have this information, select the host port identifiers that have logged into the storage array from the list provided in the Create Host dialog.

Make sure you select the appropriate host port identifiers for the host you are creating. If you associate the wrong host port identifiers, you might cause unintended access from another host to this data.

If you are automatically creating hosts using the host context agent (HCA) installed on each host, the HCA should automatically associate the host port identifiers with each host and configure them appropriately.

What is the default cluster?

The default cluster is a system-defined entity that allows any unassociated host port identifier that has logged into the storage array to gain access to volumes assigned to the default cluster.

An unassociated host port identifier is a host port that is not logically associated with a particular host but is physically installed in a host and logged into the storage array.

If you want hosts to have specific access to certain volumes in the storage array, you must not use the default cluster. Instead, you must associate the host port identifiers with their corresponding hosts. This task can be done either manually during the Create Host operation or automatically using the host context agent (HCA) installed on each host. Then, you assign volumes either to an individual host or to a host cluster.

You should only use the default cluster in special situations where your external storage environment is conducive to allowing all the hosts and all the logged-in host port identifiers connected to the storage array have access to all of the volumes (all-access mode) without specifically making the hosts known to the storage array or the user interface.

Initially, you can assign volumes only to the default cluster through the command line interface (CLI). However, after you assign at least one volume to the default cluster, this entity (called Default Cluster) is displayed in the user interface where you can then manage this entity.

What is redundancy check?

A redundancy check determines whether the data on a volume in a pool or volume group is consistent. Redundancy data is used to quickly reconstruct information on a replacement drive if one of the drives in the pool or volume group fails.

You can perform this check only on one pool or volume group at a time. A volume redundancy check performs the following actions:

- Scans the data blocks in a RAID 3 volume, a RAID 5 volume, or a RAID 6 volume, and then checks the redundancy information for each block. (RAID 3 can only be assigned to volume groups using the command line interface.)
- Compares the data blocks on RAID 1 mirrored drives.
- Returns redundancy errors if the data is determined to be inconsistent by the controller firmware.

Immediately running a redundancy check on the same pool or volume group might cause an error. To avoid this problem, wait one to two minutes before running another redundancy check on the same pool or volume group.

What is preservation capacity?

Preservation capacity is the amount of capacity (number of drives) that is reserved in a pool to support potential drive failures.

When a pool is created, the system automatically reserves a default amount of preservation capacity depending on the number of drives in the pool.

Pools use preservation capacity during reconstruction, whereas volume groups use hot spare drives for the same purpose. The preservation capacity method is an improvement over hot spare drives because it allows reconstruction to happen faster. Preservation capacity is spread over a number of drives in the pool instead of on one drive in the case of a hot spare drive, so you are not limited by the speed or availability of one drive.

What RAID level is best for my application?

To maximize the performance of a volume group, you must select the appropriate RAID level.

You can determine the appropriate RAID level by knowing the read and write percentages for the applications that are accessing the volume group. Use the Performance page to obtain these percentages.

RAID levels and application performance

RAID relies on a series of configurations, called levels, to determine how user and redundancy data is written and retrieved from the drives. Each RAID level provides different performance features. Applications with a high read percentage will perform well using RAID 5 volumes or RAID 6 volumes because of the outstanding read performance of the RAID 5 and RAID 6 configurations.

Applications with a low read percentage (write-intensive) do not perform as well on RAID 5 volumes or RAID 6 volumes. The degraded performance is the result of the way that a controller writes data and redundancy data to the drives in a RAID 5 volume group or a RAID 6 volume group.

Select a RAID level based on the following information.

RAID 0

Description:

- Non-redundant, striping mode.
- RAID 0 stripes data across all of the drives in the volume group.

Data protection features:

- RAID 0 is not recommended for high availability needs. RAID 0 is better for non-critical data.
- If a single drive fails in the volume group, all of the associated volumes fail, and all data is lost.

Drive number requirements:

- A minimum of one drive is required for RAID Level 0.
- RAID 0 volume groups can have more than 30 drives.
- You can create a volume group that includes all of the drives in the storage array.

RAID 1 or RAID 10

Description:

- Striping/mirror mode.

How it works:

- RAID 1 uses disk mirroring to write data to two duplicate disks simultaneously.
- RAID 10 uses drive striping to stripe data across a set of mirrored drive pairs.

Data protection features:

- RAID 1 and RAID 10 offer high performance and the best data availability.
- RAID 1 and RAID 10 use drive mirroring to make an exact copy from one drive to another drive.
- If one of the drives in a drive pair fails, the storage array can instantly switch to the other drive without any loss of data or service.
- A single drive failure causes associated volumes to become degraded. The mirror drive allows access to the data.
- A drive-pair failure in a volume group causes all of the associated volumes to fail, and data loss could occur.

Drive number requirements:

- A minimum of two drives is required for RAID 1: one drive for the user data, and one drive for the mirrored data.
- If you select four or more drives, RAID 10 is automatically configured across the volume group: two drives for user data, and two drives for the mirrored data.
- You must have an even number of drives in the volume group. If you do not have an even number of drives and you have some remaining unassigned drives, go to **Pools & Volume Groups** to add additional drives to the volume group, and retry the operation.
- RAID 1 and RAID 10 volume groups can have more than 30 drives. A volume group can be created that includes all of the drives in the storage array.

RAID 5

Description:

- High I/O mode.

How it works:

- User data and redundant information (parity) are striped across the drives.
- The equivalent capacity of one drive is used for redundant information.

Data protection features

- If a single drive fails in a RAID 5 volume group, all of the associated volumes become degraded. The redundant information allows the data to still be accessed.
- If two or more drives fail in a RAID 5 volume group, all of the associated volumes fail, and all data is lost.

Drive number requirements:

- You must have a minimum of three drives in the volume group.
- Typically, you are limited to a maximum of 30 drives in the volume group.

RAID 6

Description:

- High I/O mode.

How it works:

- User data and redundant information (dual parity) are striped across the drives.
- The equivalent capacity of two drives is used for redundant information.

Data protection features:

- If one or two drives fail in a RAID 6 volume group, all of the associated volumes become degraded, but the redundant information allows the data to still be accessed.
- If three or more drives fail in a RAID 6 volume group, all of the associated volumes fail, and all data is lost.

Drive number requirements:

- You must have a minimum of five drives in the volume group.
- Typically, you are limited to a maximum of 30 drives in the volume group.

You cannot change the RAID level of a pool. The user interface automatically configures pools as RAID 6.

RAID levels and data protection

RAID 1, RAID 5, and RAID 6 write redundancy data to the drive media for fault tolerance. The redundancy data might be a copy of the data (mirrored) or an error-correcting code derived from the data. You can use the redundancy data to quickly reconstruct information on a replacement drive if a drive fails.

You configure a single RAID level across a single volume group. All redundancy data for that volume group is stored within the volume group. The capacity of the volume group is the aggregate capacity of the member drives minus the capacity reserved for redundancy data. The amount of capacity needed for redundancy depends on the RAID level used.

Why are some drives not showing up?

In the Add Capacity dialog, not all drives are available for adding capacity to an existing pool or volume group.

Drives are not eligible for any of the following reasons:

- A drive must be unassigned and not secure-enabled. Drives already part of another pool, another volume group, or configured as a hot spare are not eligible. If a drive is unassigned but is secure-enabled, you must manually erase that drive for it to become eligible.

- A drive that is in a non-optimal state is not eligible.
- If the capacity of a drive is too small, it is not eligible.
- The drive media type must match within a pool or volume group. You cannot mix the following:
  - Hard Disk Drives (HDDs) with Solid State Disks (SSDs)
  - NVMe with SAS drives
  - Drives with 512-byte and 4KiB volume block sizes
- If a pool or volume group contains all secure-capable drives, non-secure-capable drives are not listed.
- If a pool or volume group contains all Federal Information Processing Standards (FIPS) drives, non-FIPS drives are not listed.
- If a pool or volume group contains all Data Assurance (DA)-capable drives and there is at least one DA-enabled volume in the pool or volume group, a drive that is not DA capable is not eligible, so it cannot be added to that pool or volume group. However, if there is no DA- enabled volume in the pool or volume group, a drive that is not DA capable can be added to that pool or volume group. If you decide to mix these drives, keep in mind that you cannot create any DA-enabled volumes.

Capacity can be increased in your storage array by adding new drives or by deleting pools or volume groups.

Why can I not increase my preservation capacity?

If you have created volumes on all available usable capacity, you might not be able to increase preservation capacity.

Preservation capacity is the amount of capacity (number of drives) that is reserved on a pool to support potential drive failures. When a pool is created, the system automatically reserves a default amount of preservation capacity depending on the number of drives in the pool. If you have created volumes on all available usable capacity, you cannot increase preservation capacity without adding capacity to the pool by either adding drives or deleting volumes.

You can change the preservation capacity from Pools & Volume Groups. Select the pool that you want to edit. Click **View/Edit Settings**, and then select the **Settings** tab.

Preservation capacity is specified as a number of drives, even though the actual preservation capacity is distributed across the drives in the pool.

What is Data Assurance?

Data Assurance (DA) implements the T10 Protection Information (PI) standard, which increases data integrity by checking for and correcting errors that might occur as data is transferred along the I/O path.

The typical use of the Data Assurance feature will check the portion of the I/O path between the controllers and drives. DA capabilities are presented at the pool and volume group level.

When this feature is enabled, the storage array appends error-checking codes (also known as cyclic redundancy checks or CRCs) to each block of data in the volume. After a data block is moved, the storage array uses these CRC codes to determine if any errors occurred during transmission. Potentially corrupted

data is neither written to disk nor returned to the host. If you want to use the DA feature, select a pool or volume group that is DA capable when you create a new volume (look for **Yes** next to **DA** in the pool and volume group candidates table).

Make sure you assign these DA-enabled volumes to a host using an I/O interface that is capable of DA. I/O interfaces that are capable of DA include Fibre Channel, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE and iSER over InfiniBand (iSCSI Extensions for RDMA/ IB). DA is not supported by SRP over InfiniBand.

What is FDE/FIPS security?

FDE/FIPS security refers to secure-capable drives that encrypt data during writes and decrypt data during reads using a unique encryption key.

These secure-capable drives prevent unauthorized access to the data on a drive that is physically removed from the storage array. Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. FIPS drives have undergone certification testing.

> For volumes that require FIPS support, use only FIPS drives. Mixing FIPS and FDE drives in a volume group or pool will result in all drives being treated as FDE drives. Also, an FDE drive cannot be added to or used as a spare in an all-FIPS volume group or pool.

What is secure-capable (Drive Security)?

Drive Security is a feature that prevents unauthorized access to data on secure-enabled drives when removed from the storage array.

These drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

How do I view and interpret all SSD Cache statistics?

You can view nominal statistics and detailed statistics for SSD Cache.

Nominal statistics are a subset of the detailed statistics. The detailed statistics can be viewed only when you export all SSD statistics to a .csv file. As you review and interpret the statistics, keep in mind that some interpretations are derived by looking at a combination of statistics.

Nominal statistics

To view SSD Cache statistics, go to the **Manage** page. Select **Provisioning › Configure Pools & Volume Groups**. Select the SSD Cache that you want to view statistics for, and then select **More › View Statistics**. The nominal statistics are shown on the View SSD Cache Statistics dialog.

> This feature is not available on the EF600 or EF300 storage system.

The list includes nominal statistics, which are a subset of the detailed statistics.

Detailed statistics

The detailed statistics consist of the nominal statistics, plus additional statistics. These additional statistics are saved along with the nominal statistics, but unlike the nominal statistics, they do not display in the View SSD Cache Statistics dialog. You can view the detailed statistics only after exporting the statistics to a .csv file.

The detailed statistics are listed after the nominal statistics.

What is shelf loss protection and drawer loss protection?

Shelf loss protection and drawer loss protection are attributes of pools and volume groups that allow you to maintain data access in the event of a single shelf or drawer failure.

Shelf loss protection

A shelf is the enclosure that contains either the drives or the drives and the controller. Shelf loss protection guarantees accessibility to the data on the volumes in a pool or volume group if a total loss of communication occurs with a single drive shelf. An example of total loss of communication might be loss of power to the drive shelf or failure of both I/O modules (IOMs).

Shelf loss protection is not guaranteed if a drive has already failed in the pool or volume group. In this situation, losing access to a drive shelf and consequently another drive in the pool or volume group causes loss of data.

The criteria for shelf loss protection depends on the protection method, as described in the following table.

Level	Criteria for shelf loss protection	Minimum number of shelves required
Pool	The pool must include drives from at least five shelves and there must be an equal number of drives in each shelf. Shelf loss protection is not applicable to high-capacity shelves; if your system contains high-capacity shelves, refer to Drawer Loss Protection.	5
RAID 6	The volume group contains no more than two drives in a single drawer.	3
RAID 3 or RAID 5	Each drive in the volume group is located in a separate shelf.	3
RAID 1	Each drive in a RAID 1 pair must be located in a separate shelf.	2
RAID 0	Cannot achieve Shelf Loss Protection.	Not applicable

Drawer loss protection

A drawer is one of the compartments of a shelf that you pull out to access the drives. Only the high-capacity shelves have drawers. Drawer loss protection guarantees accessibility to the data on the volumes in a pool or volume group if a total loss of communication occurs with a single drawer. An example of total loss of communication might be loss of power to the drawer or failure of an internal component within the drawer.

> Drawer loss protection is not guaranteed if a drive has already failed in the pool or volume group. In this situation, losing access to a drawer (and consequently another drive in the pool or volume group) causes loss of data.

The criteria for drawer loss protection depends on the protection method, as described in the following table:

Level	Criteria for drawer loss protection	Minimum number of drawers required
Pool	Pool candidates must include drives from all drawers, and there must be an equal number of drives in each drawer. The pool must include drives from at least five drawers and there must be an equal number of drives in each drawer. A 60-drive shelf can achieve Drawer Loss Protection when the pool contains 15, 20, 25, 30, 35, 40, 45, 50, 55, or 60 drives. Increments in multiples of 5 can be added to the pool after initial creation.	5
RAID 6	The volume group contains no more than two drives in a single drawer.	3
RAID 3 or 5	Each drive in the volume group is located in a separate drawer	3
RAID 1	Each drive in a mirrored pair must be located in a separate drawer.	2
RAID 0	Cannot achieve Drawer Loss Protection.	Not applicable

How do I maintain shelf and drawer loss protection?

To maintain shelf and drawer loss protection for a pool or volume group, use the criteria specified in the following table.

Level	Criteria for shelf/drawer loss protection	Minimum number of shelves/ drawers required
Pool	For shelves, the pool must contain no more than two drives in a single shelf. For drawers, the pool must include an equal number of drives from each drawer.	6 for shelves 5 for drawers
RAID 6	The volume group contains no more than two drives in a single shelf or drawer.	3
RAID 3 or RAID 5	Each drive in the volume group is located in a separate shelf or drawer.	3
RAID 1	Each drive in a mirrored pair must be located in a separate shelf or drawer.	2
RAID 0	Cannot achieve shelf/drawer loss protection.	Not applicable

Shelf/drawer loss protection is not maintained if a drive has already failed in the pool or volume group. In this situation, losing access to a drive shelf or drawer, and consequently another drive in the pool or volume group, causes loss of data.

What is optimization capacity for pools?

SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated.

For drives associated with a pool, unallocated capacity is comprised of a pool's preservation capacity, the free capacity (capacity not used by volumes), and a portion of the usable capacity set aside as additional optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation.

When a pool is created, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. The Additional Optimization Capacity slider located in the Pool Settings dialog allows adjustments to the pool'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 Additional Optimization Capacity slider is only available for EF600 and EF300 storage systems.

What is optimization capacity for volume groups?

SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated.

For drives associated with a volume group, unallocated capacity is comprised of a volume group's free capacity (capacity not used by volumes), and a portion of the usable capacity set aside as optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation.

When a volume group is created, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. The Additional Optimization Capacity slider in the Volume Group Settings dialog 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.

Additional Optimization Capacity slider is only available for EF600 and EF300 storage systems.

What is resource provisioning capable?

Resource Provisioning is a feature available in the EF300 and EF600 storage arrays, which 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). 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. With a resource provisioned volume, there is no time-bound background initialization. Instead, each RAID stripe is initialized upon the first write to a volume block in the 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. 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.

What do I need to know about the resource-provisioned volumes feature?

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

The Resource Provisioning capability is not available at this time. In some views, components might be reported as resource-provisioning capable, but the ability to create resource-provisioned volumes has been disabled until it can be re-enabled in a future update.

Resource-provisioned volumes

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). 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. With a resource provisioned volume, there is no time-bound background initialization. Instead, each RAID stripe is initialized upon the first write to a volume block in the 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. 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.

Enabling and disabling the feature

Resource provisioning is enabled by default on systems where the drives support DULBE. You can disable that default setting from Pools & Volume Groups. Disabling resource provisioning is a permanent action for existing volumes and cannot be reversed (i.e., you cannot re-enable resource provisioning for these volume groups and pools).

However, if you want to re-enable resource provisioning again for any new volumes you create, you can do so from **Settings › System**. Be aware that when you re-enable resource provisioning, only newly created volume groups and pools are affected. Any existing volume groups and pools will remain unchanged. If desired, you can also disable resource provisioning again from **Settings › System**.

What is the difference between internal security key and external security key management?

When you implement the Drive Security feature, you can use an internal security key or an external security key to lock down data when a secure-enabled drive is removed from the storage array.

A security key is a string of characters, which is shared between the secure-enabled drives and controllers in a storage array. Internal keys are maintained on the controller's persistent memory. External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP).

What do I need to know before creating a security key?

A security key is shared by controllers and secure-enabled drives within a storage array. If a secure-enabled drive is removed from the storage array, the security key protects the data from unauthorized access.

You can create and manage security keys using one of the following methods:

- Internal key management on the controller's persistent memory.
- External key management on an external key management server.

Internal key management

Internal keys are maintained and "hidden" in a non-accessible location on the controller's persistent memory. Before creating an internal security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

You can then create an internal security key, which involves defining an identifier and a pass phrase. The identifier is a string that is associated with the security key, and is stored on the controller and on all drives associated with the key. The pass phrase is used to encrypt the security key for backup purposes. When you are finished, the security key is stored on the controller in a non-accessible location. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

External key management

External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP). Before creating an external security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature
3. Obtain a signed, client certificate file. A client certificate validates the storage array's controllers, so the key management server can trust their KMIP requests.
   a. First, you complete and download a client Certificate Signing Request (CSR). Go to **Settings › Certificates › Key Management › Complete CSR**.
   b. Next, you request a signed client certificate from a CA that is trusted by the key management server. (You can also create and download a client certificate from the key management server using the downloaded CSR file.)
   c. Once you have a client certificate file, copy that file to the host where you are accessing System Manager.
4. Retrieve a certificate file from the key management server, and then copy that file to the host where you are accessing System Manager. A key management server certificate validates the key management server, so the storage array can trust its IP address. You can use a root, intermediate, or server certificate for the key management server.

You can then create an external key, which involves defining the IP address of the key management server and the port number used for KMIP communications. During this process, you also load certificate files. When you are finished, the system connects to the key management server with the credentials you entered. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

Why do I need to define a pass phrase?

The pass phrase is used to encrypt and decrypt the security key file stored on the local management client. Without the pass phrase, the security key cannot be decrypted and used to unlock data from a secure-enabled drive if it is re-installed in another storage array.

Copyright information

Trademark information