



# **Configure pools and volume groups**

## **E-Series Systems**

NetApp  
April 04, 2023

# Table of Contents

- Configure pools and volume groups . . . . . 1
  - Pools and volume group overview . . . . . 1
  - Create pool automatically . . . . . 4
  - Create pool manually . . . . . 5
  - Create a volume group . . . . . 8
  - Add capacity to a pool or volume group . . . . . 10
  - Create SSD Cache . . . . . 12
  - Change configuration settings for a pool . . . . . 14
  - Change configuration settings for a volume group . . . . . 17
  - Change SSD Cache settings . . . . . 20
  - View SSD Cache statistics . . . . . 21
  - Check volume redundancy . . . . . 23
  - Delete pool or volume group . . . . . 24
  - Consolidate free capacity for a volume group . . . . . 25
  - Turn on locator lights . . . . . 26
  - Remove capacity . . . . . 27
  - Enable security for a pool or volume group . . . . . 28

# Configure pools and volume groups

## Pools and volume group overview

To provision storage in the Storage Plugin for vCenter, you create either a pool or volume group that will contain the Hard Disk Drives (HDD) or Solid State Disk (SSD) drives that you want to use in your storage array.

### Provisioning

Physical hardware is provisioned into logical components so that data can be organized and easily retrieved. There are two types of groupings supported:

- Pools
- Volume groups

The pools and volume groups are the top-level units of storage in a storage array: they divide the capacity of drives into manageable divisions. Within these logical divisions are the individual volumes or LUNs where data is stored.

When a storage system is deployed, the first step is to present the available drive capacity to the various hosts by:

- Creating pools or volume groups with sufficient capacity
- Adding the number of drives required to meet performance requirements to the pool or volume group
- Selecting the desired level of RAID protection (if using volume groups) to meet specific business requirements

You can have pools or volume groups on the same storage system, but a drive cannot be part of more than one pool or volume group. Volumes that are presented to hosts for I/O are then created, using the space on the pool or volume group.

### Pools

Pools are designed to aggregate physical hard disk drives into a large storage space and to provide enhanced RAID protection for it. A pool creates many virtual RAID sets from the total number of drives assigned to the pool, and it spreads the data out evenly among all participating drives. If a drive is lost or added, the system dynamically re-balances the data across all the active drives.

Pools function as another RAID level, virtualizing the underlying RAID architecture to optimize performance and flexibility when performing tasks such as rebuilding, drive expansion, and handling drive loss. The system automatically sets the RAID level at 6 in an 8+2 configuration (eight data disks plus two parity disks).

### Drive matching

You can choose from either HDD or SSDs for use in pools; however, as with volume groups, all drives in the pool must use the same technology. The controllers automatically select which drives to include, so you must make sure that you have a sufficient number of drives for the technology you choose.

## Managing failed drives

Pools have a minimum capacity of 11 drives; however, one drive's worth of capacity is reserved for spare capacity in the event of a drive failure. This spare capacity is called "preservation capacity."

When pools are created, a certain amount of capacity is preserved for emergency use. This capacity is expressed in terms of a number of drives, but the actual implementation is spread across the entire pool of drives. The default amount of capacity that is preserved is based on the number of drives in the pool.

After the pool is created, you can change the preservation capacity value to more or less capacity, or even set it to no preservation capacity (0 drive's worth). The maximum amount of capacity that can be preserved (expressed as a number of drives) is 10, but the capacity that is available might be less, based on the total number of drives in the pool.

## Volume groups

Volume groups define how capacity is allotted in the storage system to volumes. Disk drives are organized into RAID groups and volumes reside across the drives in a RAID group. Therefore, volume group configuration settings identify which drives are part of the group and what RAID level is used.

When you create a volume group, controllers automatically select the drives to include in the group. You must manually choose the RAID level for the group. The capacity of the volume group is the total of the number of drives that you select, multiplied by their capacity.

## Drive matching

You must match the drives in the volume group for size and performance. If there are smaller and larger drives in the volume group, all drives are recognized as the smallest capacity size. If there are slower and faster drives in the volume group, all drives are recognized at the slowest speed. These factors affect the performance and overall capacity of the storage system.

You cannot mix different drive technologies (HDD and SSD drives). RAID 3, 5, and 6 are limited to a maximum of 30 drives. RAID 1 and RAID 10 uses mirroring, so these volume groups must have an even number of disks.

## Managing failed drives

Volume groups use hot spare drives as a standby in case a drive fails in RAID 1/10, RAID 3, RAID 5, or RAID 6 volumes contained in a volume group. A hot spare drive contains no data and adds another level of redundancy to your storage array.

If a drive fails in the storage array, the hot spare drive is automatically substituted for the failed drive without requiring a physical swap. If the hot spare drive is available when a drive fails, the controller uses redundancy data to reconstruct the data from the failed drive to the hot spare drive.

## Decide whether to use pools or volume groups

### Choose a pool

- If you need faster drive rebuilds and simplified storage administration, and/or have a highly random workload.
- If you want to distribute the data for each volume randomly across a set of drives that comprise the pool. You cannot set or change the RAID level of pools or the volumes in the pools. Pools use RAID level 6.

## Choose a volume group

- If you need maximum system bandwidth, the ability to tune storage settings, and a highly sequential workload.
- If you want to distribute the data across the drives based on a RAID level. You can specify the RAID level when you create the volume group.
- If you want to write the data for each volume sequentially across the set of drives that comprise the volume group.



Because pools can co-exist with volume groups, a storage array can contain both pools and volume groups.

## Automatic versus manual pool creation

Depending on your storage configuration, you can allow the system to create pools automatically or you can manually create them yourself. A pool is a set of logically grouped drives.

Before you create and manage pools, review the following sections for how pools are automatically created and when you might need to manually create them.

### Automatic creation

When the system detects unassigned capacity in the storage array, it initiates automatic pool creation. It automatically prompts you to create one or more pools, or add the unassigned capacity to an existing pool, or both.

Automatic pool creation occurs when one of these conditions is true:

- Pools do not exist in the storage array, and there are enough similar drives to create a new pool.
- New drives are added to a storage array that has at least one pool. Each drive in a pool must be of the same drive type (HDD or SSD) and have similar capacity. The system will prompt you to complete the following tasks:
  - Create a single pool if there are a sufficient number of drives of those types.
  - Create multiple pools if the unassigned capacity consists of different drive types.
  - Add the drives to the existing pool if a pool is already defined in the storage array, and add new drives of the same drive type to the pool.
  - Add the drives of the same drive type to the existing pool, and use the other drive types to create different pools if the new drives are of different drive types.

### Manual creation

You might want to create a pool manually when automatic creation cannot determine the best configuration. This situation can occur for one of the following reasons:

- The new drives could potentially be added to more than one pool.
- One or more of the new pool candidates can use shelf loss protection or drawer loss protection.
- One or more of the current pool candidates cannot maintain their shelf loss protection or drawer loss protection status. You might also want to create a pool manually if you have multiple applications on your storage array and do not want them competing for the same drive resources. In this case, you might consider manually creating a smaller pool for one or more of the applications. You can assign just one or

two volumes instead of assigning the workload to a large pool that has many volumes across which to distribute the data. Manually creating a separate pool that is dedicated to the workload of a specific application can allow storage array operations to perform more rapidly, with less contention.

## Create pool automatically

You can create pools automatically when the system detects at least 11 unassigned drives or it detects one unassigned drive that is eligible for an existing pool. A pool is a set of logically grouped drives.

### Before you begin

You can launch the Pool Auto-Configuration dialog box when one of these conditions are true:

- At least one unassigned drive has been detected that can be added to an existing pool with similar drive types.
- Eleven (11) or more unassigned drives have been detected that can be used to create a new pool (if they cannot be added to an existing pool due to dissimilar drive types).

### About this task

You can use automatic pool creation to easily configure all unassigned drives in the storage array into one pool and to add drives into existing pools.

Keep in mind the following:

- When you add drives to a storage array, the system automatically detects the drives and prompts you to create a single pool or multiple pools based on the drive type and the current configuration.
- If pools were previously defined, the system automatically prompts you with the option of adding the compatible drives to an existing pool. When new drives are added to an existing pool, the system automatically redistributes the data across the new capacity, which now includes the new drives that you added.
- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration helps the controllers use both drive-side PCIe buses more effectively. For pool creation, you should use all drives in the storage array.

### Steps

1. From the Manage page, select the storage array for the pool.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Select **More > Launch pool auto-configuration**.

The results table lists new pools, existing pools with drives added, or both. A new pool is named with a sequential number by default.

Notice that the system does the following:

- Creates a single pool if there are a sufficient number of drives with the same drive type (HDD or SSD) and have similar capacity.
- Creates multiple pools if the unassigned capacity consists of different drive types.
- Adds the drives to an existing pool if a pool is already defined in the storage array, and you add new drives of the same drive type to the pool.

- Adds the drives of the same drive type to the existing pool, and use the other drive types to create different pools if the new drives are of different drive types.
4. To change the name of a new pool, click the **Edit** icon (the pencil).
  5. To view additional characteristics of the pool, position the cursor over or touch the Details icon (the page).

Information about the drive type, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection appears.

For EF600 and EF300 storage arrays, settings are also displayed for resource provisioning and volume block sizes.

6. Click **Accept**.

## Create pool manually

You can create a pool manually if your setup does not meet the requirements for automatic pool configuration. A pool is a set of logically grouped drives.

### Before you begin

- You must have a minimum of 11 drives with the same drive type (HDD or SSD).
- Shelf loss protection requires that the drives comprising the pool are located in at least six different drive shelves and there are no more than two drives in a single drive shelf.
- Drawer loss protection requires that the drives comprising the pool are located in at least five different drawers and the pool includes an equal number of drive shelves from each drawer.
- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration helps the controllers use both drive-side PCIe buses more effectively. For pool creation, you should use all drives in the storage array.

### About this task

During pool creation you determine its characteristics, such as drive type, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection.

For EF600 and EF300 storage arrays, settings also include resource provisioning and volume block sizes.

### Steps

1. From the Manage page, select the storage array for the pool.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Click **Create > Pool**.

The Create Pool dialog box appears.

4. Type a name for the pool.
5. (Optional) If you have more than one type of drive in your storage array, select the drive type that you want to use.

The results table lists all the possible pools that you can create.

6. Select the pool candidate that you want to use based on the following characteristics, and then click

**Create.**



## Field Details

Characteristic	Use
Free Capacity	Shows the free capacity of the pool candidate in GiB. Select a pool candidate with the capacity for your application's storage needs. Preservation (spare) capacity is also distributed throughout the pool and is not part of the free capacity amount.
Total Drives	Shows the number of drives available in the pool candidate. The system automatically reserves as many drives as possible for preservation capacity (for every six drives in a pool, the system reserves one drive for preservation capacity). When a drive failure occurs, the preservation capacity is used to hold the reconstructed data.
Drive Block Size (EF300 and EF600 only)	Shows the block size (sector size) that the drives in the pool can write. Values may include: <ul style="list-style-type: none"> <li>• 512 — 512-byte sector size.</li> <li>• 4K — 4,096-byte sector size.</li> </ul>
Secure-Capable	Indicates whether this pool candidate is comprised entirely of secure-capable drives, which can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. <ul style="list-style-type: none"> <li>• You can protect your pool with Drive Security, but all drives must be secure-capable to use this feature.</li> <li>• If you want to create an FDE-only pool, look for <b>Yes - FDE</b> in the Secure-Capable column. If you want to create a FIPS-only pool, look for <b>Yes - FIPS</b> or <b>Yes - FIPS (Mixed)</b>. "Mixed" indicates a mixture of 140-2 and 140-3 level drives. If you use a mixture of these levels, be aware that the pool will then operate at the lower level of security (140-2).</li> <li>• You can create a pool comprised of drives that may or may not be secure-capable or are a mix of security levels. If the drives in the pool include drives that are not secure-capable, you cannot make the pool secure.</li> </ul>
Enable Security?	Provides the option for enabling the Drive Security feature with secure-capable drives. If the pool is secure-capable and you have created a security key, you can enable security by selecting the check box. <div>  <p>The only way to remove Drive Security after it is enabled is to delete the pool and erase the drives.</p> </div>

Characteristic	Use
DA Capable	<p>Indicates if Data Assurance (DA) is available for this pool candidate. DA checks for and corrects errors that might occur as data is transferred through the controllers down to the drives.</p> <p>If you want to use DA, select a pool that is DA capable. This option is available only when the DA feature has been enabled.</p> <p>A pool can contain drives that are DA-capable or not DA-capable, but all drives must be DA capable for you to use this feature.</p>
Resource Provisioning Capable (EF300 and EF600 only)	<p>Shows if Resource Provisioning is available for this pool candidate. 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.</p>
Shelf Loss Protection	<p>Shows if shelf loss protection is available.</p> <p>Shelf loss protection guarantees accessibility to the data on the volumes in a pool if a total loss of communication occurs with a single drive shelf.</p>
Drawer Loss Protection	<p>Shows if drawer loss protection is available, which is provided only if you are using a drive shelf that contains drawers.</p> <p>Drawer loss protection guarantees accessibility to the data on the volumes in a pool if a total loss of communication occurs with a single drawer in a drive shelf.</p>
Volume Block Sizes Supported (EF300 and EF600 only)	<p>Shows the block sizes that can be created for the volumes in the pool:</p> <ul style="list-style-type: none"> <li>• 512n — 512 bytes native.</li> <li>• 512e — 512 bytes emulated.</li> <li>• 4K — 4,096 bytes.</li> </ul>

## Create a volume group

You can create a volume group for one or more volumes that are accessible to the host. A volume group is a container for volumes with shared characteristics such as RAID level and capacity.

### Before you begin

Review the following guidelines:

- You need at least one unassigned drive.
- Limits exist as to how much drive capacity you can have in a single volume group. These limits vary according to your host type.
- To enable shelf/drawer loss protection, you must create a volume group that uses drives located in at least three shelves or drawers, unless you are using RAID 1, where two shelves/drawers is the minimum.
- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration

helps the controllers use both drive-side PCIe buses more effectively. The system currently allows for drive selection under the Advanced feature when creating a volume group.

Review how your choice of RAID level affects the resulting capacity of the volume group.

- If you select RAID 1, you must add two drives at a time to make sure that a mirrored pair is selected. Mirroring and striping (known as RAID 10 or RAID 1+0) is achieved when four or more drives are selected.
- If you select RAID 5, you must add a minimum of three drives to create the volume group.
- If you select RAID 6, you must add a minimum of five drives to create the volume group.

### About this task

During volume group creation you determine the group characteristics, such as the number of drives, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection.

For EF600 and EF300 storage arrays, settings also include resource provisioning, drive block sizes, and volume block sizes.



With larger capacity drives and the ability to distribute volumes across controllers, creating more than one volume per volume group is a good way to make use of your storage capacity and to protect your data.

### Steps

1. From the Manage page, select the storage array for the volume group.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Click **Create > Volume group**.

The Create Volume Group dialog box appears.

4. Type a name for the volume group.
5. Select the RAID level that best meets your requirements for data storage and protection. The volume group candidate table appears and displays only the candidates that support the selected RAID level.
6. (Optional) If you have more than one type of drive in your storage array, select the drive type that you want to use.

The volume group candidate table appears and displays only the candidates that support the selected drive type and RAID level.

7. (Optional) You can select either the automatic method or manual method to define which drives to use in the volume group. The Automatic method is the default selection.



Do not use the Manual method unless you are an expert who understands drive redundancy and optimal drive configurations.

To select drives manually, click the **Manually select drives (advanced)** link. When clicked, it changes to **Automatically select drives (advanced)**.

The Manual method lets you select which specific drives comprise the volume group. You can select specific unassigned drives to obtain the capacity that you require. If the storage array contains drives with different media types or different interface types, you can choose only the unconfigured capacity for a single drive type to create the new volume group.

8. Based on the displayed drive characteristics, select the drives you want to use in the volume group, and then click **Create**.

The drive characteristics displayed depend on whether you selected the automatic method or manual method. For more information, see the SANtricity System Manager documentation, [Create a volume group](#).

## Add capacity to a pool or volume group

You can add drives to expand the free capacity in an existing pool or volume group.

### Before you begin

- Drives must be in an Optimal status.
- Drives must have the same drive type (HDD or SSD).
- The pool or volume group must be in an Optimal status.
- If the pool or volume group contains all secure-capable drives, add only drives that are secure-capable to continue to use the encryption abilities of the secure-capable drives.

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

### About this task

In this task, you can add free capacity to be included in the pool or volume group. You can use this free capacity to create additional volumes. The data in the volumes remains accessible during this operation.

For pools, you can add a maximum of 60 drives at a time. For volume groups, you can add a maximum of two drives at a time. If you need to add more than the maximum number of drives, repeat the procedure. (A pool cannot contain more drives than the maximum limit for a storage array.)



With the addition of drives, your preservation capacity may need to be increased. You should consider increasing your reserved capacity after an expansion operation.



Avoid using drives that are Data Assurance (DA) capable to add capacity to a pool or volume group that is not DA capable. The pool or volume group cannot take advantage of the capabilities of the DA-capable drive. Consider using drives that are not DA capable in this situation.

### Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Select the pool or volume group to which you want to add drives, and then click **Add Capacity**.

The Add Capacity dialog box appears. Only the unassigned drives that are compatible with the pool or volume group appear.

4. Under **Select drives to add capacity...**, select one or more drives that you want to add to the existing pool or volume group.

The controller firmware arranges the unassigned drives with the best options listed at the top. The total free capacity that is added to the pool or volume group appears below the list in **Total capacity selected**.

## Field Details

Field	Description
Shelf	Indicates the shelf location of the drive.
Bay	Indicates the bay location of the drive
Capacity (GiB)	<p>Indicates the drive capacity.</p> <ul style="list-style-type: none"><li>• Whenever possible, select drives that have a capacity equal to the capacities of the current drives in the pool or volume group.</li><li>• If you must add unassigned drives with a smaller capacity, be aware that the usable capacity of each drive currently in the pool or volume group is reduced. Therefore, the drive capacity is the same across the pool or volume group.</li><li>• If you must add unassigned drives with a larger capacity, be aware that the usable capacity of the unassigned drives that you add is reduced so that they match the current capacities of the drives in the pool or volume group.</li></ul>
Secure-Capable	<p>Indicates whether the drive is secure-capable.</p> <ul style="list-style-type: none"><li>• You can protect your pool or volume group with the Drive Security feature, but all drives must be secure-capable to use this feature.</li><li>• It is possible to create a pool or volume group with a mix of secure-capable and non-secure-capable drives, but the Drive Security feature cannot be enabled.</li><li>• A pool or volume group with all secure-capable drives cannot accept a non-secure-capable drive for sparing or expansion, even if the encryption capability is not in use.</li><li>• Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. A FIPS drive can be level 140-2 or 140-3, with level 140-3 as the higher level of security. If you select a mixture of 140-2 and 140-3 level drives, the pool or volume group will then operate at the lower level of security (140-2).</li></ul>

Field	Description
DA Capable	<p>Indicates whether the drive is Data Assurance (DA) capable.</p> <ul style="list-style-type: none"> <li>Using drives that are not Data Assurance (DA) capable to add capacity to a DA-capable pool or volume group is not recommended. The pool or volume group no longer has DA capabilities, and you no longer have the option to enable DA on newly created volumes within the pool or volume group.</li> <li>Using drives that are Data Assurance (DA) capable to add capacity to a pool or volume group that is non DA-capable is not recommended, because that pool or volume group cannot take advantage of the capabilities of the DA-capable drive (the drive attributes do not match). Consider using drives that are not DA-capable in this situation.</li> </ul>
DULBE Capable	<p>Indicates whether the drive has the option for Deallocated or Unwritten Logical Block Error (DULBE). DULBE is an option on NVMe drives that allows the EF300 or EF600 storage array to support resource-provisioned volumes.</p>

5. Click **Add**.

If you are adding drives to a pool or volume group, a confirmation dialog box appears if you selected a drive that causes the pool or volume group to no longer have one or more of the following attributes:

- Shelf loss protection
- Drawer loss protection
- Full Disk Encryption capability
- Data Assurance capability
- DULBE capability

6. To continue, click **Yes**; otherwise click **Cancel**.

### Result

After you add the unassigned drives to a pool or volume group, the data in each volume of the pool or volume group is redistributed to include the additional drives.

## Create SSD Cache

To dynamically accelerate system performance, you can use the SSD Cache feature to cache the most frequently accessed data ("hot" data) onto lower latency Solid State Drives (SSDs). SSD Cache is used exclusively for host reads.

### Before you begin

Your storage array must contain some SSD drives.



SSD Cache is not available on the EF600 or EF300 storage system.

### About this task

When you create SSD Cache, you can use a single drive or multiple drives. Because the read cache is in the storage array, caching is shared across all applications using the storage array. You select the volumes that you want to cache, and then caching is automatic and dynamic.

Follow these guidelines when you create SSD Cache.

- You can enable security on the SSD Cache only when you are creating it, not later.
- Only one SSD Cache is supported per storage array.
- The maximum usable SSD Cache capacity on a storage array is dependent on the controller's primary cache capacity.
- SSD Cache is not supported on snapshot images.
- If you import or export volumes that are SSD Cache enabled or disabled, the cached data is not imported or exported.
- Any volume assigned to use a controller's SSD Cache is not eligible for an automatic load balance transfer.
- If the associated volumes are secure-enabled, create a secure-enabled SSD Cache.

### Steps

1. From the Manage page, select the storage array for the cache.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Click **Create › SSD Cache**.

The Create SSD Cache dialog box appears.

4. Type a name for the SSD Cache.
5. Select the SSD Cache candidate that you want to use based on the following characteristics.

## Field Details

Characteristic	Use
<b>Capacity</b>	Shows the available capacity in GiB. Select the capacity for your application's storage needs. The maximum capacity for SSD Cache depends on the controller's primary cache capacity. If you allocate more than the maximum amount to SSD Cache, then any extra capacity is unusable. SSD Cache capacity counts towards your overall allocated capacity.
<b>Total drives</b>	Shows the number of drives available for this SSD cache. Select the SSD candidate with the number of drives that you want
<b>Secure-capable</b>	Indicates whether the SSD Cache candidate is comprised entirely of secure-capable drives, which can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. If you want to create a secure-enabled SSD Cache, look for "Yes - FDE" or "Yes - FIPS" in the Secure-capable column.
<b>Enable security?</b>	Provides the option for enabling the Drive Security feature with secure-capable drives. If you want to create a secure-enabled SSD Cache, select the <b>Enable Security</b> check box.  NOTE: Once enabled, security cannot be disabled. You can enable security on the SSD Cache only when you are creating it, not later.
<b>DA capable</b>	Indicates if Data Assurance (DA) is available for this SSD Cache candidate. Data Assurance (DA) checks for and corrects errors that might occur as data is transferred through the controllers down to the drives. If you want to use DA, select an SSD Cache candidate that is DA capable. This option is available only when the DA feature has been enabled. SSD Cache can contain both DA-capable and non-DA-capable drives, but all drives must be DA-capable for you to use DA.

- Associate the SSD Cache with the volumes for which you want to implement SSD read caching. To enable SSD Cache on compatible volumes immediately, select the **Enable SSD Cache on existing compatible volumes that are mapped to hosts** check box.

Volumes are compatible if they share the same Drive Security and DA capabilities.

- Click **Create**.

## Change configuration settings for a pool

You can edit the settings for a pool, including its name, capacity alerts settings, modification priorities, and preservation capacity.

### About this task

This task describes how to change configuration settings for a pool.



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



## Steps

1. From the Manage page, select the storage array with the pool.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select the pool that you want to edit, and then click **View/Edit Settings**.

The Pool Settings dialog box appears.

4. Select the **Settings** tab, and then edit the pool settings as appropriate.

## Field Details

Setting	Description
Name	You can change the user-supplied name of the pool. Specifying a name for a pool is required.
Capacity alerts	<p>You can send alert notifications when the free capacity in a pool reaches or exceeds a specified threshold. When the data stored in the pool exceeds the specified threshold, the plugin sends a message, allowing you time to add more storage space or to delete unnecessary objects.</p> <p>Alerts are shown in the Notifications area on the Dashboard and can be sent from the server to administrators by email and SNMP trap messages. You can define the following capacity alerts:</p> <ul style="list-style-type: none"> <li>• <b>Critical alert</b> — This critical alert notifies you when the free capacity in the pool reaches or exceeds the specified threshold. Use the spinner controls to adjust the threshold percentage. Select the check box to disable this notification.</li> <li>• <b>Early alert</b> — This early alert notifies you when the free capacity in a pool is reaching a specified threshold. Use the spinner controls to adjust the threshold percentage. Select the check box to disable this notification.</li> </ul>
Modification priorities	<p>You can specify the priority levels for modification operations in a pool relative to system performance. A higher priority for modification operations in a pool causes an operation to complete faster, but can slow the host I/O performance. A lower priority causes operations to take longer, but host I/O performance is less affected.</p> <p>You can choose from five priority levels: lowest, low, medium, high, and highest. The higher the priority level, the larger is the impact on host I/O and system performance.</p> <ul style="list-style-type: none"> <li>• <b>Critical reconstruction priority</b> — This slider bar determines the priority of a data reconstruction operation when multiple drive failures result in a condition where some data has no redundancy and an additional drive failure might result in loss of data.</li> <li>• <b>Degraded reconstruction priority</b> — This slider bar determines the priority of the data reconstruction operation when a drive failure has occurred, but the data still has redundancy and an additional drive failure does not result in loss of data.</li> <li>• <b>Background operation priority</b> — This slider bar determines the priority of the pool background operations that occur while the pool is in an optimal state. These operations include Dynamic Volume Expansion (DVE), Instant Availability Format (IAF), and migrating data to a replaced or added drive.</li> </ul>

Setting	Description
Preservation capacity ("Optimization capacity" for the EF600 or EF300)	<p><b>Preservation capacity</b> — You can define the number of drives to determine the capacity that is reserved on the pool to support potential drive failures. When a drive failure occurs, the preservation capacity is used to hold the reconstructed data. Pools use preservation capacity during the data reconstruction process instead of hot spare drives, which are used in volume groups.</p> <p>Use the spinner controls to adjust the number of drives. Based on the number of drives, the preservation capacity in the pool appears next to the spinner box.</p> <p>Keep the following information in mind about preservation capacity.</p> <ul style="list-style-type: none"> <li>• Because preservation capacity is subtracted from the total free capacity of a pool, the amount of capacity that you reserve affects how much free capacity is available to create volumes. If you specify 0 for the preservation capacity, all of the free capacity on the pool is used for volume creation.</li> <li>• If you decrease the preservation capacity, you increase the capacity that can be used for pool volumes.</li> </ul> <p><b>Additional optimization capacity (EF600 and EF300 arrays only)</b> — When a pool is created, a recommended optimization capacity is generated that provides a balance of available capacity versus performance and drive wear life. You can adjust this balance by moving the slider to the right for better performance and drive wear life at the expense of increased available capacity, or by moving it to the left for increased available capacity at the expense of better performance and drive wear life. 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.</p>

5. Click **Save**.

## Change configuration settings for a volume group

You can edit the settings for a volume group, including its name and RAID level.

### Before you begin

If you are changing the RAID level to accommodate the performance needs of the applications that are accessing the volume group, be sure to meet the following prerequisites:

- The volume group must be in Optimal status.
- You must have enough capacity in the volume group to convert to the new RAID level.

### Steps

1. From the Manage page, select the storage array with the volume group.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select the volume group that you want to edit, and then click **View/Edit Settings**.

The Volume Group Settings dialog box appears.

4. Select the **Settings** tab, and then edit the volume group settings as appropriate.

## Field Details

Setting	Description
Name	You can change the user-supplied name of the volume group. Specifying a name for a volume group is required.
RAID level	<p>Select the new RAID level from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>RAID 0 striping</b> — Offers high performance but does not provide any data redundancy. If a single drive fails in the volume group, all the associated volumes fail, and all data is lost. A striping RAID group combines two or more drives into one large, logical drive.</li> <li>• <b>RAID 1 mirroring</b> — Offers high performance and the best data availability and is suitable for storing sensitive data on a corporate or personal level. Protects your data by automatically mirroring the contents of one drive to the second drive in the mirrored pair. It provides protection in the event of a single drive failure.</li> <li>• <b>RAID 10 striping/mirroring</b> — Provides a combination of RAID 0 (striping) and RAID 1 (mirroring) and is achieved when four or more drives are selected. RAID 10 is suitable for high volume transaction applications, such as a database, that require high performance and fault tolerance.</li> <li>• <b>RAID 5</b> — Optimal for multi-user environments (such as database or file system storage) where typical I/O size is small and there is a high proportion of read activity.</li> <li>• <b>RAID 6</b> — Optimal for environments requiring redundancy protection beyond RAID 5, but not requiring high write performance. RAID 3 can be assigned only to volume groups using the command line interface (CLI). When you change the RAID level, you cannot cancel this operation after it begins. During the change, your data remains available.</li> </ul>
Optimization capacity (EF600 arrays only)	When a volume group is created, a recommended optimization capacity is generated that provides a balance of available capacity versus performance and drive wear life. You can adjust this balance by moving the slider to the right for better performance and drive wear life at the expense of increased available capacity, or by moving it to the left for increased available capacity at the expense of better performance and drive wear life. 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 group's 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.

5. Click **Save**.

A confirmation dialog box appears if capacity is reduced, volume redundancy is lost, or shelf/ drawer loss

protection is lost as a result of the RAID level change. Select **Yes** to continue; otherwise click **No**.

### Result

If you change the RAID level for a volume group, the plugin changes the RAID levels of every volume that comprises the volume group. Performance might be slightly affected during the operation.

## Change SSD Cache settings

You can edit the name of the SSD Cache and view its status, maximum and current capacity, Drive Security and Data Assurance status, and its associated volumes and drives.



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

### Steps

1. From the Manage page, select the storage array with the SSD Cache.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select the SSD Cache that you want to edit, and then click **View/Edit Settings**.

The SSD Cache Settings dialog box appears.

4. Review or edit the SSD Cache settings as appropriate.

## Field Details

Setting	Description
Name	Displays the name of the SSD Cache, which you can change. A name for the SSD Cache is required.
Characteristics	Shows the status for the SSD Cache. Possible statuses include: <ul style="list-style-type: none"><li>• Optimal</li><li>• Unknown</li><li>• Degraded</li><li>• Failed (A failed state results in a critical MEL event.)</li><li>• Suspended</li></ul>
Capacities	Shows the current capacity and maximum capacity allowed for the SSD Cache. The maximum capacity allowed for the SSD Cache depends on the controller's primary cache size: <ul style="list-style-type: none"><li>• Up to 1 GiB</li><li>• 1 GiB to 2 GiB</li><li>• 2 GiB to 4 GiB</li><li>• More than 4 GiB</li></ul>
Security and DA	Shows the Drive Security and Data Assurance status for the SSD Cache. <ul style="list-style-type: none"><li>• <b>Secure-capable</b> --Indicates whether the SSD Cache is comprised entirely of secure-capable drives. A secure-capable drive is a self-encrypting drive that can protect its data from unauthorized access.</li><li>• <b>Secure-enabled</b> — Indicates whether security is enabled on the SSD Cache.</li><li>• <b>DA capable</b> — Indicates whether the SSD Cache is comprised entirely of DA-capable drives. A DA-capable drive can check for and correct errors that might occur as data is communicated between the host and storage array.</li></ul>
Associated objects	Shows the volumes and drives associated with the SSD Cache.

5. Click **Save**.

## View SSD Cache statistics

You can view statistics for the SSD Cache, such as reads, writes, cache hits, cache allocation percentage, and cache utilization percentage.



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

### About this task

The nominal statistics, which are a subset of the detailed statistics, are shown on the View SSD Cache Statistics dialog box. You can view detailed statistics for the SSD Cache 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.

### Steps

1. From the Manage page, select the storage array with the SSD Cache.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Select the SSD Cache for which you want to view statistics, and then click **More > View SSD Cache statistics**.

The View SSD Cache Statistics dialog box appears and displays the nominal statistics for the selected SSD cache.

### Field Details

Setting	Description
<b>Reads</b>	Shows the total number of host reads from the SSD Cache-enabled volumes. The greater the ratio of Reads to Writes, the better is the operation of the cache.
<b>Writes</b>	The total number of host writes to the SSD Cache-enabled volumes. The greater the ratio of Reads to Writes, the better is the operation of the cache.
<b>Cache hits</b>	Shows the number of cache hits.
<b>Cache hits %</b>	Shows the percentage of cache hits. This number is derived from Cache Hits / (reads + writes). The cache hit percentage should be greater than 50 percent for effective SSD Cache operation.
<b>Cache allocation %</b>	Shows the percentage of SSD Cache storage that is allocated, expressed as a percentage of the SSD Cache storage that is available to this controller and is derived from allocated bytes / available bytes.
<b>Cache utilization %</b>	Shows the percentage of SSD Cache storage that contains data from enabled volumes, expressed as a percentage of SSD Cache storage that is allocated. This amount represents the utilization or density of the SSD Cache. Derived from allocated bytes / available bytes.
<b>Export All</b>	Exports all SSD Cache statistics to a CSV format. The exported file contains all available statistics for the SSD Cache (both nominal and detailed).

4. Click **Cancel** to close the dialog box.



# Check volume redundancy

Under the guidance of technical support or as instructed by the Recovery Guru, you can check the redundancy on a volume in a pool or volume group to determine whether the data on that volume 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.

## Before you begin

- The status of the pool or volume group must be Optimal.
- The pool or volume group must have no volume modification operations in progress.
- You can check redundancy on any RAID level except on RAID 0, because RAID 0 has no data redundancy. (Pools are configured only as RAID 6.)



Check volume redundancy only when instructed to do so by the Recovery Guru and under the guidance of technical support.

## About this task

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 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 controller firmware determines that the data is inconsistent.



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.

## Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning** > **Configure Pools and Volume Groups**.
3. Select **Uncommon Tasks** > **Check volume redundancy**.

The Check Redundancy dialog box appears.

4. Select the volumes you want to check, and then type check to confirm you want to perform this operation.
5. Click **Check**.

The check volume redundancy operation starts. The volumes in the pool or volume group are sequentially scanned, starting from the top of the table in the dialog box. These actions occur as each volume is scanned:

- The volume is selected in the volume table.
- The status of the redundancy check is shown in the Status column.

- The check stops on any media or parity error encountered, and then reports the error. The following table provide more information about the status of the redundancy check:

#### Field Details

Status	Description
<b>Pending</b>	This is the first volume to be scanned, and you have not clicked Start to start the redundancy check. -or- The redundancy check operation is being performed on other volumes in the pool or volume group.
<b>Checking</b>	The volume is undergoing the redundancy check.
<b>Passed</b>	The volume passed the redundancy check. No inconsistencies were detected in the redundancy information.
<b>Failed</b>	The volume failed the redundancy check. Inconsistencies were detected in the redundancy information.
<b>Media error</b>	The drive media is defective and is unreadable. Follow the instructions displayed in the Recovery Guru.
<b>Parity error</b>	The parity is not what it should be for a given portion of the data. A parity error is potentially serious and could cause a permanent loss of data.

6. Click **Done** after the last volume in the pool or volume group has been checked.

## Delete pool or volume group

You can delete a pool or volume group to create more unassigned capacity, which you can reconfigure to meet your application storage needs.

#### Before you begin

- You must have backed up the data on all of the volumes in the pool or volume group.
- You must have stopped all input/output (I/O).
- You must unmount any file systems on the volumes.
- You must have deleted any mirror relationships in the pool or volume group.
- You must have stopped any volume copy operation in progress for the pool or volume group.
- The pool or volume group must not be participating in an asynchronous mirroring operation.
- The drives in the volume group must not have a persistent reservation.

#### Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select one pool or volume group from the list.

You can select only one pool or volume group at a time. Scroll down the list to see additional pools or volume groups.

4. Select **Uncommon Tasks** > **Delete** and confirm.

## Results

The system performs the following actions:

- Deletes all of the data in the pool or volume group.
- Deletes all the drives associated with the pool or volume group.
- Unassigns the associated drives, which allows you to reuse them in new or existing pools or volume groups.

## Consolidate free capacity for a volume group

Use the Consolidate Free Capacity option to consolidate existing free extents on a selected volume group. By performing this action, you can create additional volumes from the maximum amount of free capacity in a volume group.

### Before you begin

- The volume group must contain at least one free capacity area.
- All of the volumes in the volume group must be online and in Optimal status.
- Volume modification operations must not be in progress, such as changing the segment size of a volume.

### About this task

You cannot cancel the operation after it begins. Your data remains accessible during the consolidation operation.

You can launch the Consolidate Free Capacity dialog box using any of the following methods:

- When at least one free capacity area is detected for a volume group, the Consolidate free capacity recommendation appears on the Home page in the Notification area. Click the **Consolidate free capacity** link to launch the dialog box.
- You can also launch the Consolidate Free Capacity dialog box from the Pools & Volume Groups page as described in the following task.

## More about free capacity areas

A free capacity area is the free capacity that can result from deleting a volume or from not using all available free capacity during volume creation. When you create a volume in a volume group that has one or more free capacity areas, the volume's capacity is limited to the largest free capacity area in that volume group. For example, if a volume group has a total of 15 GiB free capacity, and the largest free capacity area is 10 GiB, the largest volume you can create is 10 GiB.

You consolidate free capacity on a volume group to improve write performance. Your volume group's free capacity will become fragmented over time as the host writes, modifies, and deletes files. Eventually, the available capacity will not be located in a single contiguous block, but will be scattered in small fragments across the volume group. This causes further file fragmentation, since the host must write new files as fragments to fit them into the available ranges of free clusters.

By consolidating free capacity on a selected volume group, you will notice improved file system performance whenever the host writes new files. The consolidation process will also help prevent new files from being fragmented in the future.

### Steps

1. From the Manage page, select the storage array with the volume group.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select the volume group with free capacity that you want to consolidate, and then select **Uncommon Tasks** › **Consolidate volume group free capacity**.

The Consolidate Free Capacity dialog box appears.

4. Type `consolidate` to confirm you want to perform this operation.
5. Click **Consolidate**.

### Result

The system begins consolidating (defragmenting) the volume group's free capacity areas into one contiguous amount for subsequent storage configuration tasks.

### After you finish

From the navigation sidebar, select **Operations** to view the progress of the Consolidate Free Capacity operation. This operation can be lengthy and could affect system performance.

## Turn on locator lights

You can locate drives to physically identify all of the drives that comprise a selected pool, volume group, or SSD Cache. An LED indicator lights up on each drive in the selected pool, volume group, or SSD Cache.

### Steps

1. From the Manage page, select the storage array.
2. Select **Provisioning** › **Configure Pools and Volume Groups**.
3. Select the pool, volume group, or SSD Cache you want to locate, and then click **More** › **Turn on locator lights**.

A dialog box appears that indicates the lights on the drives comprising the selected pool, volume group, or SSD Cache are turned on.

4. After you successfully locate the drives, click **Turn Off**.

## Remove capacity

You can remove drives to decrease the capacity of an existing pool or SSD Cache.

After you remove drives, the data in each volume of the pool or SSD Cache is redistributed to the remaining drives. The removed drives become unassigned, and their capacity becomes part of the total free capacity of the storage array.

### About this task

Follow these guidelines when you remove capacity:

- You cannot remove the last drive in an SSD Cache without first deleting the SSD Cache.
- You cannot reduce the number of drives in a pool to be less than 11 drives.
- You can remove a maximum of 12 drives at a time. If you need to remove more than 12 drives, repeat the procedure.
- You cannot remove drives if there is not enough free capacity in the pool or SSD Cache to contain the data, when that data is redistributed to the remaining drives in the pool or SSD Cache.

The following are potential performance impacts:

- Removing drives from a pool or SSD Cache might result in reduced volume performance.
- The preservation capacity is not consumed when you remove capacity from a pool or SSD Cache. However, the preservation capacity might decrease based on the number of drives remaining in the pool or SSD Cache.

The following are impacts to secure-capable drives:

- If you remove the last drive that is not secure-capable, the pool is left with all secure-capable drives. In this situation, you are given the option to enable security for the pool.
- If you remove the last drive that is not Data Assurance (DA) capable, the pool is left with all DA-capable drives.
- Any new volumes that you create on the pool will be DA-capable. If you want existing volumes to be DA-capable, you need to delete and then re-create the volume.

### Steps

1. From the Manage page, select the storage array.

Select **Provisioning > Configure Pools and Volume Groups**.

2. Select the pool or SSD Cache, and then click **More > Remove capacity**.

The Remove Capacity dialog box appears.

3. Select one or more drives in the list.

As you select or de-select drives in the list, the Total capacity selected field updates. This field shows the

total capacity of the pool or SSD Cache that results after you remove the selected drives.

4. Click **Remove**, and then confirm you want to remove the drives.

### Result

The newly reduced capacity of the pool or SSD Cache is reflected in the Pools and Volume Groups view.

## Enable security for a pool or volume group

You can enable Drive Security for a pool or volume group to prevent unauthorized access to the data on the drives contained in the pool or volume group.

Read and write access for the drives is only available through a controller that is configured with a security key.

### Before you begin

- The Drive Security feature must be enabled.
- A security key must be created.
- The pool or volume group must be in an Optimal state.
- All of the drives in the pool or volume group must be secure-capable drives.

### About this task

If you want to use Drive Security, select a pool or volume group that is secure-capable. A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.

After enabling security, you can only remove it by deleting the pool or volume group, and then erasing the drives.

### Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning > Configure Pools and Volume Groups**.
3. Select the pool or volume group on which you want to enable security, and then click **More > Enable security**.

The Confirm Enable Security dialog box appears.

4. Confirm that you want to enable security for the selected pool or volume group, and then click **Enable**.

## Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.