Manage

SANtricity 11.6

NetApp
February 12, 2024

Table of Contents

Manage

Discover storage arrays

Concepts

Considerations for discovering arrays

Before SANtricity Unified Manager can display and manage storage resources, it must discover the storage arrays you want to manage in your organization's network. You can discover multiple arrays or you can discover a single array.

Discovering multiple storage arrays

If you choose to discover multiple arrays, you enter a network IP address range and then Unified Manager attempts individual connections to each IP address in that range. Any storage array successfully reached appears on the **Discover** page and may be added to your management domain.

Discovering a single storage array

If you choose to discover a single array, you enter the single IP address for one of the controllers in the storage array and then the individual storage array is added.

> Unified Manager discovers and displays only the single IP address or IP address within a range assigned to a controller. If there are alternate controllers or IP addresses assigned to these controllers that fall outside of this single IP address or IP address range, then Unified Manager will not discover or display them. However, once you add the storage array, all associated IP addresses will be discovered and displayed in the **Manage** view.

User credentials

As part of the discovery process, you must supply the administrator password for each storage array you want to add.

Web services certificates

As part of the discovery process, Unified Manager verifies that the discovered storage arrays are using certificates by a trusted source. Unified Manager uses two types of certificate-based authentication for all connections that it establishes with the browser:

- **Trusted certificates**

  For arrays discovered by Unified Manager, you might need to install additional trusted certificates supplied by the Certificate Authority.

  Use the **Import** button to import these certificates. If you have connected to this array before, one or both controller certificates are either expired, revoked, or missing a root certificate or intermediate certificate in its certificate chain. You must replace the expired or revoked certificate or add the missing root certificate or intermediate certificate before managing the storage array.

- **Self-signed certificates**

Self-signed certificates can also be used. If the administrator attempts to discover arrays without importing signed certificates, Unified Manager displays an error dialog box that allows the administrator to accept the self-signed certificate. The storage array's self-signed certificate will be marked as trusted and the storage array will be added to Unified Manager.

If you do not trust the connections to the storage array, select **Cancel** and validate the storage array's security certificate strategy before adding the storage array to Unified Manager.

How tos

Discover multiple storage arrays

You discover multiple arrays to detect all storage arrays across the subnet where the management server resides and to automatically add the discovered arrays to your management domain.

About this task

Perform the following steps to discover multiple arrays.

Step1: Enter network address

You enter a network address range to search across the local sub-network. Any storage array successfully reached appears on the **Discover** page and might be added to your management domain.

About this task

If you need to stop the discovery operation for any reason, click **Stop Discovery**.

Steps

1. From the **Manage** page, select **Add/Discover**.

   The Add/Discover storage arrays dialog appears.

2. Select the **Discover all storage arrays within a network range** radio button.
3. Enter the starting network address and ending network address to search across your local sub-network, and then click **Start Discovery**.

   The discovery process starts. This discovery process can take several minutes to complete. The table on the **Discover** page is populated as the storage arrays are discovered.

   > If no manageable arrays are discovered, verify that the storage arrays are properly connected to your network and their assigned addresses are within range. Click **New Discovery Parameters** to return to the **Add/Discover** page.

4. Review the list of discovered storage arrays.
5. Select the checkbox next to any storage array that you want to add to your management domain, and then click **Next**.

   SANtricity Unified Manager performs a credential check on each array you are adding to the management domain. You might need to resolve any self-signed certificates and untrusted certificates associated with that array.

6. Click **Next** to proceed to the next step in the wizard.
7. Go to Step 2: Resolve self-signed certificates during discovery.

Step 2: Resolve self-signed certificates during discovery

As part of the discovery process, the system verifies that the storage arrays are using certificates by a trusted source.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.

Steps

1. Do one of the following:
    - If you trust the connections to the discovered storage arrays, continue to the next card in the wizard. The self-signed certificates will be marked as trusted and the storage arrays will be added to SANtricity Unified Manager.
    - If you do not trust the connections to the storage arrays, select **Cancel** and validate each storage array's security certificate strategy before adding any of them to Unified Manager.
2. Click **Next** to proceed to the next step in the wizard.
3. Go to Step 3: Resolve untrusted certificates during discovery.

Step 3: Resolve untrusted certificates during discovery

Untrusted certificates occur when a storage array attempts to establish a secure connection to SANtricity Unified Manager, but the connection fails to confirm as secure. During the array discovery process, you can resolve untrusted certificates by importing a certificate authority (CA) certificate (or CA-signed certificate) that has been issued by a trusted third party.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.
- You have generated a certificate signing request (.CSR file) for each controller in the storage array, and sent it to the CA.
- The CA returned trusted certificate files.
- The certificate files are available on your local system.

About this task

You may need to install additional trusted CA certificates if any of the following are true:

- You recently added a storage array.
- One or both certificates are expired.
- One or both certificates are revoked.
- One or both certificates are missing a root or intermediate certificate.

Steps

1. Select the check box next to any storage array that you want to resolve untrusted certificates for, and then select the **Import** button.

    A dialog box opens for importing the trusted certificate files.

2. Click **Browse** to select the certificate files for the storage arrays.

   The file names display in the dialog box.

3. Click **Import**.

   The files are uploaded and validated.

   > Any storage array with untrusted certificate issues that are unresolved will not be added to Unified Manager.

4. Click **Next** to proceed to the next step in the wizard.
5. Go to Step 4: Provide passwords.

Step 4: Provide passwords

You must enter the passwords for the storage arrays that you want to add to your management domain.

Before you begin

- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using SANtricity System Manager's **Access Management** tile.

Steps

1. Enter the password for each storage array you want to add to SANtricity Unified Manager.
2. **Optional:** Associate storage arrays to a group: From the drop-down list, select the desired group to associate with the selected storage arrays.
3. Click **Finish**.

After you finish

The storage arrays are added to your management domain and associated with the selected group (if specified).

> It can take several minutes for Unified Manager to connect to the specified storage arrays.

Discover single array

Use the Add/Discover Single Storage Array option to manually discover and add a single storage array to your organization's network.

Before you begin

- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using SANtricity System Manager's Access Management tile.

Steps

1. From the **Manage** page, select **Add/Discover**.

   The **Add/Discover storage arrays** dialog box appears.

2. Select the **Discover a single storage array** radio button.

3. Enter the IP address for one of the controllers in the storage array, and then click **Start Discovery**.

   It can take several minutes for SANtricity Unified Manager to connect to the specified storage array.

   > The **Storage Array Not Accessible** message appears when the connection to the IP address of the specified controller is unsuccessful.

4. If prompted, resolve any self-signed certificates.

   As part of the discovery process, the system verifies that the discovered storage arrays are using certificates by a trusted source. If it cannot locate a digital certificate for a storage array, it prompts you to resolve the certificate that is not signed by a recognized certificate authority (CA) by adding a security exception.

5. If prompted, resolve any untrusted certificates.

   Untrusted certificates occur when a storage array attempts to establish a secure connection to SANtricity Unified Manager, but the connection fails to confirm as secure. Resolve untrusted certificates by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

6. Click **Next**.
7. **Optional:** Associate the discovered storage array to a group: From the drop-down list, select the desired group to associate with the storage array.

   The "All" group is selected by default.

8. Enter the administrator password for the storage array that you want to add to your management domain, and then click **OK**.

After you finish

The storage array is added to SANtricity Unified Manager and, if specified, it is also added to the group you selected.

If automatic support data collection is enabled, support data is automatically collected for a storage array that you add.

Launch

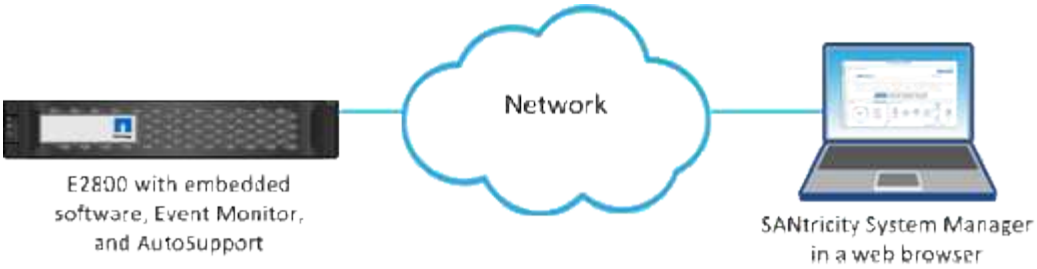
Considerations for accessing SANtricity System Manager

You select one or more storage arrays and use the Launch option to open SANtricity System Manager when you want to configure and manage storage arrays.

SANtricity System Manager is an embedded application on the E2800 or E5700 controller, which is connected to the network through an Ethernet management port.

SANtricity System Manager includes all array-based functions for E2800 or E5700 arrays.

To access SANtricity System Manager, you must have an out-of-band connection to a network management client with a web browser.



Manage an individual storage array

You can use the Launch option to open the browser-based SANtricity System Manager for one or more storage arrays when you want to perform management operations.

Steps

1. From the **Manage** page, select one or more storage arrays that you want to manage.
2. Click **Launch**.

   The system opens a new window and displays the SANtricity System Manager login page.

3. Enter your username and password, and then click **Log in**.

Import Settings

Concepts

How Import Settings works

You can use SANtricity Unified Manager to import settings from one storage array to multiple storage arrays. The Import Settings feature is a batch operation that saves time when you need to configure multiple arrays in the network.

Settings available for import

The following configurations can be imported to multiple arrays:

- **Alerts** — Alerting methods to send important events to administrators, using email, a syslog server, or an SNMP server.
- **AutoSupport** — A feature that monitors the health of a storage array and sends automatic dispatches to technical support.
- **Directory services** — A method of user authentication that is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory.
- **Storage configuration** — Configurations relating to the following:
  - Volumes (thick and non-repository volumes only)
  - Volume groups and pools
  - Hot spare drive assignments
- **System settings** — Configurations relating to the following:
  - Media scan settings for a volume

- SSD settings
- Automatic load balancing (does not include host connectivity reporting)

Configuration workflow

To import settings, follow this workflow:

1. On a storage array to be used as the source, configure the settings using SANtricity System Manager.
2. On the storage arrays to be used as the targets, back up their configuration using SANtricity System Manager.
3. From SANtricity Unified Manager, go to the **Manage** page and import the settings.
4. From the **Operations** page, review the results of the Import Settings operation.

Requirements for replicating storage configurations

Before importing a storage configuration from one storage array to another, review the requirements and guidelines.

Shelves

- The shelves where the controllers reside must be identical on the source and target arrays.
- Shelf IDs must be identical on the source and target arrays.
- Expansion shelves must be populated in the same slots with the same drive types (if the drive is used in the configuration, the location of unused drives does not matter).

Controllers

- The controller type can be different between the source and target arrays (for example, importing from an E2800 to an E5700), but the RBOD enclosure type must be identical.
- The HICs, including the DA capabilities of the host, must be identical between the source and target arrays.
- Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
- FDE settings are not included in the import process.

Status

- The target arrays must be in Optimal status.
- The source array does not need to be in Optimal status.

Storage

- Drive capacity may vary between the source and target arrays, as long as the volume capacity on the target is larger than the source. (A target array might have newer, larger capacity drives that would not be fully configured into volumes by the replication operation.)
- Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.
- Thin volumes are not included in the import process.

How tos

Import alert settings

You can import alert configurations from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Alerts are configured in SANtricity System Manager for the storage array you want to use as the source (**Settings › Alerts**).
- The existing configuration for the target storage arrays are backed up in SANtricity System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

You can select email, SNMP, or syslog alerts for the import operation. The imported settings include:

- **Email alerts** — A mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — A syslog server address and a UDP port.
- **SNMP alerts** — A community name and IP address for the SNMP server.

Steps

1. From the **Manage** page, click **Import Settings**.

   The **Import Settings** wizard opens.

2. In the **Select Settings** dialog, select either **Email alerts**, **SNMP alerts**, or **Syslog alerts**, and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the **Select Source** dialog, select the array with the settings you want to import, and then click **Next**.
4. In the **Select Targets** dialog, select one or more arrays to receive the new settings.

   > Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The **Operations** page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured to send alerts to administrators through email, SNMP, or syslog.

Import AutoSupport settings

You can import an AutoSupport configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- AutoSupport is configured in SANtricity System Manager for the storage array you want to use as the source (**Support › Support Center**).
- The existing configuration for the target storage arrays are backed up in SANtricity System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.

Steps

1. From the **Manage** page, click **Import Settings**.

   The **Import Settings** wizard opens.

2. In the **Select Settings** dialog, select **AutoSupport** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the **Select Source** dialog, select the array with the settings you want to import, and then click **Next**.
4. In the **Select Targets** dialog, select one or more arrays to receive the new settings.

   > Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The **Operations** page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same AutoSupport settings as the source array.

Import directory services settings

You can import a directory services configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Directory services are configured in SANtricity System Manager for the storage array you want to use as the source (**Settings › Access Management**).
- The existing configuration for the target storage arrays are backed up in SANtricity System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include 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.

Steps

1. From the **Manage** page, click **Import Settings**.

   The **Import Settings** wizard opens.

2. In the **Select Settings** dialog, select **Directory services** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the **Select Source** dialog, select the array with the settings you want to import, and then click **Next**.
4. In the **Select Targets** dialog, select one or more arrays to receive the new settings.

   > Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The **Operations** page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same directory services as the source array.

Import system settings

You can import the system configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- System settings are configured in SANtricity System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in SANtricity System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include media scan settings for a volume, SSD settings for controllers, and automatic load balancing (does not include host connectivity reporting).

Steps

1. From the **Manage** page, click **Import Settings**.

   The **Import Settings** wizard opens.

2. In the **Select Settings** dialog, select **System** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the **Select Source** dialog, select the array with the settings you want to import, and then click **Next**.
4. In the **Select Targets** dialog, select one or more arrays to receive the new settings.

> Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The **Operations** page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same system settings as the source array.

Import storage configuration settings

You can import the storage configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Storage is configured in SANtricity System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in SANtricity System Manager (**Settings › System › Save Storage Array Configuration**).
- The source and target arrays must meet these requirements:
  - The shelves where the controllers reside must be identical.
  - Shelf IDs must be identical.
  - Expansion shelves must be populated in the same slots with the same drive types.
  - The RBOD enclosure type must be identical.
  - The HICs, including the Data Assurance capabilities of the host, must be identical.
  - The target arrays must be in Optimal status.
  - The volume capacity on the target array is larger than the source array's capacity.
- You understand the following restrictions:
  - Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
  - Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.
  - Thin volumes are not included in the import process.

About this task

Imported settings include configured volumes (thick and non-repository volumes only), volume groups, pools, and hot spare drive assignments.

Steps

1. From the **Manage** page, click **Import Settings**.

   The **Import Settings** wizard opens.

2. In the **Select Settings** dialog, select **Storage configuration** and then click **Next**.

A dialog box opens for selecting the source array.

3. In the **Select Source** dialog, select the array with the settings you want to import, and then click **Next**.
4. In the **Select Targets** dialog, select one or more arrays to receive the new settings.

> Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The **Operations** page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same storage configuration as the source array.

FAQs

What settings will be 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 SANtricity 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 don't I 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.
- Unified Manager cannot communicate with that array (for example, it has certificate, password, or networking problems).

Manage Groups

Concepts

Storage array groups

You can manage your physical and virtualized infrastructure by grouping a set of storage arrays. You might want to group storage arrays to make it easier to run monitoring or reporting jobs.

There are two types of storage array groups:

- **All group**

  The All group is the default group and includes all the storage arrays discovered in your organization. The All group can be accessed from the main view.

- **User-created group**

  A user-created group includes the storage arrays that you manually select to add to that group. User-created groups can be accessed from the main view.

Storage array status

When you open SANtricity Unified Manager, communication with each storage array is established and the status for each storage array is displayed.

You can view the status of the storage array and the status of the connection between the Web Services Proxy and that storage array.

Status	Indicates
Optimal	The storage array is in an optimal state. There are no certificate issues and the password is valid.
Invalid Password	An invalid storage array password was provided.
Untrusted Certificate	One or more connections with the storage array is untrusted because the HTTPS certificate is either self-signed and has not been imported, or the certificate is CA-signed and the root and intermediate CA certificates have not been imported.

Status	Indicates
Needs Attention	There is a problem with the storage array that requires your intervention to correct it.
Lockdown	The storage array is in a locked-down state.
Unknown	The storage array has never been contacted. This can happen when the Web Services Proxy is starting up and has not yet made contact with the storage array, or the storage array is offline and has never been contacted since the Web Services Proxy was started.
Offline	The Web Services Proxy had previously contacted the storage array, but now has lost all connection to it.

How tos

Manage groups

Create storage array group

You create storage groups, and then add storage arrays to the groups. The storage group defines which drives provide the storage that makes up the volume.

Steps

1. From the **Manage** page, select **Manage Groups › Create storage array group**.
2. In the **Name** field, type a name for the new group.
3. Select the storage arrays that you want to add to the new group.
4. Click **Create**.

Delete storage array group

You can remove one or more storage array groups that are no longer needed.

About this task

This operation deletes only the storage array group. Storage arrays associated with the deleted group remain accessible through the Manage All view or any other group it is associated with.

Steps

1. From the **Manage** page, select **Manage Groups › Delete storage array group**.
2. Select one or more storage array groups that you want to delete.
3. Click **Delete.**

Rename storage array group

You can change the name of a storage array group when the current name is no longer

meaningful or applicable.

About this task

Keep these guidelines in mind.

- A name can consist of letters, numbers, and the special characters underscore (_), hyphen (-), and pound (#). If you choose any other characters, an error message appears. You are prompted to choose another name.
- Limit the name to 30 characters. Any leading and trailing spaces in the name are deleted.
- Use a unique, meaningful name that is easy to understand and remember.
- Avoid arbitrary names or names that would quickly lose their meaning in the future.

Steps

1. From the main view, select **Manage**, and then select the storage array group you want to rename.
2. Select **Manage Groups › Rename storage array group**.
3. In the **Group Name** field, type a new name for the group.
4. Click **Rename.**

Add storage array to group

You can add one or more storage arrays to a user-created group.

Steps

1. From the main view, select **Manage**, and then select the group that you want to add storage arrays to.
2. Select **Manage Groups › Add storage arrays to group**.
3. Select the storage arrays that you want to add to the group.
4. Click **Add.**

Remove storage arrays from group

You can remove one or more managed storage arrays from a group if you no longer want to manage it from a specific storage group.

About this task

Removing storage arrays from a group does not affect the storage array or its data in any way. If your storage array is managed by SANtricity System Manager, you can still manage it using your browser. If a storage array is accidentally removed from a group, it can be added again.

Steps

1. From the **Manage** page, select **Manage Groups › Remove storage arrays from group**.
2. From the drop-down, select the group that contains the storage arrays you want to remove, and then click the check box next to each storage array that you want to remove from the group.
3. Click **Remove**.

Remove storage arrays from SANtricity Unified Manager

You can remove one or more storage arrays if you no longer want to manage it from

SANtricity Unified Manager.

About this task

You cannot access any of the storage arrays you remove. You can, however, establish a connection to any of the removed storage arrays by pointing a browser directly to its IP address or host name.

Removing a storage array does not affect the storage array or its data in any way. If a storage array is accidentally removed, it can be added again.

Steps

1. Select the **Manage** page.
2. Select one or more storage arrays that you want to remove.
3. Select **Uncommon Tasks › Remove storage array**.

   The storage array is removed from all the views in SANtricity Unified Manager.

Upgrade Center

Concepts

How upgrades work

You can use SANtricity Unified Manager to upgrade the SANtricity OS software on multiple storage arrays of the same type to a newer version.

Upgrade workflow

The following steps provide a high-level workflow for performing software upgrades:

1. You download the latest SANtricity OS software file from the Support site (a link is available from Unified Manager in the **Support** page). Save the file on the management host system (the host where you access Unified Manager in a browser), and then unzip the file.
2. In Unified Manager, you load the SANtricity OS software file and the NVSRAM file into the repository (an area of the Web Services Proxy server where files are stored). You can add files either from **Upgrade Center › Upgrade SANtricity OS Software** or from **Upgrade Center › Manage Software Repository**.
3. After the files are loaded in the repository, you can then select the file to be used in the upgrade. From the Upgrade SANtricity OS software page (**Upgrade Center › Upgrade SANtricity OS software**), you select the SANtricity OS software file and the NVSRAM file. After you select a software file, a list of compatible storage arrays appear on this page. You then select the storage arrays that you want to upgrade with the new software. (You cannot select incompatible arrays.)
4. You can then begin an immediate software transfer and activation, or you can choose to stage the files for activation at a later time. During the upgrade process, Unified Manager performs the following tasks:
   a. Performs a health check on the storage arrays to determine if any conditions exist that might prevent the upgrade from completing. If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.
   b. Transfers the upgrade files to each controller.
   c. Reboots the controllers and activates the new SANtricity OS software, one controller at a time. During

activation, the existing SANtricity OS file is replaced with the new file.

> You can also specify that the software is activated at a later time.

Immediate or staged upgrade

You can activate the upgrade immediately or stage it for a later time. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. Depending on the IO load and cache size, a controller upgrade can typically take between 15 to 25 minutes to complete. The controllers reboot and fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

To activate staged software, go to **Support › Upgrade Center** and click **Activate** in the area labeled SANtricity OS Controller Software upgrade.

Health check

A health check runs as part of the upgrade process, but you can also run a health check separately before you begin (go to **Upgrade Center › Pre-Upgrade Health Check**).

The health check assesses all storage system components to make sure that the upgrade can proceed. The following conditions might prevent the upgrade:

- Failed assigned drives
- Hot spares in use
- Incomplete volume groups
- Exclusive operations running
- Missing volumes
- Controller in Non-optimal status
- Excess number of event log events
- Configuration database validation failure
- Drives with old versions of DACstore

Upgrade considerations

Before you use SANtricity Unified Manager to upgrade multiple storage arrays, review the key considerations as part of your planning.

Current versions

You can view the current SANtricity OS software versions from the Manage page of Unified Manager for each discovered storage array. The version is shown in the SANtricity OS Software column. The controller firmware and NVSRAM information is available in a pop-up dialog box when you click on the SANtricity OS version in each row.

Other components requiring upgrade

As part of the upgrade process, you might also need to upgrade the host's multipath/failover driver or the HBA driver so that the host can interact with the controllers correctly.

For compatibility information, refer to the NetApp Interoperability Matrix. Also, see the procedures in the Express Guides for your operating system. Express Guides are available from the E-Series Documentation Center.

Dual controllers

If a storage array contains two controllers and you have a multipath driver installed, the storage array can continue to process I/O while the upgrade occurs. During the upgrade, the following process occurs:

1. Controller A fails over all its LUNs to controller B.
2. Upgrade occurs on controller A.
3. Controller A takes back its LUNs and all of controller B's LUNs.
4. Upgrade occurs on controller B.

After the upgrade completes, you might need to manually redistribute volumes between the controllers to ensure volumes return to the correct owning controller.

How tos

Perform pre-upgrade health check

A health check runs as part of the upgrade process, but you also can run a health check separately before you begin. The health check assesses components of the storage array to make sure that the upgrade can proceed.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Pre-Upgrade Health Check**.

   The Pre-Upgrade Health Check dialog box opens and lists all the discovered storage systems.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that are not currently in the Optimal state.
3. Select the check boxes for the storage systems that you want to run through the health check.
4. Click **Start**.

   The progress is shown in the dialog box while the health check is performed.

5. When the health check completes, you can click on the ellipses (…) to the right of each row to view more information and perform other tasks.

> If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.

Upgrade SANtricity OS

Upgrade one or more storage arrays with the latest software and NVSRAM to make sure

that you have all the latest features and bug fixes. Controller NVSRAM is a controller file that specifies the default settings for the controllers.

Before you begin

- The latest SANtricity OS files are available on the host system where the SANtricity Web Services Proxy and Unified Manager are running.
- You know whether you want to activate your software upgrade now or later.

  You might choose to activate later for these reasons:

  - **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers fail over during activation, so performance might be lower than usual until the upgrade completes.
  - **Type of package** — You might want to test the new OS software on one storage array before you upgrade the files on other storage arrays.

> **Risk of data loss or risk of damage to the storage array** — Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

Steps

1. If your storage array contains only one controller or you do not have a multipath driver installed, stop I/O activity to the storage array to prevent application errors. If your storage array has two controllers and you have a multipath driver installed, you do not need to stop I/O activity.
2. From the main view, select **Manage**, and then select one or more storage arrays that you want to upgrade.
3. Select **Upgrade Center › Upgrade SANtricity OS Software**.

   The Upgrade SANtricity OS software page appears.

4. Download the latest SANtricity OS software package from the Support site to your local machine.

   a. Click **Add new file to software repository**.

   b. Click the link for finding the latest **SANtricity OS Downloads**.

   c. Click the **Download Latest Release** link.

   d. Follow the remaining instructions to download the SANtricity OS file and the NVSRAM file to your local machine.

   > Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.

5. Select the OS software file and the NVSRAM file that you want to use to upgrade the controllers:

   a. From the **Select a SANtricity OS software file** drop-down, select the OS file that you downloaded to your local machine.

   If there are multiple files available, the files are sorted from newest date to oldest date.

   > The software repository lists all software files associated with the Web Services Proxy. If you do not see the file that you want to use, you can click the link, **Add new file to software repository**, to browse to the location where the OS file that you want to add resides.

b. From the **Select an NVSRAM file** drop-down, select the controller file that you want to use.

   If there are multiple files, the files are sorted from newest date to oldest date.

6. In the Compatible Storage Array table, review the storage arrays that are compatible with the OS software file that you selected, and then select the arrays you want to upgrade.
   - The storage arrays that you selected in the Manage view and that are compatible with the selected firmware file are selected by default in the Compatible Storage Array table.
   - The storage arrays that cannot be updated with the selected firmware file are not selectable in the Compatible Storage Array table as indicated by the status **Incompatible**.
7. **Optional:** To transfer the software file to the storage arrays without activating them, select the **Transfer the OS software to the storage arrays, mark it as staged, and activate at a later time** check box.
8. Click **Start**.
9. Depending on whether you chose to activate now or later, do one of the following:
   - Type **TRANSFER** to confirm that you want to transfer the proposed OS software versions on the arrays you selected to upgrade, and then click **Transfer**.

     To activate the transferred software, select **Upgrade Center › Activate Staged OS Software**.
   - Type **UPGRADE** to confirm that you want to transfer and activate the proposed OS software versions on the arrays you selected to upgrade, and then click **Upgrade**.

     The system transfers the software file to each storage array you selected to upgrade and then activates that file by initiating a reboot.

   The following actions occur during the upgrade operation:

   - A pre-upgrade health check runs as part of the upgrade process. The pre-upgrade health check assesses all storage array components to make sure that the upgrade can proceed.
   - If any health check fails for a storage array, the upgrade stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the upgrade.
   - You can cancel the upgrade operation after the pre-upgrade health check.
10. **Optional:** Once the upgrade has completed, you can see a list of what was upgraded for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

    The file is saved in the Downloads folder for your browser with the name`upgrade_log-<date>.json`.

Activate staged OS software

You can choose to activate the software file immediately or wait until a more convenient time. This procedure assumes you chose to activate the software file at a later time.

About this task

You can transfer the firmware files without activating them. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers reboot and fail over during activation so performance might be lower than usual until

the upgrade completes.

- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

> You cannot stop the activation process after it starts.

Steps

1. From the main view, select **Manage**. If necessary, click the Status column to sort, at the top of the page, all storage arrays with a status of "OS Upgrade (awaiting activation)."
2. Select one or more storage arrays that you want to activate software for, and then select **Upgrade Center › Activate Staged OS Software**.

   The following actions occur during the upgrade operation:

   - A pre-upgrade health check runs as part of the activate process. The pre-upgrade health check assesses all storage array components to make sure that the activation can proceed.
   - If any health check fails for a storage array, the activation stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the activation.
   - You can cancel the activate operation after the pre-upgrade health check. On successful completion of the pre-upgrade health check, activation occurs. The time it takes to activate depends on your storage array configuration and the components that you are activating.
3. **Optional:** After the activation is complete, you can see a list of what was activated for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

   The file is saved in the Downloads folder for your browser with the name `activate_log-<date>.json`.

Manage software repository

The software repository lists all software files associated with the Web Services Proxy. If you do not see the file that you want to use, you can use the Manage Software Repository option to import one or more SANtricity OS files to the host system where the Web Services Proxy and Unified Manager are running. You can also choose to delete one or more SANtricity OS files that are available in the software repository.

Before you begin

- If you are adding SANtricity OS files, make sure that the OS files are available on your local system.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Manage Software Repository**.

   The **Manage Software Repository** dialog appears.

2. Do one of the following actions:

Option	Do this….
Import	a. Click **Import.** b. Click **Browse**, and then navigate to the location where the OS files you want to add reside. OS files have a filename similar to `N2800-830000-000.dlp`. c. Select one or more OS files that you want to add, and then click **Import**.
Delete	a. Select one or more OS files that you want to remove from the software repository. b. Click **Delete**.

If you selected import, the file(s) are uploaded and validated. If you selected delete, the files are removed from the software repository.

Clear staged OS software

You can remove staged OS software to ensure that a pending version is not inadvertently activated at a later time. Removing the staged OS software does not affect the current version that is running on the storage arrays.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Clear Staged OS Software**.

   The Clear Staged OS Software dialog box opens and lists all the discovered storage systems with pending software or NVSRAM.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that have staged software.
3. Select the check boxes for the storage systems with pending software that you want cleared.
4. Click **Clear**.

   The status of the operation is shown in the dialog box.

Mirroring

Concepts

Mirroring overview

Unified Manager includes configuration options for the SANtricity mirroring features, which enable administrators to replicate data between two storage arrays for data protection.

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

Types of mirroring

SANtricity applications include two types of mirroring — asynchronous and synchronous.

Asynchronous mirroring copies data volumes on demand or on a schedule, which minimizes or avoids downtime that might result from data corruption or loss. Asynchronous mirroring captures the state of the primary volume at a particular point in time and copies just the data that has changed since the last image capture. The primary site can be updated immediately and the secondary site can be updated as bandwidth allows. The information is cached and sent later, as network resources become available. This type of mirroring is ideal for periodic processes such as backup and archive.

Synchronous mirroring replicates data volumes in real time to ensure continuous availability. The purpose is to achieve a recovery point objective (RPO) of zero lost data by having a copy of important data available if a disaster happens on one of the two storage arrays. The copy is identical to production data at every moment because each time a write is done to the primary volume, a write is done to the secondary volume. The host does not receive an acknowledgment that the write was successful until the secondary volume is updated with the changes that were made on the primary volume. This type of mirroring is ideal for business continuity purposes such as disaster recovery.

Differences between mirroring types

The following table describes the main differences between the two types of mirroring.

Attribute	Asynchronous	Synchronous
Replication method	Point-in-time — Mirroring is done on demand or automatically according to a user-defined schedule.	Continuous — Mirroring is automatically executed continuously, copying data from every host write.
Distance	Supports long distances between arrays. Typically, the distance is limited only by the capabilities of the network and the channel extension technology.	Restricted to shorter distances between arrays. Typically, the distance must be within about 10 km (6.2 miles) of the local storage array to meet the latency and application performance requirements.
Communication method	A standard IP or Fibre Channel network.	Fibre Channel network only.
Volume types	Standard or thin.	Standard only.

For more information on how mirroring works in SANtricity applications, refer to the online help for System Manager.

Mirroring configuration workflow

You configure asynchronous or synchronous mirroring in Unified Manager, and then use

System Manager to manage synchronizations.

Asynchronous mirroring workflow

Asynchronous mirroring involves the following workflow:

1. Perform the initial configuration in Unified Manager:
   a. Select the local storage array as the source for the data transfer.
   b. Create or select an existing mirror consistency group, which is a container for the primary volume on the local array and the secondary volume on the remote array. The primary and secondary volumes are referred to as the "mirrored pair." If you are creating the mirror consistency group for the first time, you specify whether you want to perform manual or scheduled synchronizations.
   c. Select a primary volume from the local storage array, and then determine its reserved capacity. Reserved capacity is the physical allocated capacity to be used for the copy operation.
   d. Select a remote storage array as the destination of the transfer, a secondary volume, and then determine its reserved capacity.
   e. Begin the initial data transfer from the primary volume to the secondary volume. Depending on the volume size, this initial transfer could take several hours.
2. Check the progress of the initial synchronization:
   a. In Unified Manager, launch System Manager for the local array.
   b. In System Manager, view the status of the mirroring operation. When mirroring is complete, the status of the mirrored pair is "Optimal."
3. **Optional:** You can reschedule or manually perform subsequent data transfers in System Manager. Only new and changed blocks are transferred from the primary volume to the secondary volume.

> Because asynchronous replication is periodic, the system can consolidate the changed blocks and conserve network bandwidth. There is minimal impact on write throughput and write latency.

Synchronous mirroring workflow

Synchronous mirroring involves the following workflow:

1. Perform the initial configuration in Unified Manager:
   a. Select a local storage array as the source for the data transfer.
   b. Select a primary volume from the local storage array.
   c. Select a remote storage array as the destination for the data transfer, and then select a secondary volume.
   d. Select synchronization and resynchronization priorities.
   e. Begin the initial data transfer from the primary volume to the secondary volume. Depending on the volume size, this initial transfer could take several hours.
2. Check the progress of the initial synchronization:
   a. In Unified Manager, launch System Manager for the local array.
   b. In System Manager, view the status of the mirroring operation. When mirroring is complete, the status of the mirrored pair is "Optimal." The two arrays attempt to stay synchronized through normal operations. Only new and changed blocks are transferred from the primary volume to the secondary

volume.

3. **Optional:** You can change synchronization settings in System Manager.

> Because synchronous replication is continuous, the replication link between the two sites must provide sufficient bandwidth capabilities.

Mirroring terminology

Learn how the mirroring terms apply to your storage array.

Term	Description
Local storage array	The local storage array is the storage array that you are acting upon.
Mirror consistency group	A mirror consistency group is a container for one or more mirrored pairs. For asynchronous mirroring operations, you must create a mirror consistency group. All mirrored pairs in a group are resynchronized simultaneously, thus preserving a consistent recovery point. Synchronous mirroring does not use mirror consistency groups.
Mirrored pair	A mirrored pair is comprised of two volumes, a primary volume and a secondary volume. In asynchronous mirroring, a mirrored pair always belongs to a mirror consistency group. Write operations are performed first to the primary volume and then replicated to the secondary volume. Each mirrored pair in a mirror consistency group share the same synchronization settings.
Primary volume	The primary volume of a mirrored pair is the source volume to be mirrored.
Remote storage array	The remote storage array is usually designated as the secondary site, which usually holds a replica of the data in a mirroring configuration.
Reserved capacity	Reserved capacity is the physical allocated capacity that is used for any copy service operation and storage object. It is not directly readable by the host. These volumes are required so that the controller can persistently save information needed to maintain mirroring in an operational state. They contain information such as delta logs and copy-on-write data.

Term	Description
Secondary volume	The secondary volume of a mirrored pair is usually located at a secondary site and holds a replica of the data.
Synchronization	Synchronization occurs at initial synchronization between the local storage array and the remote storage array. Synchronization also occurs when the primary and secondary volumes become unsynchronized after a communication interruption. When the communication link is working again, any unreplicated data is synchronized to the secondary volume's storage array.

Requirements for using mirroring

If you plan to configure mirroring, keep the following requirements in mind.

SANtricity Unified Manager

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Storage arrays

Mirroring is not available on the EF600 storage array.

- You must have two storage arrays.
- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.
- Asynchronous mirroring is supported on controllers with Fibre Channel (FC) or iSCSI host ports, while synchronous mirroring is supported only on controllers with FC host ports.

Connectivity requirements

Mirroring through an FC interface (asynchronous or synchronous) requires the following:

- Each controller of the storage array dedicates its highest numbered FC host port to mirroring operations.

- If the controller has both base FC ports and host interface card (HIC) FC ports, the highest numbered port is on a HIC. Any host logged on to the dedicated port is logged out, and no host login requests are accepted. I/O requests on this port are accepted only from controllers that are participating in mirroring operations.
- The dedicated mirroring ports must be attached to an FC fabric environment that supports the directory service and name service interfaces. In particular, FC-AL and point-to-point are not supported as connectivity options between the controllers that are participating in mirror relationships.

Mirroring through an iSCSI interface (asynchronous only) requires the following:

- Unlike FC, iSCSI does not require a dedicated port. When asynchronous mirroring is used in iSCSI environments, it is not necessary to dedicate any of the storage array's front-end iSCSI ports for use with asynchronous mirroring; those ports are shared for both asynchronous mirror traffic and host-to-array I/O connections.
- The controller maintains a list of remote storage systems with which the iSCSI initiator attempts to establish a session. The first port that successfully establishes an iSCSI connection is used for all subsequent communication with that remote storage array. If communication fails, a new session is attempted using all available ports.
- iSCSI ports are configured at the array level on a port-by-port basis. Intercontroller communication for configuration messaging and data transfer uses the global settings, including settings for:
  - VLAN: Both local and remote systems must have the same VLAN setting to communicate
  - iSCSI listening port
  - Jumbo frames
  - Ethernet priority

> The iSCSI intercontroller communication must use a host connect port and not the management Ethernet port.

Mirrored volume candidates

- RAID level, caching parameters, and segment size can be different on the primary and secondary volumes of a mirrored pair.
- The secondary volume must be at least as large as the primary volume.
- A volume can participate in only one mirror relationship.
- For a synchronous mirrored pair, the primary and secondary volumes must be standard volumes. They cannot be thin volumes or snapshot volumes.
- For synchronous mirroring, there are limits to the number of volumes that are supported on a given storage array. Make sure that the number of configured volumes on your storage array is less than the supported limit. When synchronous mirroring is active, the two reserved capacity volumes that are created count against the volume limit.

Reserved capacity

Asynchronous mirroring:

- A reserved capacity volume is required for a primary volume and for a secondary volume in a mirrored pair for logging write information to recover from controller resets and other temporary interruptions.
- Because both the primary volume and the secondary volume in a mirrored pair require additional reserved capacity, you must ensure that you have free capacity available on both storage arrays in the mirror

relationship.

Synchronous mirroring:

- Reserved capacity is required for a primary volume and for a secondary volume for logging write information to recover from controller resets and other temporary interruptions.
- The reserved capacity volumes are created automatically when synchronous mirroring is activated. Because both the primary volume and the secondary volume in a mirrored pair require reserved capacity, you must ensure that you have enough free capacity available on both storage arrays that are participating in the synchronous mirror relationship.

Drive Security feature

- If you are using secure-capable drives, the primary volume and the secondary volume must have compatible security settings. This restriction is not enforced; therefore, you must verify it yourself.
- If you are using secure-capable drives, the primary volume and the secondary volume should use the same drive type. This restriction is not enforced; therefore, you must verify it yourself.
- If you are using Data Assurance (DA), the primary volume and the secondary volume must have the same DA settings.

How tos

Create asynchronous mirrored pair

To configure asynchronous mirroring, you create a mirrored pair that includes a primary volume on the local array and a secondary volume on the remote array.

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

Before you begin

Before you create a mirrored pair, meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays:

- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.

- Your local and remote storage arrays are connected through a Fibre Channel fabric or iSCSI interface.
- You have created both the primary and secondary volumes that you want to use in the asynchronous mirror relationship.

About this task

The process to create an asynchronous mirrored pair is a multi-step procedure.

Step 1: Create or select a mirror consistency group

You can create a new mirror consistency group or select an existing one.

Before you begin

- To create a new mirror consistency group, the local and remote storage arrays must be discovered in Unified Manager.

About this task

A mirror consistency group is a container for the primary and secondary volumes (the mirrored pair), and specifies the desired resynchronization method (manual or automatic) for all pairs in the group.

Steps

1. From the **Manage** page, select the local storage array that you want to use for the source.
2. Select **Actions › Create Asynchronous Mirrored Pair**.

   The **Create Asynchronous Mirrored Pair** wizard opens.

3. Select either an existing mirror consistency group or create a new one.

   To select an existing group, make sure **An existing mirror consistency group** is selected, and then select the group from the table. A consistency group can include multiple mirrored pairs.

   To create a new group, do the following:

   a. Select **A new mirror consistency group**, and then click **Next**.
   b. Enter a unique name that best describes the data on the volumes that will be mirrored between the two storage arrays. A name can only consist of letters, numbers, and the special characters underscore (_), dash (-), and the hash sign (#). A name may not exceed 30 characters and may not contain spaces.
   c. Select the remote storage array on which you want to establish a mirror relationship with the local storage array.

      If your remote storage array is password protected, the system prompts for a password.

   d. Choose whether you want to synchronize the mirrored pairs manually or automatically:
      - **Manual** — Select this option to manually start synchronization for all mirrored pairs within this group. Note that when you want to perform a resynchronization later, you must launch System Manager for the primary storage array, and then go to **Storage › Asynchronous Mirroring**, select the group from the **Mirror Consistency Groups** tab, and then select **More › Manually resynchronize**.
      - **Automatic** — Select the desired interval in **Minutes**, **Hours**, or **Days**, from the beginning of the previous update to the beginning of the next update. For example, if the synchronization interval is set at 30 minutes, and the synchronization process starts at 4:00 p.m., the next process starts at

4:30 p.m.

e. Select the desired alert settings:

   - For manual synchronizations, specify the threshold (defined by the percentage of the capacity remaining) for when you receive alerts.
   - For automatic synchronizations, you can set three methods of alerting: when the synchronization has not completed in a specific length of time, when the recovery point data on the remote array is older than a specific time limit, and when the reserved capacity is nearing a specific threshold (defined by the percentage of the capacity remaining).

4. Select **Next** and go to Step 2: Select the primary volume.

   If you defined a new mirror consistency group, Unified Manager creates the mirror consistency group on the local storage array first and then creates the mirror consistency group on the remote storage array. You can view and manage the mirror consistency group by launching System Manager for each array.

   > If Unified Manager successfully creates the mirror consistency group on the local storage array, but fails to create it on the remote storage array, it automatically deletes the mirror consistency group from the local storage array. If an error occurs while Unified Manager is attempting to delete the mirror consistency group, you must manually delete it.

Step 2: Select the primary volume

Select the primary volume that you want to use in the mirror relationship and allocate its reserved capacity.

Before you begin

- You must have created the primary volume on the local storage array that you want to use in the asynchronous mirror relationship.

About this task

When you select a primary volume on the local storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

Any volumes you add to the mirror consistency group on the local storage array will hold the primary role in the mirror relationship.

Steps

1. From the list of eligible volumes, select a volume that you want to use as the primary volume, and then click **Next** to allocate the reserved capacity.
2. From the list of eligible candidates, select reserved capacity for the primary volume.

   Keep the following guidelines in mind:

   - The default setting for reserved capacity is 20% of the capacity of the base volume, and usually this capacity is sufficient. If you change the percentage, click **Refresh Candidates**.
   - The capacity needed varies, depending on the frequency and size of I/O writes to the primary volume and how long you need to keep the capacity.
   - In general, choose a larger capacity for reserved capacity if one or both of these conditions exist:
     - You intend to keep the mirrored pair for a long period of time.
     - A large percentage of data blocks will change on the primary volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O

activity to the primary volume.

3. Select **Next** and go to Step 3: Select the secondary volume.

Step 3: Select the secondary volume

Select the secondary volume that you want to use in the mirror relationship and allocate its reserved capacity.

Before you begin

- You must have created the secondary volume on the remote storage array that you want to use in the asynchronous mirror relationship.
- The secondary volume must be at least as large as the primary volume.

About this task

When you select a secondary volume on the remote storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

Any volumes you add to the mirror consistency group on the remote storage array will hold the secondary role in the mirror relationship.

Steps

1. From the list of eligible volumes, select a volume that you want to use as the secondary volume in the mirrored pair, and then click **Next** to allocate the reserved capacity.
2. From the list of eligible candidates, select reserved capacity for the secondary volume.

   Keep the following guidelines in mind:

   - The default setting for reserved capacity is 20% of the capacity of the base volume, and usually this capacity is sufficient. If you change the percentage, click **Refresh Candidates**.
   - The capacity needed varies, depending on the frequency and size of I/O writes to the primary volume and how long you need to keep the capacity.
   - In general, choose a larger capacity for reserved capacity if one or both of these conditions exist:
     - You intend to keep the mirrored pair for a long period of time.
     - A large percentage of data blocks will change on the primary volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O activity to the primary volume.
3. Select **Finish** to complete the asynchronous mirroring sequence.

Results

Unified Manager performs the following actions:

- Begins initial synchronization between the local storage array and the remote storage array.
- If the volume being mirrored is a thin volume, only the provisioned blocks (allocated capacity rather than reported capacity) are transferred to the secondary volume during the initial synchronization. This reduces the amount of data that must be transferred to complete the initial synchronization.
- Creates the reserved capacity for the mirrored pair on the local storage array and on the remote storage array.

Create synchronous mirrored pair

To configure synchronous mirroring, you create a mirrored pair that includes a primary volume on the local array and a secondary volume on the remote array.

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

Before you begin

Before you create a mirrored pair, meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays:

- The two storage arrays you plan to use for mirroring are discovered in Unified Manager.
- Each storage array must have two controllers.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- Your local and remote storage arrays are connected through a Fibre Channel fabric.
- You have created both the primary and secondary volumes that you want to use in the synchronous mirror relationship.

About this task

The process to create synchronous mirrored pairs is a multi-step procedure.

Step 1: Select the primary volume

Select the primary volume that you want to use in the synchronous mirror relationship.

Before you begin

- You must have created the primary volume that you want to use in the synchronous mirror relationship.
- The primary volume must be a standard volume. It cannot be a thin volume or a snapshot volume.

About this task

When you select a primary volume on the local storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

The volume you select holds the primary role in the mirror relationship.

Steps

1. From the **Manage** page, select the local storage array that you want to use for the source.
2. Select **Actions › Create Synchronous Mirrored Pair**.

The **Create Synchronous Mirrored Pair** wizard opens.

3. From the list of eligible volumes, select a volume that you want to use as the primary volume in the mirror.
4. Select **Next** and go to Step 2: Select the secondary volume.

Step 2: Select the secondary volume

Select the secondary volume that you want to use in the mirror relationship.

Before you begin

- You must have created the secondary volume that you want to use in the synchronous mirror relationship.
- The secondary volume must be a standard volume. It cannot be a thin volume or a snapshot volume.
- The secondary volume should be at least as large as the primary volume.

About this task

When you select a secondary volume on the remote storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

The volume you select will hold the secondary role in the mirror relationship.

Steps

1. Select the remote storage array on which you want to establish a mirror relationship with the local storage array.

   If your remote storage array is password protected, the system prompts for a password.

   - Storage arrays are listed by their storage array name. If you have not named a storage array, it will be listed as "unnamed."
   - If the storage array you want to use is not in the list, make sure it has been discovered in Unified Manager.
2. From the list of eligible volumes, select a volume that you want to use as the secondary volume in the mirror.

   If a secondary volume is chosen with a capacity that is larger than the primary volume, the usable capacity is restricted to the size of the primary volume.

3. Click **Next** and go to Step 3: Select synchronization settings.

Step 3: Select synchronization settings

Select the settings that determine how data is synchronized after a communication interruption.

About this task

You can set the priority at which the controller owner of the primary volume resynchronizes data with the secondary volume after a communication interruption. You must also select the resynchronization policy, either manual or automatic.

Steps

1. Use the slider bar to set the synchronization priority.

   The synchronization priority determines how much of the system resources are used to complete initial

synchronization and the resynchronization operation after a communication interruption as compared to service I/O requests.

The priority set on this dialog applies to both the primary volume and the secondary volume. You can modify the rate on the primary volume at a later time by going to System Manager and selecting **Storage › Synchronous Mirroring › More › Edit Settings**.

There are five synchronization priority rates:

- Lowest
- Low
- Medium
- High
- Highest If the synchronization priority is set to the lowest rate, I/O activity is prioritized, and the resynchronization operation takes longer. If the synchronization priority is set to the highest rate, the resynchronization operation is prioritized, but I/O activity for the storage array might be affected.

2. Choose whether you want to resynchronize the mirrored pairs on the remote storage array either manually or automatically.
   - **Manual**(the recommended option) — Select this option to require synchronization to be manually resumed after communication is restored to a mirrored pair. This option provides the best opportunity for recovering data.
   - **Automatic** — Select this option to start resynchronization automatically after communication is restored to a mirrored pair. To manually resume synchronization, go to System Manager and select **Storage › Synchronous Mirroring**, highlight the mirrored pair in the table, and select **Resume** under **More**.
3. Click **Finish** to complete the synchronous mirroring sequence.

Results

Once mirroring is activated, the system performs the following actions:

- Begins initial synchronization between the local storage array and the remote storage array.
- Sets the synchronization priority and resynchronization policy.
- Reserves the highest-numbered port of the controller's HIC for mirror data transmission.

  I/O requests received on this port are accepted only from the remote preferred controller owner of the secondary volume in the mirrored pair. (Reservations on the primary volume are allowed.)

- Creates two reserved capacity volumes, one for each controller, which are used for logging write information to recover from controller resets and other temporary interruptions.

  The capacity of each volume is 128 MiB. However, if the volumes are placed in a pool, 4 GiB will be reserved for each volume.

After you finish

Go to System Manager and select **Home › View Operations in Progress** to view the progress of the synchronous mirroring operation. This operation can be lengthy and could affect system performance.

FAQs

What do I need to know before creating a mirror consistency group?

Follow these guidelines before you create a mirror consistency group.

Meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays:

- The two storage arrays must be discovered in Unified Manager.
- Each storage array must have two controllers.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- Your local and remote storage arrays are connected through a Fibre Channel fabric or iSCSI interface.

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

What do I need to know before creating a mirrored pair?

Before creating a mirrored pair, follow these guidelines.

- You must have two storage arrays.
- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.
- Asynchronous mirroring is supported on controllers with Fibre Channel (FC) or iSCSI host ports, while synchronous mirroring is supported only on controllers with FC host ports.

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

Why would I change this percentage?

Reserved capacity is typically 20 percent of the base volume for asynchronous mirroring operations. Usually this capacity is sufficient.

The capacity needed varies, depending on the frequency and size of I/O writes to the base volume and how long you intend to use the storage object's copy service operation. In general, choose a larger percentage for reserved capacity if one or both of these conditions exist:

- If the lifespan of a particular storage object's copy service operation will be very long.
- If a large percentage of data blocks will change on the base volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O activity to the base volume.

Why do I see more than one reserved capacity candidate?

If there is more than one volume in a pool or volume group that meets the capacity percentage amount you selected for the storage object, then you will see multiple candidates.

You can refresh the list of recommended candidates by changing the percentage of physical drive space that you want to reserve on the base volume for copy service operations. The best candidates are displayed based on your selection.

Why don't I see all my volumes?

When you are selecting a primary volume for a mirrored pair, a list shows all the eligible volumes.

Any volumes that are not eligible to be used do not display in that list. Volumes might not be eligible for any of the following reasons:

- The volume is not optimal.
- The volume is already participating in a mirroring relationship.
- For synchronous mirroring, the primary and secondary volumes in a mirrored pair must be standard volumes. They cannot be thin volumes or snapshot volumes.
- For asynchronous mirroring, thin volumes must have auto-expansion enabled.

Why don't I see all the volumes on the remote storage array?

When you are selecting a secondary volume on the remote storage array, a list shows all the eligible volumes for that mirrored pair.

Any volumes that are not eligible to be used, do not display in that list. Volumes may not be eligible for any of the following reasons:

- The volume is a non-standard volume, such as a snapshot volume.
- The volume is not optimal.
- The volume is already participating in a mirroring relationship.

- For asynchronous mirroring, the thin volume attributes between the primary volume and the secondary volume do not match.
- If you are using Data Assurance (DA), the primary volume and the secondary volume must have the same DA settings.
  - If the primary volume is DA enabled, the secondary volume must be DA enabled.
  - If the primary volume is not DA enabled, the secondary volume must not be DA enabled.

What impact does synchronization priority have on synchronization rates?

The synchronization priority defines how much processing time is allocated for synchronization activities relative to system performance.

The controller owner of the primary volume performs this operation in the background. At the same time, the controller owner processes local I/O writes to the primary volume and associated remote writes to the secondary volume. Because the resynchronization diverts controller processing resources from I/O activity, resynchronization can have a performance impact to the host application.

Keep these guidelines in mind to help you determine how long a synchronization priority might take and how the synchronization priorities can affect system performance.

These priority rates are available:

- Lowest
- Low
- Medium
- High
- Highest

The lowest priority rate supports system performance, but the resynchronization takes longer. The highest priority rate supports resynchronization, but system performance might be compromised.

These guidelines roughly approximate the differences between the priorities.

Priority rate for full synchronization	Time elapsed compared to highest synchronization rate
Lowest	Approximately eight times as long as at the highest priority rate.
Low	Approximately six times as long as at the highest priority rate.
Medium	Approximately three-and-a-half times as long as at the highest priority rate.
High	Approximately twice as long as at the highest priority rate.

Volume size and host I/O rate loads affect the synchronization time comparisons.

Why is it recommended to use a manual synchronization policy?

Manual resynchronization is recommended because it lets you manage the resynchronization process in a way that provides the best opportunity for recovering data.

If you use an Automatic resynchronization policy and intermittent communication problems occur during resynchronization, data on the secondary volume could be temporarily corrupted. When resynchronization is complete, the data is corrected.