Support

SANtricity 11.5

NetApp
August 29, 2024

Table of Contents

Support

Support center

Concepts

AutoSupport feature overview

The AutoSupport feature monitors the health of a storage array and sends automatic dispatches to technical support.

Technical support uses the AutoSupport data reactively to speed the diagnosis and resolution of customer issues and proactively to detect and avoid potential issues.

AutoSupport data includes information about a storage array’s configuration, status, performance, and system events. The AutoSupport data does not contain any user data. Dispatches are sent daily and weekly.

Key benefits

Some key benefits of the AutoSupport feature include:

- Expedited case resolution times
- Sophisticated monitoring for faster incident management
- Automated reporting according to a schedule that you set up, as well as automated reporting about critical events
- Automated hardware replacement requests for selected components such as drives
- Nonintrusive alerting to notify you of a problem and provide information for technical support to take corrective action
- AutoSupport analysis tools that monitor dispatches for known configuration issues

Individual AutoSupport features

The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

Difference between AutoSupport and Collect Support Data

Two methods of collecting support data exist in the storage array:

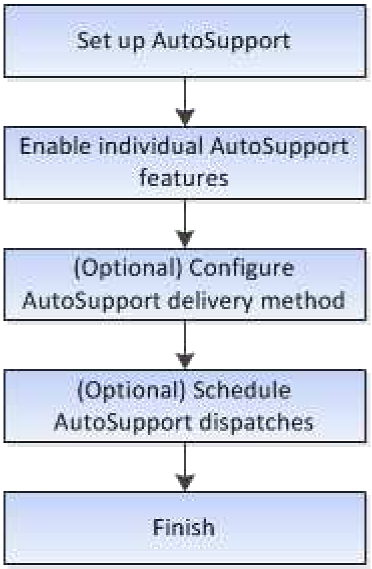
- The AutoSupport feature
- The Collect Support Data option

With the AutoSupport feature, data is automatically collected. With the Collect Support Data option, you collect the data manually. With the AutoSupport feature, data is automatically sent to technical support. With Collect Support Data, you manually send the data to technical support.

The AutoSupport feature is easier to use because data is collected and sent automatically. AutoSupport data can be used proactively to prevent problems before they occur. The AutoSupport feature speeds troubleshooting because technical support already has access to the data. For these reasons, the AutoSupport feature is the preferred data collection method to use.

Workflow for the AutoSupport feature

In SANtricity System Manager, you configure the AutoSupport feature by following these steps.


Set up AutoSupport
Enable individual AutoSupport features
(Optional) Configure AutoSupport delivery method
(Optional) Schedule AutoSupport dispatches
Finish

How tos

View storage array information

View storage array profile

The storage array profile provides a description of all of the components and properties of the storage array.

About this task

You can use the storage array profile as an aid during recovery or as an overview of the current configuration of the storage array. You might want to save a copy of the storage array profile on the management client and keep a hard copy of the storage array profile with the storage array. Create a new copy of the storage array profile if your configuration changes.

Steps

1. Select **Support › Support Center › Support Resources** tab.

2. Scroll down to **Launch detailed storage array information**, and then select **Storage Array Profile**.

   The report appears on your screen.

Field details

Section	Description
Storage Array	Shows all of the options that you can configure and the system static options for your storage array. These options include the number of controllers, drive shelves, drives, disk pools, volume groups, volumes, and hot spare drives; the maximum number of drive shelves, drives, Solid State Disks (SSDs), and volumes allowed; the number of snapshot groups, snapshot images, snapshot volumes and consistency groups; information about features; information about firmware versions; information about the chassis serial number; AutoSupport status and AutoSupport schedule information;the settings for automatic support data collection and scheduled support data collection; the storage array World-Wide Identifier (WWID); and the media scan and cache settings.
Storage	Shows a list of all of the storage devices in the storage array. Depending on your storage array configuration, the Storage section might show these sub-sections. • **Disk Pools** — Shows a list of all of the disk pools in the storage array. • **Volume Groups** — Shows a list of all of the volume groups in the storage array. Volumes and free capacity are listed in the order in which they were created. • **Volumes** — Shows a list of all of the volumes in the storage array. The information listed includes the volume name, the volume status, the capacity, the RAID level, the volume group or disk pool, the drive type, and additional details. • **Missing Volumes** — Shows a list of all of the volumes in the storage array that currently have a missing status. The information listed includes the World Wide Identifier (WWID) for each missing volume.

Section	Description
Copy Services	Shows a list of all the copy services that are used for the storage array. Depending on your storage array configuration, the Copy Services section might show these sub-sections: • **Volume Copies** — Shows a list of all copy pairs in the storage array. The information listed includes the number of copies, the copy pair names, the status, the start timestamp, and additional details. • **Snapshot Groups** — Shows a list of all snapshot groups in the storage array. • **Snapshot Images** — Shows a list of all snapshots in the storage array. • **Snapshot Volumes** — Shows a list of all snapshot volumes in the storage array. • **Consistency Groups** — Shows a list of all consistency groups in the storage array. • **Member Volumes** — Shows a list of all consistency group member volumes in the storage array. • **Mirror Groups** — Shows a list of all mirrored volumes. • **Reserved Capacity** — Shows a list of all reserved capacity volumes in the storage array.
Host Assignments	Shows a list of host assignments in the storage array. The information listed includes the volume name, logical unit number (LUN), controller ID, host name or host cluster name, and volume status. Additional information listed includes topology definitions and host type definitions.

Section	Description
Hardware	Shows a list of all of the hardware in the storage array. Depending on your storage array configuration, the Hardware section might show these sub-sections. • **Controllers** — Shows a list of all of the controllers in the storage array and includes the controller location, status, and configuration. In addition, it includes drive channel information, host channel information, and Ethernet port information. • **Drives** — Shows a list of all of the drives in the storage array. The drives are listed in shelf ID, drawer ID, slot ID order. The information listed includes the shelf ID, the drawer ID, the slot ID, the status, the raw capacity, the media type, the interface type, the current data rate, the product ID, and the firmware version for each drive. The Drive section also includes drive channel information, hot spare coverage information, and wear life information (only for SSD drives). The wear life information includes the percent endurance used, which is the amount of data written to the SSD drives to date, divided by the total theoretical write limit for the drives. • **Drive Channels** — Shows information for all of the drive channels in the storage array. The information listed includes the channel status, the link status (if applicable), drive counts, and cumulative error counts. • **Shelves** — Shows information for all of the shelves in the storage array. The information listed includes drive types, and status information for each component of the shelf. Shelf components might include battery packs, Small Form-factor Pluggable (SFP) transceivers, power-fan canisters, or input/output module (IOM) canisters. The Hardware section also shows the security key identifier if a security key is used by the storage array.

Section	Description
Features	Shows a list of the feature packs installed and maximum allowed number of snapshot groups, snapshots (legacy), and volumes per host or host cluster. The information in the Features section also includes Drive Security; that is, whether the storage array is security enabled or security disabled.

3. To search the storage array profile, type a search term in the **Find** text box, and then click **Find**.

   All matching terms are highlighted. To scroll through all the results one at a time, continue to click **Find**.

4. To save the storage array profile, click **Save**.

   The file is saved in the Downloads folder for your browser with the name `storage-array-profile.txt`.

View software and firmware inventory

The software and firmware inventory lists the firmware versions for each component in your storage array.

About this task

A storage array is made up of many components, which might include controllers, drives, drawers, and input/output modules (IOMs). Each of these components contains firmware. Some versions of firmware depend on other versions of firmware. To capture information about all of the firmware versions in your storage array, view the software and firmware inventory. Technical support can analyze the software and firmware inventory to detect any firmware mismatches.

Steps

1. Select **Support › Support Center › Support Resources** tab.
2. Scroll down to **Launch detailed storage array information**, and then select **Software and Firmware Inventory**.

   The software and firmware inventory report appears on the screen.

3. To save the software and firmware inventory, click **Save**.

   The file is saved in the Downloads folder for your browser with the filename `firmware-inventory.txt`.

4. Follow the instructions provided by technical support to send the file to them.

Collect diagnostic data

Collect support data manually

You can gather various types of inventory, status, and performance data about your storage array in a single file. Technical support can use the file for troubleshooting and further analysis.

About this task

You can run only one collection operation at a time. If you try to start another operation, you receive an error message.

> Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Collect Support Data**.
3. Click **Collect**.

   The file is saved in the Downloads folder for your browser with the name `support-data.7z`. If your shelf contains drawers, the diagnostic data for that shelf is archived in a separate zipped file named `tray-component-state-capture.7z`.

4. Follow the instructions provided by technical support to send the file to them.

Retrieve recovery support files

Technical support can use recovery support files to troubleshoot issues. System Manager automatically saves these files.

Before you begin

Technical support has requested that you send them additional files for troubleshooting.

About this task

Recovery support files include these types of files:

- Support data files
- AutoSupport history
- AutoSupport log
- SAS/RLS diagnostics files
- Recovery profile data
- Database capture files

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Retrieve Recovery Support Files**.

   A dialog box lists all the recovery support files that your storage array has collected. To find particular files, you can sort any of the columns or type characters in the **Filter** box.

3. Select a file, and then click **Download**.

   The file is saved in the Downloads folder for your browser.

4. If you need to save additional files, repeat the previous step.

5. Click **Close**.
6. Follow the instructions provided by technical support to send the file to them.

Retrieve trace buffers

You can retrieve the trace buffers from the controllers and send the file to technical support for analysis.

About this task

The firmware uses the trace buffers to record processing, especially exception conditions, that might be useful for debugging. You can retrieve trace buffers without interrupting the operation of the storage array and with minimal effect on performance.

ⓘ Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Retrieve Trace Buffers**.
3. Select the check box next to each controller for which you want to retrieve trace buffers.

   You can select one or both controllers. If the controller status message to the right of a check box is Failed or Disabled, the check box is disabled.

4. Click **Yes**.

   The file is saved in the Downloads folder for your browser with the filename `trace-buffers.7z`.

5. Follow the instructions provided by technical support to send the file to them.

Collect drive data

You can collect log data from all drives in your storage array and send the file to technical support for analysis.

About this task

Log data consists of statistical information that is maintained by each of the drives in your storage array. Technical support can use this information to analyze the performance of your drives and for troubleshooting problems that might exist.

ⓘ Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Collect Drive Data**.

   A dialog box appears listing all drives in your storage array.

3. In the first column of the table, you can either select individual drives for which you want to collect data (click the check box next to each drive) or select all drives (select the check box in the table header).

To find particular drives, you can sort any of the columns or type characters in the **Filter** box.

4. Click **Collect**.

   The file is saved in the Downloads folder for your browser with the name `drive-data.7z`.

5. Follow the instructions provided by technical support to send the file to them.

Collect I/O path statistics

You can save the I/O path statistics file and send it to technical support for analysis.

About this task

Technical support uses the I/O path statistics to help diagnose performance issues. Application performance issues can be caused by memory utilization, CPU utilization, network latency, I/O latency, or other issues. The I/O path statistics are collected automatically during support data collection or you can collect them manually. In addition, if you have AutoSupport turned on, the I/O path statistics are automatically collected and sent to technical support.

The counters for the I/O path statistics are reset after you confirm that you want to collect the I/O path statistics. The counters are reset even if you subsequently cancel the operation. The counters are also reset when the controller resets (reboots).

ⓘ Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Collect I/O Path Statistics**.
3. Confirm that you want to perform the operation by typing `collect`, and then click **Collect**.

   The file is saved in the Downloads folder for your browser with the filename `io-path-statistics.7z`.

4. Follow the instructions provided by technical support to send the file to them.

Retrieve health image

You can review a health image for the controller. A health image is a raw data dump of the controller’s processor memory that technical support can use to diagnose a problem with a controller.

About this task

The firmware automatically generates a health image when it detects certain errors. After a health image is generated, the controller that had the error reboots and an event is logged in the event log.

If you have AutoSupport turned on, the health image is automatically sent to technical support. If you do not have AutoSupport turned on, you need to contact technical support for instructions on retrieving the health image and sending it to them for analysis.

ⓘ Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Retrieve Health Image**.

   You can look at the details section to see the size of the health image before downloading the file.

3. Click **Collect**.

   The file is saved in the Downloads folder for your browser with the name `health-image.7z`.

4. Follow the instructions provided by technical support to send the file to them.

Take recovery action on storage array status

View unreadable sectors log

You can save the unreadable sectors log and send the file to technical support for analysis.

About this task

The unreadable sectors log contains detailed records of unreadable sectors caused by drives reporting unrecoverable media errors. Unreadable sectors are detected during normal I/O and during modification operations, such as reconstructions. When unreadable sectors are detected on a storage array, a Needs Attention alert appears for the storage array. The Recovery Guru distinguishes which unreadable sector condition needs attention. Any data contained in an unreadable sector cannot be recovered and should be considered lost.

The unreadable sectors log can store up to 1,000 unreadable sectors. When the unreadable sectors log reaches 1,000 entries, the following conditions apply:

- If new unreadable sectors are detected during reconstruction, the reconstruction fails, and no entry is logged.
- For new unreadable sectors detected during I/O, the I/O fails, and no entry is logged.

> ⓘ These actions include RAID 5 writes and RAID 6 writes that would have succeeded before the overflow.

> ! **Possible loss of data** — Recovery from unreadable sectors is a complicated procedure that can involve several different methods. Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View/Clear Unreadable Sectors**.
3. To save the unreadable sectors log:

   a. In the first column of the table, you can either select individual volumes for which you want to save the unreadable sectors log (click the check box next to each volume) or select all volumes (select the check box in the table header).

      To find particular volumes, you can sort any of the columns or type characters in the **Filter** box.

   b. Click **Save**.

   The file is saved in the Downloads folder for your browser with the name `unreadable-sectors.txt`.

4. If technical support instructs you to clear the unreadable sectors log, perform the following steps:
   a. In the first column of the table, you can either select individual volumes for which you want to clear the unreadable sectors log (click the check box next to each volume) or select all volumes (select the check box in the table header).
   b. Click **Clear**, and confirm that you want to perform the operation.

View NVMe over InfiniBand statistics packages

You can view data about the NVMe over InfiniBand connections to your storage array.

About this task

System Manager shows these types of NVMe over InfiniBand statistics. All statistics are read-only and cannot be set.

- **NVMe Controller statistics** — Provides statistics for the NVMe controller, including timeouts and connection failures.
- **NVMe Queue statistics** — Provides statistics for the NVMe queue, including connection requests and command status.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

You can access NVMe over InfiniBand statistics from the System page (**Settings › System**) or from the Support page. These instructions describe how to access the statistics from the Support page.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View NVMe over InfiniBand Statistics Packages**.
3. To set the baseline, click **Set new baseline**.

   Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all NVMe statistics.

Re-enable drive ports

You can indicate to the controller that corrective action has been taken to recover from a mis-wire condition.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Re-enable Drive Ports**, and confirm that you want to perform the operation.

   This option appears only when the storage array has disabled drive ports.

   The controller re-enables any SAS ports that were disabled when a mis-wire was detected.

Clear recovery mode

After restoring a storage array configuration, use the Clear Recovery Mode operation to resume I/O on the storage array and return it to normal operations.

Before you begin

- If you want to return the storage array to a previous configuration, you must restore the configuration from the backup before clearing recovery mode.
- You must perform validation checks or check with technical support to make sure that the restore was successful. After determining that the restore was successful, recovery mode can be cleared.

About this task

The storage array contains a configuration database that includes a record of its logical configuration (pools, volume groups, volumes, and so on). If you intentionally clear the storage array configuration or if the configuration database gets corrupted, the storage array enters recovery mode. Recovery mode stops I/O and freezes the configuration database, which gives you time to do one of the following:

- Restore the configuration from the automatic backup that is stored in the controller’s flash devices. You must contact technical support to do this.
- Restore the configuration from a previous Save Configuration Database operation. Save Configuration Database operations are performed through the command line interface (CLI).
- Reconfigure the storage array from scratch.

After the storage array configuration has been restored or redefined and you have verified that all is well, you must manually clear recovery mode.

> You cannot cancel the Clear Recovery Mode operation after it starts. Clearing recovery mode can take a long time. Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **Clear Recovery Mode**, and confirm that you want to perform this operation.

   This option appears only if the storage array is in recovery mode.

Manage iSCSI connections

View iSCSI statistics packages

You can view data about the iSCSI connections to your storage array.

About this task

System Manager shows these types of iSCSI statistics. All statistics are read-only and cannot be set.

- **Ethernet MAC statistics** — Provides statistics for the media access control (MAC). MAC also provides an addressing mechanism called the physical address or the MAC address. The MAC address is a unique address that is assigned to each network adapter. The MAC address helps deliver data packets to a destination within the subnetwork.
- **Ethernet TCP/IP statistics** — Provides statistics for the TCP/IP, which is the Transmission Control Protocol (TCP) and Internet Protocol (IP) for the iSCSI device. With TCP, applications on networked hosts

can create connections to one another, over which they can exchange data in packets. The IP is a data-oriented protocol that communicates data across a packet-switched inter-network. The IPv4 statistics and the IPv6 statistics are shown separately.

- **Local Target/Initiator (Protocol) statistics** — Shows statistics for the iSCSI target, which provides block level access to its storage media, and shows the iSCSI statistics for the storage array when used as an initiator in asynchronous mirroring operations.
- **DCBX Operational States statistics** — Displays the operational states of the various Data Center Bridging Exchange (DCBX) features.
- **LLDP TLV statistics** — Displays the Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) statistics.
- **DCBX TLV statistics** — Displays the information that identifies the storage array host ports in a Data Center Bridging (DCB) environment. This information is shared with network peers for identification and capability purposes.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View iSCSI Statistics Packages**.
3. Click a tab to view the different sets of statistics.
4. To set the baseline, click **Set new baseline**.

   Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all iSCSI statistics.

View the different types of iSCSI statistics

You can review different sets of statistics as either raw or baseline statistics: Ethernet MAC statistics, Ethernet TCP/IP statistics, Target (protocol) statistics, Local initiator (protocol) statistics, DCBX operational state statistics, LLDP TLV statistics, and DCBX TLV statistics.

MAC transmit and MAC receive statistics

When you select Ethernet MAC statistics, these MAC transmit statistics appear. You can view each of these statistics as raw statistics or as baseline statistics.

Statistic	Definition
F	Frame count
B	Byte count
MF	Multicast frame count
BF	Broadcast frame count

Statistic	Definition
PF	Pause frame count
CF	Control frame count
FDF	Frame deferral count
FED	Frame excess deferral count
FLC	Frame late collisions count
FA	Frame abort count
FSC	Frame single collision count
FMC	Frame multiple collisions count
FC	Frame collision count
FDR	Frame dropped count
JF	Jumbo frame count

When you select Ethernet MAC statistics, these MAC receive statistics appear.

Statistic	Definition
F	Frame count
B	Byte count
MF	Multicast frame count
BF	Broadcast frame count
PF	Pause frame count
CF	Control frame count
FLE	Frame length error count
FD	Frame dropped count
FCRCE	Frame CRC error count

Statistic	Definition
FEE	Frame encoding error count
LFE	Large frame error count
SFE	Small frame error count
J	Jabber count
UCC	Unknown control frame count
CSE	Carrier sense error count

Ethernet TCP/IP statistics

When you select Ethernet TCP/IP statistics, the TCP statistics in this table appear. You can view each of these statistics as raw statistics or as baseline statistics.

Statistic	Definition
TxS	Transmitted segment count
TxB	Transmitted byte count
RTxTE	Retransmit timer expired count
TxDACK	Transmit delayed ACK count
TxACK	Transmit ACK count
RxS	Received segment count
RxB	Received byte count
RxDACK	Received duplicate ACK count
RxACK	Received ACK count
RxSEC	Received segment error count
RxSOOC	Received segment out-of-order count
RxWP	Received window probe count
RxWU	Received window update count

When you select Ethernet TCP/IP statistics, the IP statistics in this table appear.

Statistic	Definition
TxP	Transmitted packet count
TxB	Transmitted byte count
TxF	Transmitted fragment count
RxP	Packets received count. Select **Show IPv4** to show the IPv4 packets received count. Select **Show IPv6** to show the IPv6 packets received count.
RxB	Received byte count
RxF	Received fragment count
RxPE	Received packet error count
DR	Datagram reassembly count
DRE-OLFC	Datagram reassembly error, overlapped fragment count
DRE-OOFC	Datagram reassembly error, out-of-order fragment count
DRE-TOC	Datagram reassembly error, time-out count

iSCSI target statistics and local initiator statistics

When you select Target (protocol) statistics or Local initiator (protocol) statistics, the following statistics are shown. You can view each of these statistics as raw statistics or as baseline statistics.

Statistic	Definition
SL	Successful iSCSI login count
UL	Unsuccessful iSCSI login count
SA	Successful iSCSI authentication count (when authentication is enabled)
UA	Unsuccessful iSCSI authentication count (when authentication is enabled)

Statistic	Definition
PDU	Correct iSCSI PDUs processed count
HDE	iSCSI PDUs with header digest errors count
DDE	iSCSI PDUs with data digest errors count
PE	PDUs with iSCSI protocol errors count
UST	Unexpected iSCSI session terminations count
UCT	Unexpected iSCSI connection termination count

DCBX operational state statistics

When you select Data Center Bridging Exchange (DCBX) Operational State Statistics, these statistics appear.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.
Priority Group	Indicates the operational state of the Priority Group (PG) application. The state is either Enabled or Disabled.
Priority-based Flow Control	Indicates the operational state of the Priority-based Flow Control (PFC) feature. The state is either Enabled or Disabled.
iSCSI Feature	Indicates the operational state of the Internet Small Computer System Interface (iSCSI) application. The state is either Enabled or Disabled.
FCoE Bandwidth	Indicates the state of the Fibre Channel over Ethernet (FCoE) Bandwidth. The state is either True or False.
No FCoE/FIP Map Mismatch	Indicates whether a map mismatch exists between FCoE and FCoE Initialization Protocol (FIP). The value is either True or False.

You can find additional DCBX operational state statistics in the state capture file.

LLDP TLV statistics

When you select Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) Statistics, these statistics appear. Two sets of statistics appear: one for the local device and one for the remote device. The local device refers to the controller. The remote device refers to the peer device that the controller is attached to, typically a switch.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.
Chassis ID	Indicates the chassis ID.
Chassis ID Subtype	Indicates the chassis ID subtype.
Port ID	Indicates the port ID.
Port ID Subtype	Indicates the port ID subtype.
Time to Live	Indicates the number of seconds that the recipient LLDP agent considers the information to be valid.

You can find additional LLDP TLV statistics in the state capture file.

DCBX TLV statistics

When you select Data Center Bridging Exchange (DCBX) Type Length Value (TLV) Statistics, these statistics appear:

- **Local statistics** — The DCBX parameters configured on the controller at the factory.
- **Operational statistics** — The DCBX parameters that result from DCBX negotiations.
- **Remote statistics** — The DCBX parameters from the peer device that the controller is connected to, typically a switch.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.
Flow Control Mode	The Flow Control Mode of the entire port. Valid values are Disabled, Standard, Per Priority, or Indeterminate.
Protocol	The communication protocol. Valid values are FCoE, FIP, iSCSI, or UNKNOWN.
Priority	Integer value indicating the priority number of the communication.
Priority Group	Integer value representing the priority group to which the protocol has been assigned.

Statistic	Definition
Priority Group % Bandwidth	Percentage value indicating the amount of bandwidth allocated to the priority group.
DCBX PFC Status	Priority-based Flow Control (PFC) status of the specific port. The value is either enabled or disabled.

You can find additional DCBX TLV statistics in the state capture file.

View iSCSI sessions

You can view detailed information about the iSCSI connections to your storage array. iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View/End iSCSI Sessions**.

   A list of the current iSCSI sessions appears.

3. To see additional information about a specific iSCSI session, select a session, and then click **View Details**.

Field Details

Item	Description
Session Identifier (SSID)	A hexadecimal string that identifies a session between an iSCSI initiator and an iSCSI target. The SSID is composed of the ISID and the TPGT.
Initiator Session ID (ISID)	The initiator part of the session identifier. The initiator specifies the ISID during login.
Target Portal Group	The iSCSI target.
Target Portal Group Tag (TPGT)	The target part of the session identifier. A 16-bit numerical identifier for an iSCSI target portal group.
Initiator iSCSI name	The worldwide unique name of the initiator.
Initiator iSCSI label	The user label set in System Manager.
Initiator iSCSI alias	A name that also can be associated with an iSCSI node. The alias allows an organization to associate a user-friendly string with the iSCSI name. However, the alias is not a substitute for the iSCSI name. The initiator iSCSI alias only can be set at the host, not in System Manager
Host	A server that sends input and output to the storage array.
Connection ID (CID)	A unique name for a connection within the session between the initiator and the target. The initiator generates this ID and presents it to the target during login requests. The connection ID is also presented during logouts that close connections.
Ethernet port identifier	The controller port associated with the connection.
Initiator IP address	The IP address of the initiator.
Negotiated login parameters	The parameters that are transacted during the login of the iSCSI session.

Item	Description
Authentication method	The technique to authenticate users who want access to the iSCSI network. Valid values are **CHAP** and **None**.
Header digest method	The technique to show possible header values for the iSCSI session. HeaderDigest and DataDigest can be either **None** or **CRC32C**. The default value for both is **None**.
Data digest method	The technique to show possible data values for the iSCSI session. HeaderDigest and DataDigest can be either **None** or **CRC32C**. The default value for both is **None**.
Maximum connections	The greatest number of connections allowed for the iSCSI session. The maximum number of connections can be 1 through 4. The default value is **1**.
Target alias	The label associated with the target.
Initiator alias	The label associated with the initiator.
Target IP address	The IP address of the target for the iSCSI session. DNS names are not supported.
Initial R2T	The initial ready to transfer status. The status can be either **Yes** or **No**.
Maximum burst length	The maximum SCSI payload in bytes for this iSCSI session. The maximum burst length can be from 512 to 262,144 (256 KB). The default value is **262,144 (256 KB)**.
First burst length	The SCSI payload in bytes for unsolicited data for this iSCSI session. The first burst length can be from 512 to 131,072 (128 KB). The default value is **65,536 (64 KB)**.
Default time to wait	The minimum number of seconds to wait before you attempt to make a connection after a connection termination or a connection reset. The default time to wait value can be from 0 to 3600. The default is **2**.

Item	Description
Default time to retain	The maximum number of seconds that connection is still possible following a connection termination or a connection reset. The default time to retain can be from 0 to 3600. The default value is **20**.
Maximum outstanding R2T	The maximum number of "ready to transfers" outstanding for this iSCSI session. The maximum outstanding ready to transfer value can be from 1 to 16. The default is **1**.
Error recovery level	The level of error recovery for this iSCSI session. The error recovery level value is always set to **0**.
Maximum receive data segment length	The maximum amount of data that either the initiator or the target can receive in any iSCSI payload data unit (PDU).
Target name	The official name of the target (not the alias). The target name with the *iqn* format.
Initiator name	The official name of the initiator (not the alias). The initiator name that uses either the *iqn* or *eui* format.

4. To save the report to a file, click **Save**.

   The file is saved in the Downloads folder for your browser with the filename `iscsi-session-connections.txt`.

End iSCSI session

You can end an iSCSI session that is no longer needed. iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship.

About this task

You might want to end an iSCSI session for these reasons:

- **Unauthorized access** — If an iSCSI initiator is logged on and should not have access, you can end the iSCSI session to force the iSCSI initiator off the storage array. The iSCSI initiator could have logged on because the None authentication method was available.
- **System downtime** — If you need to take down a storage array and you see that iSCSI initiators are still logged on, you can end the iSCSI sessions to get the iSCSI initiators off the storage array.

Steps

1. Select **Support › Support Center › Diagnostics** tab.

2. Select **View/End iSCSI Sessions**.

   A list of the current iSCSI sessions appears.

3. Select the session that you want to end.
4. Click **End Session**, and confirm that you want to perform the operation.

View iSER over InfiniBand statistics

If your storage array’s controller includes an iSER over InfiniBand port, you can view data about the host connections.

About this task

System Manager shows the following types of iSER over InfiniBand statistics. All statistics are read-only and cannot be set.

- **Local Target (Protocol) statistics** — Provides statistics for the iSER over InfiniBand target, which shows block-level access to its storage media.
- **iSER over InfiniBand Interface statistics** — Provides statistics for all iSER ports on the InfiniBand interface, which includes performance statistics and link error information associated with each switch port.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

You can access iSER over InfiniBand statistics from the System page (**Settings › System**) or from the Support page. These instructions describe how to access the statistics from the Support page.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View iSER over InfiniBand Statistics**.
3. Click a tab to view the different sets of statistics.
4. To set the baseline, click **Set new baseline**.

   Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all iSER over InfiniBand statistics.

Manage NVMe connections

View NVMe over Fabrics statistics

You can view data about the NVMe over Fabrics connections to your storage array.

About this task

System Manager shows these types of NVMe over Fabrics statistics. All statistics are read-only and cannot be set.

- **NVMe Subsystem statistics** — Provides statistics for the NVMe controller, including timeouts and connection failures.
- **RDMA Interface statistics** — Provides statistics for the RDMA interface, including received and

transmitted packet information.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

You can access NVMe over Fabrics statistics from the System page (**Settings › System**) or from the Support page. These instructions describe how to access the statistics from the Support page.

Steps

1. Select **Support › Support Center › Diagnostics** tab.
2. Select **View NVMe over Fabrics Statistics**.
3. To set the baseline, click **Set new baseline**.

   Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all NVMe statistics.

Manage AutoSupport

Enable or disable AutoSupport features

You enable the AutoSupport feature and the individual AutoSupport features during initial setup or you can enable them later.

Before you begin

If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.

About this task

You can disable the AutoSupport feature at any time, but you are strongly advised to leave it enabled. Enabling the AutoSupport feature can significantly speed problem determination and resolution should a problem occur on your storage array.

The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Enable/Disable AutoSupport Features**.
3. Select the check boxes next to the AutoSupport features that you want to enable.

The features depend on each other as indicated by the indentation of the items in the dialog box. For example, you must enable AutoSupport OnDemand before you can enable Remote Diagnostics.

4. Click **Save**.

Enable AutoSupport maintenance window

Enable the AutoSupport maintenance window to suppress automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a case with Support if there is an issue.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Enable AutoSupport Maintenance window**.
3. Enter the email address to receive a confirmation that the maintenance window request has been processed.

   Depending on your configuration, you may be able to enter up to five email addresses. If you want to add more than one address, select **Add another email** to open another field.

4. Specify the duration (in hours) to enable the maintenance window.

   The maximum supported duration is 72 hours.

5. Click **Yes**.

   AutoSupport automatic ticket creation on error events is temporarily suppressed for the specified duration window.

After you finish

The maintenance window does not begin until the storage array’s request is processed by the AutoSupport servers. Wait until you have received a confirmation email before performing any maintenance activities on your storage array.

Disable AutoSupport maintenance window

Disable the AutoSupport maintenance window to allow automatic ticket creation on error events. When AutoSupport maintenance window is disabled, the storage array will use AutoSupport to open a case with Support if there is an issue.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Disable AutoSupport Maintenance window**.
3. Enter the email address to receive a confirmation that the disable maintenance window request has been processed.

   Depending on your configuration, you may be able to enter up to five email addresses. If you want to add more than one address, select **Add another email** to open another field.

4. Click **Yes**.

AutoSupport automatic ticket creation on error events is enabled.

After you finish

The maintenance window will not end until the storage array's request has been processed by the AutoSupport servers. Wait until you have received a confirmation email before proceeding.

Configure AutoSupport delivery method

The AutoSupport feature supports the HTTPS, HTTP, and SMTP protocols for delivering dispatches to technical support.

Before you begin

- The AutoSupport feature is enabled. You can see whether it is enabled on the AutoSupport page.
- A DNS server must be installed and configured in your network. The DNS server address must be configured in System Manager (this task is available from the Hardware page).

About this task

Review the different protocols:

- **HTTPS** — Allows you to connect directly to the destination technical support server using HTTPS. If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.
- **HTTP** — Allows you to connect directly to the destination technical support server using HTTP.
- **Email** — Allows you to use an email server as the delivery method for sending AutoSupport dispatches.

> ⓘ **Differences between the HTTPS/HTTP and Email methods**. The Email delivery method, which uses SMTP, has some important differences from the HTTPs and HTTP delivery methods. First, the size of the dispatches for the Email method are limited to 5MB, which means that some ASUP data collections will not be dispatched. Second, the AutoSupport OnDemand feature is available only on HTPP and HTTPS methods.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Configure AutoSupport Delivery Method**.

   A dialog box appears, which lists the dispatch delivery methods.

3. Select the desired delivery method, and then select the parameters for that delivery method. Do one of the following:
   - If you selected HTTPS or HTTP, select one of the following delivery parameters:
     - **Directly** — This delivery parameter is the default selection. Choosing this option allows you to connect directly to the destination technical support system using the HTTPS or HTTP protocol.
     - **Via Proxy server** — Choosing this option allows you to specify the HTTP proxy server details required for establishing connection with the destination technical support system. You must specify the host address and port number. However, you only need to enter the host authentication details (user name and password) if required.
     - **Via Proxy auto-configuration script (PAC)** — Specify the location of a Proxy Auto-Configuration (PAC) Script file. A PAC file allows the system to automatically choose the appropriate proxy server for establishing a connection with the destination technical support system.

   - If you selected Email, enter the following information:
      - The mail server address as a fully qualified domain name, IPv4 address, or IPv6 address.
      - The email address that appears in the From field of the AutoSupport dispatch email.
      - (Optional; if you want to perform a configuration test.) The email address where a confirmation is sent when the AutoSupport system receives the test dispatch.

4. Click **Test Configuration** to test the connection to the technical support server using the specified delivery parameters. If you enabled the AutoSupport On-Demand feature, the system will also test the connection for AutoSupport OnDemand dispatch delivery.

   If the configuration test fails, check your configuration settings and run the test again. If the test continues to fail, contact technical support.

5. Click **Save**.

Schedule AutoSupport dispatches

System Manager automatically creates a default schedule for AutoSupport dispatches. If you prefer, you can specify your own schedule.

Before you begin

The AutoSupport feature is enabled. You can see whether it is enabled on the AutoSupport page.

About this task

- **Daily time** — Daily dispatches are collected and sent every day during the time range that you specify. System Manager selects a random time during the range. All times are in Coordinated Universal Time (UTC), which might be different from the storage array’s local time. You must convert your storage array’s local time into UTC.
- **Weekly day** — Weekly dispatches are collected and sent once a week. System Manager selects a random day from the days that you specify. Deselect any days on which you do not want to allow a weekly dispatch to occur. System Manager selects a random day from the days that you allow.
- **Weekly time** — Weekly dispatches are collected and sent once a week during the time range that you specify. System Manager selects a random time during the range. All times are in Coordinated Universal Time (UTC), which might be different from the storage array’s local time. You must convert your storage array’s local time into UTC.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Schedule AutoSupport Dispatches**.

   The Schedule AutoSupport Dispatches wizard appears.

3. Follow the steps in the wizard.

View AutoSupport status

The AutoSupport page shows you whether the AutoSupport feature and the individual AutoSupport features are currently enabled.

Steps

1. Select **Support › Support Center › AutoSupport** tab.

2. Look at the right side of the page just below the tabs to see whether the basic AutoSupport feature is enabled.
3. Hover your cursor over the question mark to see whether individual AutoSupport features are enabled.

View AutoSupport log

The AutoSupport log provides information about status, dispatch history, and errors encountered during the delivery of AutoSupport dispatches.

About this task

Multiple log files can exist. When the current log file reaches 200 KB, it is archived and a new log file is created. The archived log file name is ASUPMessages.*n*, where `n` is an integer from 1 to 9. If multiple log files exist, you can choose to view the most current log or a previous log.

- **Current log** — Shows a list of the latest captured events.
- **Archived log** — Shows a list of earlier events.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **View AutoSupport Log**.

   A dialog box appears, which lists the current AutoSupport log.

3. If you want to see previous AutoSupport logs, select the **Archived** radio button, and then select a log from the **Select AutoSupport log** drop-down list.

   The Archived option appears only if archived logs exist on the storage array.

   The selected AutoSupport log appears in the dialog box.

4. **Optional:** To search the AutoSupport log, type a term in the **Find** box, and click **Find**.

   Click **Find** again to search for additional occurrences of the term.

FAQs

What data am I collecting?

The AutoSupport feature and the manual Support Data Collection feature provide ways to collect data in a customer support bundle for remote troubleshooting and problem analysis by technical support.

The customer support bundle gathers all types of information about the storage array into a single compressed file. The information collected includes the physical configuration, logical configuration, version information, events, log files, and performance data. The information is used only by technical support to solve problems with the storage array.

What does unreadable sectors data show me?

You can display detailed data about unreadable sectors detected on the drives in your storage array.

The unreadable sectors log shows the most recent unreadable sector first. The log contains the following information about the volumes that contain the unreadable sectors. The fields are sortable.

Field	Description
Affected Volume	Shows the label of the volume. If a missing volume contains unreadable sectors, the World Wide Identifier appears for the missing volume.
Logical Unit Number (LUN)	Shows the LUN for the volume. If the volume does not have a LUN, the dialog box shows NA.
Assigned To	Shows the hosts or host clusters that have access to the volume. If the volume is not accessible by a host, host cluster, or even a Default Cluster, the dialog box shows NA.

To see additional information about the unreadable sectors, click the plus (+) sign next to a volume.

Field	Description
Date/Time	Shows the date and the time that the unreadable sector was detected.
Volume Logical Block Address	Shows the logical block address (LBA) of the volume.
Drive Location	Shows the drive shelf, drawer (if your drive shelf has drawers), and the bay location.
Drive Logical Block Address	Shows the LBA of the drive.
Failure Type	Shows one of the following failure types: • **Physical** — A physical media error. • **Logical** — A read error elsewhere in the stripe causing unreadable data. For example, an unreadable sector due to media errors elsewhere in the volume. • **Inconsistent** — Inconsistent redundancy data. • **Data Assurance** — A Data Assurance error.

What is a health image?

A health image is a raw data dump of the controller’s processor memory that technical support can use to diagnose a problem with a controller.

The firmware automatically generates a health image when it detects certain errors. Under certain troubleshooting scenarios, technical support might request that you retrieve the health image file and send it to them.

What else do I need to do to configure or diagnose iSCSI?

iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship. The following tables list the System Manager functions that you can use to configure and manage these iSCSI sessions.

ⓘ The iSCSI settings are only available if your storage array supports iSCSI.

Configure iSCSI

Action	Location
Manage iSCSI settings	1. Select **Settings › System**. 2. Scroll down to **iSCSI settings** to view all the management functions.
Configure iSCSI ports	1. Select **Hardware**. 2. Select **Show back of shelf**. 3. Select a controller. 4. Select **Configure iSCSI ports**.
Set the host CHAP secret	1. Select **Settings › System**. 2. Scroll down to **iSCSI settings**, and then select **Configure Authentication**. or 1. Select **Storage › Hosts**. 2. Select a host member. 3. Click **View/Edit Settings › Host Ports** tab.

Diagnose iSCSI

Action	Location
View or end iSCSI sessions	1. Select **Settings › System**. 2. Scroll down to **iSCSI settings**, and then select **View/End iSCSI Sessions**. or 1. Select **Support › Support Center › Diagnostics** tab. 2. Select **View/End iSCSI Sessions**.

Action	Location
View iSCSI statistics	1. Select **Settings › System**. 2. Scroll down to **iSCSI settings**, and then select **View iSCSI Statistics Packages**. or 1. Select **Support › Support Center › Diagnostics** tab. 2. Select **View iSCSI Statistics Packages**.

What do the AutoSupport features do?

The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

What type of data is collected through the AutoSupport feature?

The AutoSupport feature contains three standard dispatch types: event dispatches, scheduled dispatches, and on-demand and remote diagnostics dispatches.

The AutoSupport data does not contain any user data.

- **Event dispatches**

  When events occur on the system that warrant proactive notification to technical support, the AutoSupport feature automatically sends an event-triggered dispatch.

  - Sent when a support event on the managed storage array occurs.
  - Includes a comprehensive snapshot of what was going on with the storage array at the time the event occurred.
- **Scheduled dispatches**

  The AutoSupport feature automatically sends several dispatches on a regular schedule.

  - **Daily dispatches** — Sent once every day during a user-configurable time interval. Includes the current system event logs and performance data.

    - **Weekly dispatches** — Sent once every week during a user-configurable time interval and day. Includes configuration and system state information.

- **AutoSupport OnDemand and Remote Diagnostics dispatches**
    - **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
    - **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

How do I configure the delivery method for the AutoSupport feature?

The AutoSupport feature supports the protocols HTTPS, HTTP, and SMTP for delivering AutoSupport dispatches to technical support.

Before you begin

- The AutoSupport feature is enabled. You can see whether it is enabled on the AutoSupport page.
- A DNS server must be installed and configured in your network. The DNS server address must be configured in System Manager (this task is available from the Hardware page).

About this task

Review the different protocols:

- **HTTPS** — Allows you to connect directly to the destination technical support server using HTTPS. If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.
- **HTTP** — Allows you to connect directly to the destination technical support server using HTTP.
- **Email** — Allows you to use an email server as the delivery method for sending AutoSupport dispatches.

> **Differences between the HTTPS/HTTP and Email methods**. The Email delivery method, which uses SMTP, has some important differences from the HTTPs and HTTP delivery methods. First, the size of the dispatches for the Email method are limited to 5MB, which means that some ASUP data collections will not be dispatched. Second, the AutoSupport OnDemand feature is available only on HTPP and HTTPS methods.

Steps

1. Select **Support › Support Center › AutoSupport** tab.
2. Select **Configure AutoSupport Delivery Method**.

   A dialog box appears, which lists the dispatch delivery methods.

3. Select the desired delivery method, and then select the parameters for that delivery method. Do one of the following:
    - If you selected HTTPS or HTTP, select one of the following delivery parameters:
        - **Directly** — This delivery parameter is the default selection. Choosing this option allows you to connect directly to the destination technical support system using the HTTPS or HTTP protocol.

        - **Via Proxy server** — Choosing this option allows you to specify the HTTP proxy server details required for establishing connection with the destination technical support system. You must specify the host address and port number. However, you only need to enter the host authentication details (user name and password) if required.
        - **Via Proxy auto-configuration script (PAC)** — Specify the location of a Proxy Auto-Configuration (PAC) Script file. A PAC file allows the system to automatically choose the appropriate proxy server for establishing a connection with the destination technical support system.
    - If you selected Email, enter the following information:
        - The mail server address as a fully qualified domain name, IPv4 address, or IPv6 address.
        - The email address that appears in the From field of the AutoSupport dispatch email.
        - (Optional; if you want to perform a configuration test.) The email address where a confirmation is sent when the AutoSupport system receives the test dispatch.
4. Click **Test Configuration** to test the connection to the technical support server using the specified delivery parameters. If you enabled the AutoSupport On-Demand feature, the system will also test the connection for AutoSupport OnDemand dispatch delivery.

    If the configuration test fails, check your configuration settings and run the test again. If the test continues to fail, contact technical support.
5. Click **Save**.

Event log

Concepts

Critical events

Critical events indicate a problem with the storage array. If you resolve the critical event immediately, you might prevent loss of data access.

When a critical event occurs, it is logged in the event log. All critical events are sent to the SNMP management console or to the email recipient that you have configured to receive alert notifications. If the shelf ID is not known at the time of the event, the shelf ID is listed as "Shelf unknown."

When you receive a critical event, refer to the Recovery Guru procedure for a detailed description of the critical event. Complete the Recovery Guru procedure to correct the critical event. To correct certain critical events, you might need to contact technical support.

Event log

The event log provides a historical record of events that have occurred on the storage array and aids technical support in troubleshooting events leading up to failures.

The event log is a detailed record of events that occur in the storage array. It records configuration events and storage array component failures. You can use the event log as a supplementary diagnostic tool to the Recovery Guru for tracing storage array events. Always refer to the Recovery Guru first when you attempt to recover from component failures in the storage array.

The events in the event log are categorized with different statuses. Events that you need to take action on have the following statuses:

- Critical
- Warning

Events that are informational and do not require any immediate action are the following:

- Informational

How tos

View events using the event log

You can view the event log, which provides a historical record of events that have occurred on the storage array.

Steps

1. Select **Support › Event Log**.

   The Event Log page appears.

   Page details

Item	Description
View All field	Toggles between all events, and only the critical and warning events.
Filter field	Filters the events. Useful for displaying only events related to a specific component, a specific event, etc.
Select columns icon.	Allows you to select other columns to view. Other columns give you additional information about the event.
Check boxes	Allows you to select the events to save. The check box in the table header selects all events.
Date/Time column	The date and time stamp of the event, according to the controller clock. ⓘ The event log initially sorts events based on sequence number. Usually, this sequence corresponds to the date and time. However, the two controller clocks in the storage array could be unsynchronized. In this case, some perceived inconsistencies could appear in the event log relative to events and the date and time shown.

Item	Description
Priority column	These priority values exist: • **Critical** — A problem exists with the storage array. However, if you take immediate action, you might prevent losing access to data. Critical events are used for alert notifications. All critical events are sent to any network management client (through SNMP traps) or to the email recipient that you configured. • **Warning** — An error has occurred that has degraded the performance and the ability of the storage array to recover from another error. • **Informational** — Non-critical information related to the storage array.
Component Type column	The component that is affected by the event. The component could be hardware, such as a drive or a controller, or it could be software, such as controller firmware.
Component Location column	The physical location of the component in the storage array.
Description column	A description of the event. **Example** — `Drive write failure - retries exhausted`
Sequence Number column	A 64-bit number that uniquely identifies a specific log entry for a storage array. This number increments by one with every new event log entry. To display this information, click the **Select columns** icon.
Event Type column	A 4-digit number that identifies each type of logged event. To display this information, click the **Select columns** icon.
Event Specific Codes column	This information is used by technical support. To display this information, click the **Select columns** icon.

Item	Description
Event Category column	• **Failure** – A component in the storage array has failed; for example, drive failure or battery failure. • **State Change** – An element of the storage array that has changed state; for example, a volume transitioned to Optimal status, or a controller transitioned to Offline status. • **Internal** – Internal controller operations that do not require user action; for example, the controller has completed start-of-day. • **Command** – A command that has been issued to the storage array; for example, a hot spare has been assigned. • **Error** – An error condition has been detected on the storage array; for example, a controller is unable to synchronize and purge cache, or a redundancy error is detected on the storage array. • **General** – Any event that does not fit well into any other category. To display this information, click the **Select columns** icon.
Logged By column	The name of the controller that logged the event. To display this information, click the **Select columns** icon.

2. **Optional**: To retrieve new events from the storage array, click **Refresh**.

   It can take several minutes for an event to be logged and become visible in the **Event Log** page.

3. To save the event log to a file:

   a. Select the check box next to each event that you want to save.

   b. Click **Save**.

   The file is saved in the Downloads folder for your browser with the name `major-event-log-timestamp.log`.

4. **Optional**: To clear events from the event log:

   The event log stores approximately 8,000 events before it replaces an event with a new event. If you want to keep the events, you can save them, and clear them from the event log.

   a. First, save the event log.

   b. Click **Clear All**, and confirm that you want to perform the operation.

Upgrade center

Concepts

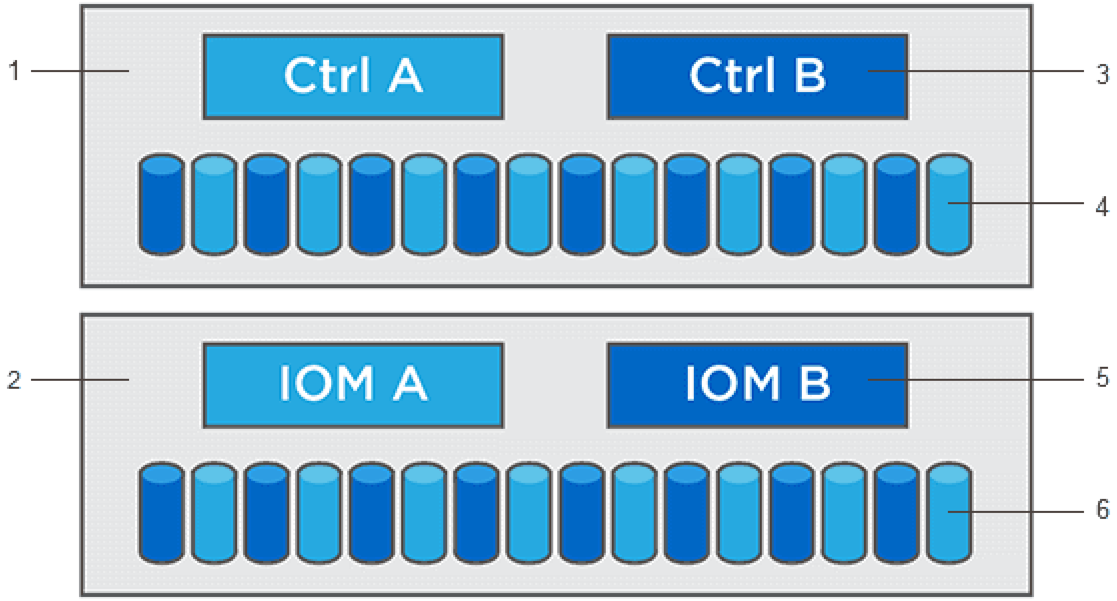
Controller software and firmware upgrades

You can upgrade your storage array’s software and firmware for all the latest features and bug fixes.

Components included in the SANtricity OS controller software upgrade

Several storage array components contain software or hardware that you might want to upgrade occasionally.

- **Management software** — System Manager is the software that manages the storage array.
- **Controller firmware** — Controller firmware manages the I/O between hosts and volumes.
- **Controller NVSRAM** — Controller NVSRAM is a controller file that specifies the default settings for the controllers.
- **IOM firmware** — The I/O module (IOM) firmware manages the connection between a controller and a drive shelf. It also monitors the status of the components.
- **Supervisor software** — Supervisor software is the virtual machine on a controller in which the software runs.



[1] Controller shelf; [2] Drive shelf; [3] Software, controller firmware, controller NVSRAM, supervisor software; [4] Drive firmware; [5] IOM firmware; [6] Drive firmware

You can view your current software and firmware versions in the Software and Firmware Inventory dialog box. Go to **Support › Upgrade Center**, and then click the link for **Software and Firmware Inventory**.

As part of the upgrade process, the host’s multipath/failover driver and/or HBA driver might also need to be upgraded so the host can interact with the controllers correctly. To determine if this is the case, see the Netapp Interoperability Matrix Tool.

When to stop I/O

If your storage array contains two controllers and you have a multipath driver installed, the storage array can remain processing I/O while the upgrade occurs. During the upgrade, controller A fails over all of its LUNs to controller B, upgrades, takes back its LUNs and all of controller B’s LUNs, and then upgrades 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.

Pre-upgrade health check

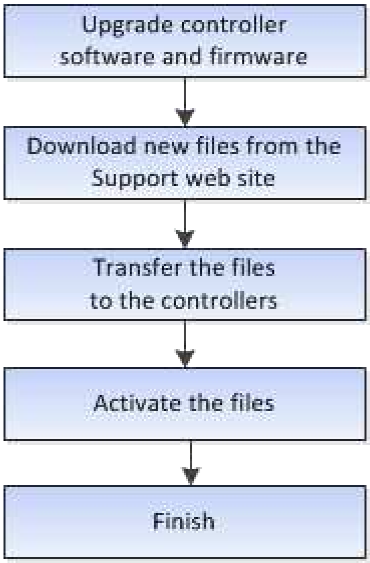
A pre-upgrade health check runs as part of the upgrade process. The pre-upgrade health check assesses all storage array components to make sure the upgrade can proceed. The following conditions might prevent the upgrade:

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

You also can run the pre-upgrade health check separately without doing an upgrade.

Workflow for controller software and firmware upgrade

In SANtricity System Manager, you can upgrade the controller software and firmware by following these steps.


Upgrade controller software and firmware
Download new files from the Support web site
Transfer the files to the controllers
Activate the files
Finish

Drive firmware upgrades

Drive firmware controls the low-level operating characteristics of a drive. Periodically, the drive manufacturers release updates to drive firmware to add new features, improve performance, and fix defects.

Online and offline drive firmware upgrades

There are two types of drive firmware upgrade methods: online and offline.

Online

During an online upgrade, drives are upgraded sequentially, one at a time. The storage array continues processing I/O while the upgrade occurs. You do not have to stop I/O. If a drive can do an online upgrade, the online method is used automatically.

Drives that can do an online upgrade include the following:

- Drives in an Optimal pool
- Drives in an Optimal redundant volume group (RAID 1, RAID 5, and RAID 6)
- Unassigned drives
- Standby hot spare drives

Doing an online drive firmware upgrade can take several hours exposing the storage array to potential volume failures. Volume failure could occur in these cases:

- In a RAID 1 or RAID 5 volume group, one drive fails while a different drive in the volume group is being upgraded.
- In a RAID 6 pool or volume group, two drives fail while a different drive in the pool or volume group is being upgraded.

Offline (parallel)

During an offline upgrade, all drives of the same drive type are upgraded at the same time. This method requires stopping I/O activity to the volumes associated with the selected drives. Because multiple drives can be upgraded concurrently (in parallel), the overall downtime is significantly reduced. If a drive can do only an offline upgrade, the offline method is used automatically.

The following drives MUST use the offline method:

- Drives in a non-redundant volume group (RAID 0)
- Drives in a non-optimal pool or volume group
- Drives in SSD cache

Compatibility

Each drive firmware file contains information about the drive type on which the firmware runs. You can download the specified firmware file only to a compatible drive. System Manager automatically checks compatibility during the upgrade process.

How tos

Upgrade software and firmware

You can upgrade your storage array’s software and, optionally, the IOM firmware and the nonvolatile static random access memory (NVSRAM) to make sure you have all the latest features and bug fixes.

Before you begin

- You know whether you want to upgrade your IOM firmware.

  Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the IOM firmware if you do not want to upgrade it as part of the SANtricity OS software upgrade or if technical support has instructed you to downgrade your IOM firmware (you can only downgrade firmware by using the command line interface).

- You know whether you want to upgrade the controller NVSRAM file.

  Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the controller NVSRAM file if your file has either been patched or is a custom version and you do not want to overwrite it.

- You know whether you want to activate your OS upgrade now or later.

  Reasons for activating later might include:

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

- You know whether you want to switch from unsecured drives or internally secured drives to use an external key management server (KMS) for drive security (new feature in release 11.40).
- You know whether you want to use role-based access control in your storage array (new feature in release 11.40).

About this task

You can choose to upgrade only the OS software file or only the Controller NVSRAM file or you can choose to upgrade both files.

Perform this operation only when instructed to do so by technical support.

> ! **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. Select **Support › Upgrade Center**.

3. Download the new file from the Support site to your management client.

    a. In the area labeled SANtricity OS Controller Software upgrade, click **NetApp Support**.

    b. On the Support web site, click the **Downloads** tab, and then select **Software**.

    c. Select **SANtricity OS Controller Software**.

    d. Follow the remaining instructions.

        The file to download has a filename similar to `E28xx_1140` with a `.zip` or `.tar.gz` extension.

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

4. If you do NOT want to upgrade the IOM firmware at this time, click **Suspend IOM Auto-Synchronization**.

    If you have a storage array with a single controller, the IOM firmware is not upgraded.

5. Under SANtricity OS Software upgrade, click **Begin Upgrade**.

    The Upgrade SANtricity OS Software dialog appears.

6. Select one or more files to begin the upgrade process:

    a. Select the SANtricity OS Software file by clicking **Browse** and navigating to the OS software file you downloaded from the Support web site.

    b. Select the Controller NVSRAM file by clicking **Browse** and navigating to the NVSRAM file that you downloaded from the Support site. Controller NVSRAM files have a filename similar to `N2800-830000-000.dlp`.

    These actions occur:

    - By default, only the files that are compatible with the current storage array configuration appear.
    - When you select a file for upgrade, the file’s name and size appear.

7. **Optional:** If you selected a SANtricity OS Software file to upgrade, you can transfer the files to the controller without activating them by selecting the **Transfer files now, but do not upgrade (activate upgrade later)** check box.

8. Click **Start**, and confirm that you want to perform the operation.

    You can cancel the operation during the pre-upgrade health check, but not during transferring or activating.

9. **Optional:** To see a list of what was upgraded, click **Save Log**.

    The file is saved in the Downloads folder for your browser with the name `drive_upgrade_log-timestamp.txt`.

After you finish

- Verify that all components appear on the Hardware page.
- Verify the new software and firmware versions by checking the Software and Firmware Inventory dialog box (go to **Support › Upgrade Center**, and then click the link for **Software and Firmware Inventory**).
- If you upgraded controller NVSRAM, any custom settings that you have applied to the existing NVSRAM are lost during the process of activation. You need to apply the custom settings to the NVSRAM again after

the process of activation is complete.

Activate controller software and firmware

You can choose to activate the upgrade files immediately or wait until a more convenient time.

About this task

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

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

When you have software or firmware that has been transferred but not activated, you see a notification in the Notifications area of the System Manager Home page and also on the Upgrade Center page.

> ⓘ You cannot stop the activation process after it starts.

Steps

1. Select **Support › Upgrade Center**.
2. In the area labeled SANtricity OS Controller Software upgrade, click **Activate**, and confirm that you want to perform the operation.

   You can cancel the operation during the pre-upgrade health check, but not during activating.

   The pre-upgrade health check begins. If the pre-upgrade health check passes, the upgrade process proceeds to activating the files. If the pre-upgrade health check fails, use the Recovery Guru or contact technical support to resolve the problem.

   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:** To see a list of what was upgraded, click **Save Log**.

   The file is saved in the Downloads folder for your browser with the name `drive_upgrade_log-timestamp.txt`.

After you finish

- Verify that all components appear on the **Hardware** page.
- Verify the new software and firmware versions by checking the Software and Firmware Inventory dialog box (go to **Support › Upgrade Center**, and then click the link for **Software and Firmware Inventory**).
- If you upgraded controller NVSRAM, any custom settings that you have applied to the existing NVSRAM are lost during the process of activation. You need to apply the custom settings to the NVSRAM again after the process of activation is complete.

Upgrade drive firmware

You can upgrade your drives' firmware to make sure you have all the latest features and bug fixes.

Before you begin

- You have backed up your data using disk-to-disk backup, volume copy (to a volume group not affected by the planned firmware upgrade), or a remote mirror.
- The storage array has an Optimal status.
- All drives have an Optimal status.
- No configuration changes are running on the storage array.
- If the drives are capable of only an offline upgrade, I/O activity to all volumes associated with the drives is stopped.

Steps

1. Select **Support › Upgrade Center**.
2. Download the new files from the Support site to your management client.
    a. Under Drive Firmware upgrade, click **NetApp Support**.
    b. On the NetApp Support web site, click the **Downloads** tab, and then select **Firmware**.
    c. Select **Disk Drive & Firmware Matrix**.
    d. Follow the remaining instructions.
3. Under Drive Firmware upgrade, click **Begin Upgrade**.

    A dialog box appears, which lists the drive firmware files currently in use.

4. Extract (unzip) the files you downloaded from the Support site.
5. Click **Browse**, and select the new drive firmware files that you downloaded from the Support site.

    Drive firmware files have a filename similar to `D_HUC101212CSS600_30602291_MS01_2800_0002` with the extension of `.dlp`.

    You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

6. Click **Next**.

    The **Select Drives** dialog box appears, which lists the drives that you can upgrade with the selected files.

    Only drives that are compatible appear.

    The selected firmware for the drive appears in the **Proposed Firmware** information area. If you must change the firmware, click **Back** to return to the previous dialog.

7. Select the type of upgrade you want to perform:
    - **Online (default)**- Shows the drives that can support a firmware download *while the storage array is processing I/O*. You do not have to stop I/O to the associated volumes using these drives when you select this upgrade method. These drives are upgraded one at a time while the storage array is processing I/O to those drives.

- **Offline (parallel)** - Shows the drives that can support a firmware download *only while all I/O activity is stopped* on any volumes that use the drives. You must stop all I/O activity on any volumes that use the drives you are upgrading when you select this upgrade method. Drives that do not have redundancy must be processed as an offline operation. This requirement includes any drive associated with SSD cache, a RAID 0 volume group, or any pool or volume group that is degraded. The offline (parallel) upgrade is typically faster than the online (default) method.

8. In the first column of the table, select the drive or drives you want to upgrade.
9. Click **Start**, and confirm that you want to perform the operation.

   If you need to stop the upgrade, click **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.

   ! Stopping the drive firmware upgrade might result in data loss or unavailable drives.

10. **Optional:** To see a list of what was upgraded, click **Save Log**.

    The file is saved in the Downloads folder for your browser with the name `drive_upgrade_log-timestamp.txt`.

11. If any of the following errors occur during the upgrade procedure, take the appropriate recommended action.

If you encounter this firmware download error…	Then do the following…
Failed assigned drives	One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information. When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing. You can replace the failed drive while the storage array is receiving I/O.
Check storage array	• Make sure that an IP address has been assigned to each controller. • Make sure that all cables connected to the controller are not damaged. • Make sure that all cables are tightly connected.
Integrated hot spare drives	This error condition must be corrected before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem.

If you encounter this firmware download error…	Then do the following…
Incomplete volume groups	If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware. Launch System Manager and use the Recovery Guru to resolve the problem.
Exclusive operations \(other than background media/parity scan\) currently running on any volume groups	If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations.
Missing volumes	You must correct the missing volume condition before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem.
Either controller in a state other than Optimal	One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded. Launch System Manager and use the Recovery Guru to resolve the problem.
Mismatched Storage Partition information between Controller Object Graphs	An error occurred while validating the data on the controllers. Contact technical support to resolve this issue.
SPM Verify Database Controller check fails	A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue.
Configuration Database Validation \(If supported by the storage array's controller version\)	A configuration database error occurred on a controller. Contact technical support to resolve this issue.
MEL Related Checks	Contact technical support to resolve this issue.
More than 10 DDE Informational or Critical MEL events were reported in the last 7 days	Contact technical support to resolve this issue.
More than 2 Page 2C Critical MEL Events were reported in the last 7 days	Contact technical support to resolve this issue.
More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days	Contact technical support to resolve this issue.
More than 4 critical MEL entries in the last 7 days	Contact technical support to resolve this issue.

After you finish

Your drive firmware upgrade is complete. You can resume normal operations.

Review the possible software and firmware upgrade errors

Errors can occur during either the controller software upgrade or the drive firmware upgrade.

Firmware download error	Description	Recommended action
Failed assigned drives	Failed to upgrade an assigned drive in the storage array.	One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information. When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing. You can replace the failed drive while the storage array is receiving I/O.
Integrated hot spare drives	If the drive is marked as a hot spare and is in use for a volume group, the firmware upgrade process fails.	This error condition must be corrected before you can upgrade the firmware. Launch SANtricity System Manager and use the Recovery Guru to resolve the problem.
Incomplete volume groups	If any drive that is part of a volume group is bypassed, removed or unresponsive, it is considered an incomplete volume group. An incomplete volume group prevents firmware upgrades.	If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware. Launch SANtricity System Manager and use the Recovery Guru to resolve the problem.
Exclusive operations (other than background media/parity scan) currently running on any volume groups	Cannot upgrade the firmware if any exclusive operations are in progress on a volume.	If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use SANtricity System Manager to monitor the progress of the operations.

Firmware download error	Description	Recommended action
Missing volumes	Cannot upgrade the firmware if any volume is missing.	You must correct the missing volume condition before the firmware can be upgraded. Launch SANtricity System Manager and use the Recovery Guru to resolve the problem.
Either controller in a state other than Optimal	Cannot upgrade the firmware if either controller is in a state other than optimal.	One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded. Launch SANtricity System Manager and use the Recovery Guru to resolve the problem.
SPM Verify Database Controller check fails	Cannot upgrade the firmware because the storage partitions mappings database is corrupted.	A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue.
Configuration Database Validation (If supported by the storage array's controller version)	Cannot upgrade the firmware because the configuration database is corrupted.	A configuration database error occurred on a controller. Contact technical support to resolve this issue.
MEL Related Checks	Cannot upgrade the firmware because the event log contains errors.	Contact technical support to resolve this issue.
More than 10 DDE Informational or Critical MEL events were reported in the last 7 days	Cannot upgrade the firmware because there are more than 10 DDE informational or critical MEL events reported in the last seven days.	Contact technical support to resolve this issue.
More than 2 Page 2C Critical MEL Events were reported in the last 7 days	Cannot upgrade the firmware because there are more than two page 2C critical MEL Events reported in the last seven days.	Contact technical support to resolve this issue.
More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days	Cannot upgrade the firmware because there are more than two degraded drive channel critical MEL events reported in the last seven days.	Contact technical support to resolve this issue.

Firmware download error	Description	Recommended action
More than 4 critical MEL entries in the last 7 days	Cannot upgrade the firmware because there are more than four critical event log entries reported in the last seven days.	Contact technical support to resolve this issue.
A valid management IP address is required.	A valid controller IP address is required to perform this operation.	Contact technical support to resolve this issue.
The command requires an active management IP address for each controllers to be provided.	A controller IP address for each controller associated with the storage array is required for this operation.	Contact technical support to resolve this issue.
Unhandled download file type returned.	The specified download file is not supported.	Contact technical support to resolve this issue.
An error occurred during the firmware download upload procedure.	The firmware download failed because the controller cannot process the request. Verify the storage array is optimal and retry the operation.	If this error occurs again after verifying the storage array is optimal, contact technical support to resolve this issue.
An error occurred during the firmware activation procedure.	The firmware activation failed because the controller cannot process the request. Verify the storage array is optimal and retry the operation.	If this error occurs again after verifying the storage array is optimal, contact technical support to resolve this issue.
Timeout has reached while waiting for controller {0} to reboot.	The management software is unable to reconnect to controller {0} following a reboot. Validate there is an operational connection path to the storage array and retry the operation if it did not complete successfully.	If this error occurs again after verifying the storage array is optimal, contact technical support to resolve this issue.

You can correct some of these conditions by using the Recovery Guru in SANtricity System Manager. However, for some of the conditions, you might need to contact technical support. The information about the latest controller firmware download is available from the storage array. This information helps technical support to understand the error conditions that prevented the firmware upgrade and download.

FAQs

What do I need to know before upgrading the SANtricity OS Software?

Before you upgrade your controller's software and firmware, be aware of these items.

- You have read the document and the `readme.txt` file and have determined that you want to do the upgrade.

- You know whether you want to upgrade your IOM firmware.

  Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the IOM firmware if you do not want to upgrade it as part of the SANtricity OS controller software upgrade or if technical support has instructed you to downgrade your IOM firmware (you can only downgrade firmware by using the command line interface).

- You know whether you want to upgrade the controller NVSRAM file.

  Normally, you should upgrade all components at the same time. However, you might decide not to upgrade the controller NVSRAM file if your file has either been patched or is a custom version and you do not want to overwrite it.

- You know whether you want to activate now or later.

  Reasons for activating later might include:

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

These components are part of the SANtricity OS controller software upgrade:

- **Management software** — System Manager is the software that manages the storage array.
- **Controller firmware** — Controller firmware manages the I/O between hosts and volumes.
- **Controller NVSRAM** — Controller NVSRAM is a controller file that specifies the default settings for the controllers.
- **IOM firmware** — The I/O module (IOM) firmware manages the connection between a controller and a drive shelf. It also monitors the status of the components.
- **Supervisor software** — Supervisor software is the virtual machine on a controller in which the software runs.

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

> ⓘ To determine if this is the case, see the NetApp Interoperability Matrix Tool.

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.

Do not make changes to the storage array while the upgrade occurs.

What do I need to know before suspending IOM auto-synchronization?

Suspending IOM auto-synchronization prevents the IOM firmware from being upgraded the next time a SANtricity OS controller software upgrade occurs.

Normally, controller software and IOM firmware are upgraded as a bundle. You can suspend IOM auto-synchronization if you have a special build of IOM firmware that you want to preserve on your enclosure.

Otherwise, you will revert to the IOM firmware bundled with the controller software the next time you do a controller software upgrade.

Why is my firmware upgrade progressing so slowly?

The firmware upgrade progress depends on the overall load of the system.

During an online upgrade of drive firmware, if a volume transfer takes place during the rapid reconstruction process, the system initiates a full reconstruction on the volume that was transferred. This operation might take a considerable amount of time. Actual full reconstruction time depends on several factors, including the amount of I/O activity occurring during the reconstruction operation, the number of drives in the volume group, the rebuild priority setting, and the drive performance.

What do I need to know before upgrading drive firmware?

Before upgrading your drive firmware, be aware of these items.

- As a precaution, back up your data using disk-to-disk backup, volume copy (to a volume group not affected by the planned firmware upgrade), or a remote mirror.
- You might want to upgrade only a few drives to test the behavior of the new firmware to ensure it is functioning correctly. If the new firmware is functioning correctly, upgrade the remaining drives.
- If you have any failed drives, fix them before you start the firmware upgrade.
- If the drives can do an offline upgrade, stop I/O activity to all volumes associated with the drives. When I/O activity is stopped, no configuration operations associated with those volumes can occur.
- Do not remove any drives while upgrading drive firmware.
- Do not make any configuration changes to the storage array while upgrading drive firmware.

How do I choose which type of upgrade to perform?

You choose the type of upgrade to perform on the drive depending on the state of the pool or volume group.

- **Online**

  If the pool or volume group supports redundancy and is Optimal, you can use the Online method to upgrade the drive firmware. The Online method downloads firmware *while the storage array is processing I/O* to the associated volumes using these drives. You do not have to stop I/O to the associated volumes using these drives. These drives are upgraded one at a time to the volumes associated with the drives. If the drive is not assigned to a pool or volume group, its firmware can be updated by the Online or the Offline method. System performance may be impacted when you use the Online method to upgrade drive firmware.

- **Offline**

  If the pool or volume group does not support redundancy (RAID 0), or is degraded, you must use the Offline method to upgrade the drive firmware. The Offline method will upgrade firmware *only while all I/O activity is stopped* to the associated volumes using these drives. You must stop all I/O to any associated volumes using these drives. If the drive is not assigned to a pool or volume group, its firmware may be updated by the Online or the Offline method.

Copyright information

Trademark information