Note

Before using this information and the product it supports, read the general information in “Notices” on page 152, the information in the “Safety and environmental notices” on page ix, as well as the information in the IBM Environmental Notices and User Guide, which is provided on a DVD.

This edition applies to IBM Storwize V7000, Version 6.4.1, and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces GC27-2291-03.

© Copyright IBM Corporation 2010, 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

Figures ..................................... v
Tables ....................................... vii
Safety and environmental notices .... ix
About this guide .......................... xi
Who should use this guide .......... xi
Accessibility .............................. xi
Summary of changes for GC27-2291-04 Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide ............................ xi
Summary of changes for GC27-2291-03 Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide ............................ xii
Storwize V7000 library and related publications .... xii
How to order IBM publications ....... xv
Sending your comments ............... xv

Chapter 1. Storwize V7000 hardware components ................................... 1
Components in the front of the enclosure ............... 2
Drives ....................................... 2
Drive indicators ................................ 2
Enclosure end cap indicators ....................... 4
Components in the rear of the enclosure ............... 5
Power supply unit and battery for the control enclosure ............... 6
Power supply unit for the expansion enclosure ....... 7
Node canister ports and indicators .......... 8
Expansion canister ports and indicators ....... 15

Chapter 2. Best practices for troubleshooting ........................................ 19
Record access information ....................... 19
Follow power management procedures .... 20
Set up event notifications .................... 20
Set up inventory reporting ..................... 21
Back up your data ................................ 21
Manage your spare and failed drives ............... 21
Resolve alerts in a timely manner .......... 21
Keep your software up to date ............... 22
Keep your records up to date ............... 22
Subscribe to support notifications .......... 22
Know your IBM warranty and maintenance agreement details .......... 22

Chapter 3. Understanding the Storwize V7000 battery operation for the control enclosure ................................... 25
Maintenance discharge cycles ....................... 26

Chapter 4. Understanding the medium errors and bad blocks ....................... 29

Chapter 5. Storwize V7000 user interfaces for servicing your system .......... 31
Management GUI interface ....................... 31
When to use the management GUI .......... 32
Accessing the management GUI .......... 32
Service assistant interface ....................... 33
When to use the service assistant .......... 33
Accessing the service assistant .......... 34
Cluster (system) command-line interface .......... 35
When to use the cluster (system) CLI .......... 35
Accessing the cluster (system) CLI .......... 35
Service command-line interface .......... 35
When to use the service CLI .......... 36
Accessing the service CLI .......... 36
USB flash drive and Initialization tool interface .......... 36
When to use the USB flash drive .......... 36
Using a USB flash drive .......... 36
Using the initialization tool .......... 37
satask.txt commands .......... 38

Chapter 6. Resolving a problem ....................... 43
Start here: Use the management GUI recommended actions .......... 43
Problem: Management IP address unknown .......... 44
Problem: Unable to connect to the management GUI .......... 45
Problem: Unable to log on to the management GUI .......... 46
Problem: Cannot create a clustered storage system .......... 46
Problem: Node canister service IP address unknown .......... 46
Problem: Cannot connect to the service assistant .......... 47
Problem: Management GUI or service assistant does not display correctly .......... 48
Problem: A node canister has a location node error .......... 48
Problem: SAS cabling not valid .......... 49
Problem: New expansion enclosure not detected .......... 49
Problem: Control enclosure not detected .......... 50
Problem: Mirrored volume copies no longer identical .......... 50
Problem: Command file not processed from USB flash drive .......... 50
Procedure: Resetting superuser password .......... 51
Procedure: Identifying which enclosure or canister to service .......... 51
Procedure: Checking the status of your system .......... 52
Procedure: Getting node canister and system information using the service assistant .......... 53
Procedure: Getting node canister and system information using a USB flash drive .......... 53
Procedure: Understanding the system status using the LEDs .......... 54
Procedure: Finding the status of the Ethernet connections .......... 59
## Chapter 7. Recovery procedures

### Recover system procedure
- When to run the recover system procedure
- Fix hardware errors
- Removing system information for node canisters with error code 550 or error code 578 using the service assistant
- Performing system recovery using the service assistant
- Recovering from offline VDisks using the CLI
- What to check after running the system recovery
- Backing up and restoring the system configuration
- Backing up the system configuration using the CLI
- Restoring the system configuration
- Deleting backup configuration files using the CLI

### Chapter 8. Removing and replacing parts

- Preparing to remove and replace parts
- Replacing a node canister
- Replacing an expansion canister
- Replacing an SFP transceiver
- Replacing a power supply unit for a control enclosure
- Replacing a power supply unit for an expansion enclosure
- Replacing a battery in a power supply unit
- Releasing the cable retention bracket
- Replacing a 3.5" drive assembly or blank carrier
- Replacing a 2.5" drive assembly or blank carrier
- Replacing enclosure end caps
- Replacing a SAS cable
- Replacing a control enclosure chassis
- Replacing an expansion enclosure chassis
- Replacing the support rails

### Storwize V7000 replaceable units

### Chapter 9. Event reporting

- Understanding events
- Viewing the event log
- Managing the event log
- Describing the fields in the event log
- Event notifications
- Power-on self-test
- Understanding the error codes
- Event IDs
- Error event IDs and error codes
- Node error code overview
- Clustered-system code overview
- Error code range

### Appendix. Accessibility features for IBM Storwize V7000

### Notices

- Trademarks
- Electronic emission notices
- Federal Communications Commission (FCC) statement
- Industry Canada compliance statement
- Avis de conformité à la réglementation d’Industrie Canada
- Australia and New Zealand Class A Statement
- European Union Electromagnetic Compatibility Directive
- Germany Electromagnetic compatibility directive
- Japan VCCI Council Class A statement
- People’s Republic of China Class A Electronic Emission Statement
- International Electrotechnical Commission (IEC) statement
- United Kingdom telecommunications requirements
- Korean Communications Commission (KCC) Class A Statement
- Russia Electromagnetic Interference (EMI) Class A Statement
- Taiwan Class A compliance statement
- European Contact Information
- Taiwan Contact Information

### Index
Figures

1. 12 drives on either 2076-112 or 2076-312 .......................... 2
2. 24 drives on either 2076-124 or 2076-324 .......................... 2
3. LED indicators on a single 3.5" drive ............................. 3
4. LED indicators on a single 2.5" drive ............................. 3
5. 12 drives and two end caps ........................................ 4
6. Left enclosure end cap .............................................. 4
7. Rear view of a model 2076-112 or a model 2076-124 control enclosure ........................................ 5
8. Rear view of a model 2076-312 or a model 2076-324 control enclosure ........................................ 6
9. Rear view of a model 2076-212 or a model 2076-224 expansion enclosure ........................................ 6
10. LEDs on the power supply units of the control enclosure .................................................. 7
11. LEDs on the power supply units of the expansion enclosure .................................................. 7
12. Fibre Channel ports on the node canisters .................................................. 9
13. LEDs on the Fibre Channel ports .................................................. 9
14. USB ports on the node canisters .................................................. 11
15. Ethernet ports on the 2076-112 and 2076-124 node canisters .................................................. 12
16. 10 Gbps Ethernet ports on the 2076-312 and 2076-324 node canisters .................................................. 12
17. SAS ports on the node canisters .................................................. 13
18. LEDs on the node canisters .................................................. 14
19. SAS ports and LEDs in rear of expansion enclosure .................................................. 16
20. LEDs on the expansion canisters .................................................. 17
21. LEDs on the power supply units of the control enclosure .................................................. 55
22. LEDs on the node canisters .................................................. 57
23. LEDs on the node canisters .................................................. 66
24. Rear of node canisters that shows the handles .................................................. 86
25. Removing the canister from the enclosure .................................................. 87
26. Rear of expansion canisters that shows the handles .................................................. 88
27. Removing the canister from the enclosure .................................................. 89
28. SFP transceiver .................................................. 90
29. Directions for lifting the handle on the power supply unit .................................................. 93
30. Using the handle to remove a power supply unit .................................................. 93
31. Directions for lifting the handle on the power supply unit .................................................. 97
32. Using the handle to remove a power supply unit .................................................. 97
33. Removing the battery from the control enclosure power-supply unit .................................................. 101
34. Unlocking the 3.5" drive .................................................. 103
35. Removing the 3.5" drive .................................................. 104
36. Unlocking the 2.5" drive .................................................. 105
37. Removing the 2.5" drive .................................................. 105
38. SAS cable .................................................. 107
39. Removing a rail assembly from a rack cabinet .................................................. 116
Tables

1. Storwize V7000 library .................. xiii
2. Other IBM publications ................. xiv
3. IBM documentation and related websites xv
4. Drive LEDs ................................ 3
5. LED descriptions ......................... 5
6. Power supply unit LEDs in the rear of the control enclosure .................. 7
7. Power supply unit LEDs in the rear of the expansion enclosure .................. 8
8. Fibre Channel port LED locations on canister 1 10
9. Fibre Channel port LED status descriptions 10
10. 1 Gbps Ethernet port LEDs ............. 12
11. 10 Gbps Ethernet port LEDs ........... 13
12. SAS port LEDs on the node canister .... 13
13. Node canister LEDs ..................... 14
14. SAS port LEDs on the expansion canister 16
15. Expansion canister LEDs ............... 17
16. Access information for your system .... 19
17. Bad block errors ......................... 29
18. Power-supply unit LEDs ................. 55
19. Power LEDs ............................. 56
20. System status and fault LEDs .......... 57
21. Control enclosure battery LEDs ........ 58
22. Replaceable units ........................ 117
23. Description of data fields for the event log 120
24. Notification levels ....................... 121
25. Informational events .................... 122
26. Error event IDs and error codes ........ 126
27. Message classification number range 138
Safety and environmental notices

Review the multilingual safety notices for the IBM® Storwize® V7000 system before you install and use the product.

Suitability for telecommunication environment: This product is not intended to connect directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

To find the translated text for a caution or danger notice:
1. Look for the identification number at the end of each caution notice or each danger notice. In the following examples, the numbers (C001) and (D002) are the identification numbers.

   CAUTION:
   A caution notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury. (C001)

   DANGER
   A danger notice indicates the presence of a hazard that has the potential of causing death or serious personal injury. (D002)

2. Locate IBM Storwize V7000 Safety Notices with the user publications that were provided with the Storwize V7000 hardware.
3. Find the matching identification number in the IBM Storwize V7000 Safety Notices. Then review the topics concerning the safety notices to ensure that you are in compliance.
4. Optionally, read the multilingual safety instructions on the Storwize V7000 website. Go to www.ibm.com/storage/support/storwize/v7000 and click the documentation link.

Sound pressure

Attention: Depending on local conditions, the sound pressure can exceed 85 dB(A) during service operations. In such cases, wear appropriate hearing protection.
About this guide

This guide describes how to service, maintain, and troubleshoot the IBM Storwize V7000.

The chapters that follow introduce you to the hardware components and to the tools that assist you in troubleshooting and servicing the Storwize V7000, such as the management GUI and the service assistant.

The troubleshooting procedures can help you analyze failures that occur in a Storwize V7000 system. With these procedures, you can isolate the components that fail.

You are also provided with step-by-step procedures to remove and replace parts.

Who should use this guide

This guide is intended for system administrators who use and diagnose problems with the Storwize V7000.

Accessibility

IBM has a long-standing commitment to people with disabilities. In keeping with that commitment to accessibility, IBM strongly supports the U.S. Federal government’s use of accessibility as a criterion in the procurement of Electronic Information Technology (EIT).

IBM strives to provide products with usable access for everyone, regardless of age or ability.

This product uses standard Windows navigation keys.

For more information, see “Accessibility features for IBM Storwize V7000,” on page 155.

Summary of changes for GC27-2291-04 Storwize V7000

Troubleshooting, Recovery, and Maintenance Guide

The summary of changes provides a list of new and changed information since the last version of the guide.

New information

This topic describes the changes to this guide since the previous edition, GC27-2291-03. The following sections summarize the changes that have since been implemented from the previous version.

This version includes the following new information:

• Backing up and restoring the system configuration
Summary of changes for GC27-2291-03 Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide

The summary of changes provides a list of new and changed information since the last version of the guide.

**New information**

This topic describes the changes to this guide since the previous edition, GC27-2291-02. The following sections summarize the changes that have since been implemented from the previous version.

This version includes the following new information:

- Fibre Channel over Ethernet

**Changed information**

This version does not include any changed information.

**Emphasis**

Different typefaces are used in this guide to show emphasis.

The following typefaces are used to show emphasis:

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Text in <strong>boldface</strong> represents menu items.</td>
</tr>
<tr>
<td><strong>Bold monospace</strong></td>
<td>Text in <strong>bold monospace</strong> represents command names.</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Text in <em>italics</em> is used to emphasize a word. In command syntax, it is used for variables for which you supply actual values, such as a default directory or the name of a system.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Text in monospace identifies the data or commands that you type, samples of command output, examples of program code or messages from the system, or names of command flags, parameters, arguments, and name-value pairs.</td>
</tr>
</tbody>
</table>

**Storwize V7000 library and related publications**

Product manuals, other publications, and websites contain information that relates to Storwize V7000.

**Storwize V7000 Information Center**

The IBM Storwize V7000 Information Center contains all of the information that is required to install, configure, and manage the Storwize V7000. The information center is updated between Storwize V7000 product releases to provide the most current documentation. The information center is available at the following website:

Storwize V7000 library

Unless otherwise noted, the publications in the Storwize V7000 library are available in Adobe portable document format (PDF) from the following website:

www.ibm.com/storage/support/storwize/v7000

Each of the PDF publications in Table 1 is available in this information center by clicking the number in the “Order number” column:

Table 1. Storwize V7000 library

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Order number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Storwize V7000 Quick Installation Guide</td>
<td>This guide provides instructions for unpacking your shipping order and installing your system. The first of three chapters describes verifying your order, becoming familiar with the hardware components, and meeting environmental requirements. The second chapter describes installing the hardware and attaching data cables and power cords. The last chapter describes accessing the management GUI to initially configure your system.</td>
<td>GC27-2290</td>
</tr>
<tr>
<td>IBM Storwize V7000 Expansion Enclosure Installation Guide, Machine type 2076</td>
<td>This guide provides instructions for unpacking your shipping order and installing the 2076 expansion enclosure for the Storwize V7000 system.</td>
<td></td>
</tr>
<tr>
<td>IBM Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide</td>
<td>This guide describes how to service, maintain, and troubleshoot the Storwize V7000 system.</td>
<td>GC27-2291</td>
</tr>
<tr>
<td>IBM Storwize V7000 CIM Agent Developer’s Guide</td>
<td>This guide describes the concepts of the Common Information Model (CIM) environment. Procedures describe such tasks as using the CIM agent object class instances to complete basic storage configuration tasks, establishing new Copy Services relationships, and performing CIM agent maintenance and diagnostic tasks.</td>
<td>GC27-2292</td>
</tr>
</tbody>
</table>
**Table 1. Storwize V7000 library (continued)**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Order number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Systems Safety Notices</td>
<td>This guide contains translated caution and danger statements. Each caution and danger statement in the Storwize V7000 documentation has a number that you can use to locate the corresponding statement in your language in the IBM Systems Safety Notices document.</td>
<td>G229-9054</td>
</tr>
<tr>
<td>IBM Storwize V7000 Read First Flyer</td>
<td>This document introduces the major components of the Storwize V7000 system and describes how to get started with the IBM Storwize V7000 Quick Installation Guide.</td>
<td>GC27-2293</td>
</tr>
<tr>
<td>IBM System Storage SAN Volume Controller and IBM Storwize V7000 Command-Line Interface User’s Guide</td>
<td>This guide describes the commands that you can use from the Storwize V7000 command-line interface (CLI).</td>
<td>GC27-2287</td>
</tr>
<tr>
<td>IBM Statement of Limited Warranty (2145 and 2076)</td>
<td>This multilingual document provides information about the IBM warranty for machine types 2145 and 2076.</td>
<td>Part number: 4377322</td>
</tr>
<tr>
<td>IBM License Agreement for Machine Code</td>
<td>This multilingual guide contains the License Agreement for Machine Code for the Storwize V7000 product.</td>
<td>SC28-6872 (contains Z125-5465)</td>
</tr>
</tbody>
</table>

**Other IBM publications**

Table 2 lists IBM publications that contain information related to the Storwize V7000.

**Table 2. Other IBM publications**

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Order number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Storage Management Pack for Microsoft System Center Operations Manager User Guide</td>
<td>This guide describes how to install, configure, and use the IBM Storage Management Pack for Microsoft System Center Operations Manager (SCOM).</td>
<td>GC27-3909</td>
</tr>
<tr>
<td>IBM Storage Management Console for VMware vCenter, version 3.0.0, User Guide</td>
<td>This publication describes how to install, configure, and use the IBM Storage Management Console for VMware vCenter, which enables Storwize V7000 and other IBM storage systems to be integrated in VMware vCenter environments.</td>
<td>GA32-0929</td>
</tr>
</tbody>
</table>
IBM documentation and related websites

Table 3 lists websites that provide publications and other information about the Storwize V7000 or related products or technologies.

Table 3. IBM documentation and related websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Storwize V7000 (2076)</td>
<td><a href="http://www.ibm.com/storage/support/storwize/v7000">www.ibm.com/storage/support/storwize/v7000</a></td>
</tr>
<tr>
<td>Support for IBM System Storage® and IBM TotalStorage products</td>
<td><a href="http://www.ibm.com/storage/support/">www.ibm.com/storage/support/</a></td>
</tr>
<tr>
<td>IBM Publications Center</td>
<td><a href="http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss">www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss</a></td>
</tr>
<tr>
<td>IBM Redbooks® publications</td>
<td><a href="http://www.redbooks.ibm.com/">www.redbooks.ibm.com/</a></td>
</tr>
</tbody>
</table>

Related accessibility information

To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded from the Adobe website:


How to order IBM publications

The IBM Publications Center is a worldwide central repository for IBM product publications and marketing material.

The IBM Publications Center offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download at no charge. You can also order publications. The publications center displays prices in your local currency. You can access the IBM Publications Center through the following website:

www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

Sending your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

To submit any comments about this book or any other Storwize V7000 documentation:

- Go to the feedback page on the website for the Storwize V7000 Information Center at publib.boulder.ibm.com/infocenter/storwize/ic/index.jsp?topic=/com.ibm.storwize v7000.doc/feedback.htm. There you can use the feedback page to enter and submit comments or browse to the topic and use the feedback link in the running footer of that page to identify the topic for which you have a comment.
- Send your comments by email to starpubs@us.ibm.com. Include the following information for this publication or use suitable replacements for the publication title and form number for the publication on which you are commenting:
  - Publication title: IBM Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide
  - Publication form number: GC27-2291-02

About this guide  XV
- Page, table, or illustration numbers that you are commenting on
- A detailed description of any information that should be changed
Chapter 1. Storwize V7000 hardware components

A Storwize V7000 system consists of one or more machine type 2076 rack-mounted enclosures.

There are several model types. The main differences among the model types are the following items:

- The number of drives that an enclosure can hold. Drives are located on the front of the enclosure. An enclosure can hold up to 12 3.5-inch drives or up to 24 2.5-inch drives.
- Whether the model is a control enclosure or an expansion enclosure. Control enclosures contain the main processing units that control the whole system. They are where external systems, such as host application servers, other storage systems, and management workstations are connected through the Ethernet ports or Fibre Channel ports. Control enclosures can also be connected to expansion enclosures through the serial-attached SCSI (SAS) ports. Expansion enclosures contain additional storage capacity. Expansion enclosures connect either to control enclosures or to other expansion enclosures through the SAS ports.
- If the control enclosure has either 1 Gbps Ethernet capability or 10 Gbps Ethernet capability.

These are the control enclosure models:

- Machine type and model 2076-112, which can hold up to 12 3.5-inch drives
- Machine type and model 2076-124, which can hold up to 24 2.5-inch drives
- Machine type and model 2076-312, which can hold up to 12 3.5-inch drives and includes 10 Gbps Ethernet capability
- Machine type and model 2076-324, which can hold up to 24 2.5-inch drives and includes 10 Gbps Ethernet capability

These are the expansion enclosure models:

- Machine type and model 2076-212, which can hold up to 12 3.5-inch drives
- Machine type and model 2076-224, which can hold up to 24 2.5-inch drives

The machine type and model (MTM) are shown on these labels that are located on the front and the rear of each enclosure:

- The left end cap on the front of the enclosure. The label also indicates if the enclosure is a control enclosure or an expansion enclosure.
- The rear of the left enclosure flange.
Note: The labels also show the enclosure serial number. You must know the serial number when you contact IBM support.

Because of the differences between the enclosures, you must be able to distinguish between the control enclosures and the expansion enclosures when you service the system. Be aware of the following differences:
- The model type that is shown on the labels.
- The model description that is shown on the left end cap.
- The number of ports at the rear of the enclosure. Control enclosures have Ethernet ports, Fibre Channel ports, and USB ports. Expansion enclosures do not have any of these ports.

### Components in the front of the enclosure

This topic describes the components in the front of the enclosure.

#### Drives

An enclosure can hold up to twelve 3.5 in. (8.89 cm) drives or up to twenty-four 2.5 in. (6.35 cm) drives.

The drives are located in the front of the enclosure. The 12 drives are mounted horizontally in four columns with three rows.

The 24 drives are mounted vertically in one row.

Note: The drive slots cannot be empty. A drive assembly or blank carrier must be in each slot.

Figure 1 shows 12 drives, and Figure 2 shows 24 drives.

**Figure 1. 12 drives on either 2076-112 or 2076-312**

**Figure 2. 24 drives on either 2076-124 or 2076-324**

#### Drive indicators

The drives have two LED indicators each. They have no controls or connectors.

The LED color is the same for both drives. The LEDs for the 3.5-inch drives are placed vertically above and below each other. The LEDs for the 2.5-inch drives are placed next to each other at the bottom.
Table 4 shows the status descriptions for the two LEDs.

Table 4. Drive LEDs

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
</tr>
</thead>
</table>
| Activity | Indicates if the drive is ready or active.  
  • If the LED is on, the drive is ready to be used.  
  • If the LED is off, the drive is not ready.  
  • If the LED is flashing, the drive is ready, and there is activity. | Green |
| Fault  | Indicates a fault or identifies a drive.  
  • If the LED is on, a fault exists on the drive.  
  • If the LED is off, no known fault exists on the drive.  
  • If the LED is flashing, the drive is being identified. A fault might or might not exist. | Amber |
Enclosure end cap indicators

This topic describes the indicators on the enclosure end cap.

Figure 5 shows where the end caps are located on the front of an enclosure with 12 drives. The end caps are located in the same position for an enclosure with 24 drives.

- **1** Left end cap
- **2** Drives
- **3** Right end cap

Figure 6 shows the indicators on the front of the enclosure end cap.

The left enclosure end caps for both enclosures are identical and contain only indicators. The left enclosure end cap contains no controls or connectors. The right enclosure end cap for both enclosures has no controls, indicators, or connectors.
### Table 5. LED descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>The power LED is the upper LED. When the green LED is lit, it indicates that the main power is available to the enclosure</td>
<td>Green</td>
<td>🕯️</td>
</tr>
<tr>
<td>Fault</td>
<td>The fault LED is the middle LED. When the amber LED is lit, it indicates that one of the enclosure components has a hardware fault.</td>
<td>Amber</td>
<td>!</td>
</tr>
<tr>
<td>Identify</td>
<td>The identify LED is the lower LED. When the blue LED is lit, it identifies the enclosure.</td>
<td>Blue</td>
<td>🔍</td>
</tr>
<tr>
<td>N/A</td>
<td>The two-character LCD display shows the enclosure ID.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## Components in the rear of the enclosure

This topic describes the hardware components in the rear of the enclosure.

Two canisters are located in the middle of each enclosure. The power supply units are located on the left and right of the canisters. The left slot is power supply 1 (1), and the right slot is power supply 2 (2). Power supply 1 is top side up, and power supply 2 is inverted. The upper slot is canister 1 (3), and the lower slot is canister 2 (4). Canister 1 is top side up, and canister 2 is inverted.

Figure 7 shows the rear view of a model 2076-112 or a model 2076-124 control enclosure. Figure 8 on page 6 shows the rear view of a model 2076-312 or a model 2076-324 control enclosure with the 10 Gbps Ethernet port (5). Figure 9 on page 6 shows the rear of an expansion enclosure.

Figure 7. Rear view of a model 2076-112 or a model 2076-124 control enclosure
The control enclosure contains two power supply units, each with an integrated battery.

The two power supply units in the enclosure are installed with one unit top side up and the other inverted. The power supply unit for the control enclosure has six LEDs.

There is a power switch on each of the power supply units. The switch must be on for the power supply unit to be operational. If the power switches are turned off, or the main power is removed, the integrated batteries temporarily continue to supply power to the node canisters. As a result, the canisters can store configuration data and cached data to their internal drives. Battery power is required only if both power supply units stop operating.

Figure 10 on page 7 shows the location of the LEDs in the rear of the power supply unit.
Table 6 identifies the LEDs in the rear of the control enclosure.

Table 6. Power supply unit LEDs in the rear of the control enclosure

<table>
<thead>
<tr>
<th>Name</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac power failure</td>
<td>Amber</td>
<td>⏳️</td>
</tr>
<tr>
<td>Power supply OK</td>
<td>Green</td>
<td>⚡️</td>
</tr>
<tr>
<td>Fan failure</td>
<td>Amber</td>
<td>⌻</td>
</tr>
<tr>
<td>dc power failure</td>
<td>Amber</td>
<td>⏳️</td>
</tr>
<tr>
<td>Battery failure</td>
<td>Amber</td>
<td>📦</td>
</tr>
<tr>
<td>Battery state</td>
<td>Green</td>
<td>🛠️</td>
</tr>
</tbody>
</table>

See “Procedure: Understanding the system status using the LEDs” on page 54 for help in diagnosing a particular failure.

**Power supply unit for the expansion enclosure**

The expansion enclosure contains two power supply units.

The two power supply units in the enclosure are installed with one unit top side up and the other inverted. The power supply unit for the expansion enclosure has four LEDs, two less than the power supply for the control enclosure.
There is a power switch on each of the power supply units. The switch must be on for the power supply unit to be operational. If the power switches are turned off, the power supply units stop providing power to the system.

Figure 11 shows the locations of the LEDs in the rear of the power supply unit.

![Image of LEDs on power supply unit]

Figure 11. LEDs on the power supply units of the expansion enclosure

Table 7 identifies the LEDs in the rear of the expansion enclosure.

Table 7. Power supply unit LEDs in the rear of the expansion enclosure

<table>
<thead>
<tr>
<th>Name</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac power failure</td>
<td>Amber</td>
<td>~</td>
</tr>
<tr>
<td>Power supply OK</td>
<td>Green</td>
<td>🏴</td>
</tr>
<tr>
<td>Fan failure</td>
<td>Amber</td>
<td>⚡</td>
</tr>
<tr>
<td>dc power failure</td>
<td>Amber</td>
<td>...</td>
</tr>
</tbody>
</table>

See “Procedure: Understanding the system status using the LEDs” on page 54 for help in diagnosing a particular failure.

**Node canister ports and indicators**

The node canister has indicators and ports but no controls.

**Fibre Channel ports and indicators**

The Fibre Channel port LEDs show the speed of the Fibre Channel ports and activity level.
Each node canister has four Fibre Channel ports located on the left side of the canister as shown in Figure 12. The ports are in two rows of two ports. The ports are numbered 1 - 4 from left to right and top to bottom.

**Note:** The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

---

**Figure 12. Fibre Channel ports on the node canisters**

There are two green LEDs associated with each port: the speed LED and the link activity LED. These LEDs are in the shape of a triangle. The LEDs are located in between the two rows of the ports as shown in Figure 13. Figure 13 shows the LEDs for the Fibre Channel ports on canister 1. Each LED points to the associated port. The first and second LEDs in each set show the speed state, and the third and fourth LEDs show the link state.

---

**Figure 13. LEDs on the Fibre Channel ports**
Table 8. Fibre Channel port LED locations on canister 1

<table>
<thead>
<tr>
<th>Associated port</th>
<th>LED location</th>
<th>LED status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 3 3</td>
<td>First LED between ports 1 and 3 1</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 1 1</td>
<td>Second LED between ports 1 and 3 2</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 3 3</td>
<td>Third LED between ports 1 and 3 3</td>
<td>Link</td>
</tr>
<tr>
<td>Port 1 1</td>
<td>Fourth LED between ports 1 and 3 4</td>
<td>Link</td>
</tr>
<tr>
<td>Port 4 4</td>
<td>First LED between ports 2 and 4 5</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 2 2</td>
<td>Second LED between ports 2 and 4 6</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 4 4</td>
<td>Third LED between ports 2 and 4 7</td>
<td>Link</td>
</tr>
<tr>
<td>Port 2 2</td>
<td>Fourth LED between ports 2 and 4 8</td>
<td>Link</td>
</tr>
</tbody>
</table>

Table 9 provides the status descriptions for the LEDs on the Fibre Channel ports.

Table 9. Fibre Channel port LED status descriptions

<table>
<thead>
<tr>
<th>Speed state LED</th>
<th>Link state LED</th>
<th>Link state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Off</td>
<td>Inactive</td>
</tr>
<tr>
<td>Off</td>
<td>On or flashing</td>
<td>Active low speed (2 Gbps)</td>
</tr>
<tr>
<td>Flashing</td>
<td>On or flashing</td>
<td>Active medium speed (4 Gbps)</td>
</tr>
<tr>
<td>On</td>
<td>On or flashing</td>
<td>Active high speed (8 Gbps)</td>
</tr>
</tbody>
</table>

Fibre Channel port numbers and worldwide port names:

Fibre Channel ports are identified by their physical port number and by a worldwide port name (WWPN).

The physical port numbers identify Fibre Channel cards and cable connections when you perform service tasks. The WWPNs are used for tasks such as Fibre Channel switch configuration and to uniquely identify the devices on the SAN.

The WWPNs are derived from the worldwide node name (WWNN) that is allocated to the Storwize V7000 node in which the ports are installed. The WWNN for each node is stored within the enclosure. When you replace a node canister, the WWPNs of the ports do not change.

The WWNN is in the form 50050768020XXXXX, where XXXXX is specific to an enclosure.

USB ports

Two USB ports are located side by side on each node canister.

The USB ports are numbered 1 on the left and 2 on the right as shown in Figure 14 on page 11. One port is used during installation.
Note: The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

The USB ports have no indicators.

Ethernet ports and indicators
Ethnic ports are located side by side on the rear of the node canister. All control enclosure models have two 1 Gbps Ethernet ports per node canister. Model 2076-312 and model 2076-324 also have two 10 Gbps Ethernet ports per node canister.

For the 1 Gbps support, the Ethernet ports are numbered 1 on the left and 2 on the right as shown in Figure 15 on page 12. Port 1 must be connected; the use of port 2 is optional. Two LEDs are associated with each port.

Note: The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.
Table 10 provides a description of the two LEDs.

**Table 10. 1 Gbps Ethernet port LEDs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link speed (LED on right of upper canister)</td>
<td>The LED is on when there is a link connection; otherwise, the LED is off.</td>
<td>Green</td>
</tr>
<tr>
<td>Activity (LED on left of upper canister)</td>
<td>The LED is flashing when there is activity on the link; otherwise, the LED is off.</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Figure 15 shows the location of the 10 Gbps Ethernet ports.

Table 11 on page 13 provides a description of the LEDs.

Figure 16 shows the location of the 10 Gbps Ethernet ports.

Figure 16. 10 Gbps Ethernet ports on the 2076-312 and 2076-324 node canisters
Table 11. 10 Gbps Ethernet port LEDs

<table>
<thead>
<tr>
<th>Name</th>
<th>Symbol</th>
<th>Description</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>Tx/Rx</td>
<td>The LED is flashing when there is activity on the link; otherwise, the LED is off.</td>
<td>Green</td>
</tr>
<tr>
<td>Link</td>
<td>LNK</td>
<td>The LED is on when there is a link connection; otherwise, the LED is off.</td>
<td>Amber</td>
</tr>
</tbody>
</table>

Node canister SAS ports and indicators

Two serial-attached SCSI (SAS) ports are located side by side in the rear of the node canister.

The SAS ports are numbered 1 on the left and 2 on the right as shown in Figure 17. Port 1 is used if you add one expansion enclosure. Port 2 is used if you add a second expansion enclosure. Each port provides four data channels.

Note: The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

**Figure 17. SAS ports on the node canisters.**

SAS ports must be connected to Storwize V7000 enclosures only. See “Problem: SAS cabling not valid” on page 49 for help in attaching the SAS cables.

Four LEDs are located with each port. Each LED describes the status of one data channel within the port. The data channel number is shown with the LED.

Table 12. SAS port LEDs on the node canister

<table>
<thead>
<tr>
<th>LED state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No link is connected.</td>
</tr>
<tr>
<td>Flashing</td>
<td>The link is connected and has activity.</td>
</tr>
<tr>
<td>On</td>
<td>The link is connected.</td>
</tr>
</tbody>
</table>
Node canister LEDs
Each node canister has three LEDs that provide status and identification for the node canister.

The three LEDs are located in a horizontal row near the upper right of the canister. Figure 18 shows the rear view of the node canister LEDs.

![Figure 18. LEDs on the node canisters](image)

Note: The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

Table 13. Node canister LEDs

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>System status</td>
<td>Indicates the status of the node.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The on status indicates that the node is active, that is, it is an active member of a clustered system. When the node is active, do not remove it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The off state indicates there is no power to the canister or the canister is in standby mode. These conditions can cause the off state:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>  - The main processor is off and only the service processor is active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>  - A power-on self-test (POST) is running on the canister.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>  - The operating system is loading.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The flashing status indicates that the node is in candidate state or service state. It is not able to perform I/O in a system. When the node is in either of these states, it can be removed. Do not remove the canister unless directed by a service procedure.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 13. Node canister LEDs (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
</table>
| Fault | Indicates if a fault is present and identifies which canister.  
• The on status indicates that the node is in service state or an error exists that might be preventing the code from starting. Do not assume that this status indicates a hardware error. Further investigation is required before replacing the node canister.  
• The off status indicates that the node is a candidate or is active. This status does not mean that there is not a hardware error on the node. Any error that was detected is not severe enough to stop the node from participating in a system.  
• The flashing status indicates that the canister is being identified. This status might or might not be a fault. | Amber |  |
| Power | Indicates if power is available and the boot status of the canister.  
• The on status indicates that the canister is powered on and that the main processor or processors are running.  
• The off status indicates that no power is available.  
• The slow flashing (1 Hz) status indicates that power is available and that the canister is in standby mode. The main processor or processors are off and only the service processor is active.  
• The fast flashing (2 Hz) indicates that the canister is running the power-on self-test (POST). | Green |  |

Notes:
1. If the system status LED is on and the fault LED is off, the node canister is an active member of a system.
2. If the system status LED is on and the fault LED is on, there is a problem establishing a system.

For a more complete identification of the system LEDs, go to “Procedure: Understanding the system status using the LEDs” on page 54.

Expansion canister ports and indicators

An expansion canister is one of two canisters that is located in the rear of the expansion enclosure. The expansion canister has no controls.

There is a diagnostic port on the left of the canister. There are no indicators that are associated with the port. There are no defined procedures that use the port.

Note: The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

Expansion canister SAS ports and indicators

Two SAS ports are located in the rear of the expansion canister.
The SAS ports are numbered 1 on the left and 2 on the right as shown in Figure 19. Use of port 1 is required. Use of port 2 is optional. Each port connects four data channels.

**Note:** The reference to the left and right locations applies to canister 1, which is the upper canister. The port locations are inverted for canister 2, which is the lower canister.

![SAS ports and LEDs in rear of expansion enclosure](image)

**Figure 19. SAS ports and LEDs in rear of expansion enclosure**

- 1 Port 1, 6 Gbps SAS port and LEDs
- 2 Port 2, 6 Gbps SAS port and LEDs

Four LEDs are located with each port. Each LED describes the status of one data channel within the port. The data channel is shown with the LED.

<table>
<thead>
<tr>
<th>LED state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No link is connected.</td>
</tr>
<tr>
<td>Flashing</td>
<td>The link is connected and has activity.</td>
</tr>
<tr>
<td>On</td>
<td>The link is connected.</td>
</tr>
</tbody>
</table>

**Table 14. SAS port LEDs on the expansion canister**

**Expansion canister LEDs**

Each expansion canister has two LEDs that provide status and identification for the expansion canister.

The two LEDs are located in a vertical row on the left side of the canister. Figure 20 on page 17 shows the LEDs (1) in the rear of the expansion canister.
Table 15. Expansion canister LEDs

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates if the canister is active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the LED is on, the canister is active.</td>
<td>Green</td>
<td>![Green]</td>
</tr>
<tr>
<td></td>
<td>• If the LED is off, the canister is not active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the LED is flashing, there is a vital product data (VPD) error.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault</td>
<td>Indicates if a fault is present and identifies the canister.</td>
<td>Amber</td>
<td>![Amber]</td>
</tr>
<tr>
<td></td>
<td>• If the LED is on, a fault exists.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the LED is off, no fault exists.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the LED is flashing, the canister is being identified. This status might or might not be a fault.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 20. LEDs on the expansion canisters
Chapter 2. Best practices for troubleshooting

Taking advantage of certain configuration options, and ensuring vital system access information has been recorded, makes the process of troubleshooting easier.

Record access information

It is important that anyone who has responsibility for managing the system know how to connect to and log on to the system. Give attention to those times when the normal system administrators are not available because of vacation or illness.

Record the following information and ensure that authorized people know how to access the information:

- The management IP addresses. This address connects to the system using the management GUI or starts a session that runs the command-line interface (CLI) commands. The system has two Ethernet ports. Each port can have either an IPv4 address or an IPv6 address or both. Record this address and any limitations regarding where it can be accessed from within your Ethernet network.

- The service IP addresses for the control enclosure canister. These addresses are normally not needed. You might need a service IP address to access the service assistant during some recovery procedures. Use this address if the control enclosure CLI is not working. These addresses are not set during the installation of a Storwize V7000 system, but you can set these IP addresses later by using the `chserviceip` CLI command.

- The service IP address of the node canisters on the control enclosures is used only in certain circumstances. The service IP address connects to a node canister in the control enclosure. Access to the address is sometimes required if the canister has a fault that stops it from becoming an active member of the system. Each of the two node canisters can have a service IP address that is specified for Ethernet port 1. Each address can have either an IPv4 address or an IPv6 address or both. Ensure that the address specified for each node canister is different.

- The system password for user `superuser`. The password is required to access the system through the service IP address. The authentication of superuser is always local; therefore, the user ID can be used when a remote authentication server that is used for other users is not available.

Table 16. Access information for your system

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The management IP address for the GUI and CLI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The management user ID (the default is admin)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The management user ID password (the default is admin)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The control enclosure management IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control enclosure service IP address: node canister 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 16. Access information for your system (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control enclosure service IP address:</td>
<td>node canister 2</td>
<td></td>
</tr>
<tr>
<td>The control enclosure superuser password</td>
<td>(the default is passw0rd)</td>
<td></td>
</tr>
</tbody>
</table>

Follow power management procedures

Access to your volume data can be lost if you incorrectly power off all or part of a system.

Use the management GUI or the CLI commands to power off a system. Using either of these methods ensures that the data that is cached in the node canister memory is correctly flushed to the RAID arrays.

Do not power off an enclosure unless instructed to do so. If you power off an expansion enclosure, you cannot read or write to the drives in that enclosure or to any other expansion enclosure that is attached to it from the SAS ports. Powering off an expansion enclosure can prevent the control enclosure from flushing all the data that it has cached to the RAID arrays.

Remove a node canister only when directed to do so by a service action. Physically removing an active node canister means that it is unable to write any configuration data or volume data that it has cached to its internal disk and the data is lost. If both node canisters in a control enclosure are removed in quick succession, run recovery actions, which might include restoring your volume data from a backup.

Set up event notifications

Configure your system to send notifications when a new event is reported.

Correct any issues reported by your system as soon as possible. To avoid monitoring for new events by constantly monitoring the management GUI, configure your system to send notifications when a new event is reported. Select the type of event that you want to be notified about. For example, restrict notifications to just events that require immediate action. Several event notification mechanisms exist:

- Email. An event notification can be sent to one or more email addresses. This mechanism notifies individuals of problems. Individuals can receive notifications wherever they have email access which includes mobile devices.
- Simple Network Management Protocol (SNMP). An SNMP trap report can be sent to a data-center management system, such as IBM Systems Director, that consolidates SNMP reports from multiple systems. Using this mechanism, you can monitor your data center from a single workstation.
- Syslog. A syslog report can be sent to a data-center management system that consolidates syslog reports from multiple systems. Using this mechanism, you can monitor your data center from a single workstation.

If your system is within warranty, or you have a hardware maintenance agreement, configure your system to send email events to IBM if an issue that requires hardware replacement is detected. This mechanism is called Call Home. When this
event is received, IBM automatically opens a problem report, and if appropriate, contacts you to verify if replacement parts are required.

If you set up Call Home to IBM, ensure that the contact details that you configure are correct and kept up to date as personnel change.

**Set up inventory reporting**

Inventory reporting is an extension to the Call Home email.

Rather than reporting a problem, an email is sent to IBM that describes your system hardware and critical configuration information. Object names and other information, such as IP addresses, are not sent. The inventory email is sent on a regular basis. Based on the information that is received, IBM can inform you if the hardware or software that you are using requires an upgrade because of a known issue.

**Back up your data**

Back up your system configuration data and volume data.

The storage system backs up your control enclosure configuration data to a file every day. This data is replicated on each control node canister in the system. Download this file regularly to your management workstation to protect the data. This file must be used if there is a serious failure that requires you to restore your system configuration. It is important to back up this file after modifying your system configuration.

Your volume data is susceptible to failures in your host application or your Storwize V7000 system. Follow a backup and archive policy that is appropriate to the data that you have for storing the volume data on a different system.

**Manage your spare and failed drives**

Your RAID arrays that are created from drives consist of drives that are active members and drives that are spares.

The spare drives are used automatically if a member drive fails. If you have sufficient spare drives, you do not have to replace them immediately when they fail. However, monitoring the number, size, and technology of your spare drives, ensures that you have sufficient drives for your requirements. Ensure that there are sufficient spare drives available so that your RAID arrays are always online.

**Resolve alerts in a timely manner**

Your system reports an alert when there is an issue or a potential issue that requires user attention. The Storwize V7000 helps resolve these problems through the **Recommended actions only** option from the Events panel.

Perform the recommended actions as quickly as possible after the problem is reported. Your system is designed to be resilient to most single hardware failures. However, if you operate for any period of time with a hardware failure, the possibility increases that a second hardware failure can result in some volume data that is unavailable.
If there are a number of unfixed alerts, fixing any one alert might become more difficult because of the effects of the other alerts.

**Keep your software up to date**

Check for new code releases and update your code on a regular basis.

This can be done using the management GUI or check the IBM support website to see if new code releases are available:

[www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000)

The release notes provide information about new function in a release plus any issues that have been resolved. Update your code regularly if the release notes indicate an issue that you might be exposed to.

**Keep your records up to date**

Record the location information for your enclosures.

If you have only one system, it is relatively easy to identify the enclosures that make up the system. Identification becomes more difficult when you have multiple systems in your data center and multiple systems in the same rack.

The enclosure identifier that is displayed on the front of the display is unique within a system. However, the identifiers can be repeated between different systems. Do not rely solely on this identifier.

For each system, record the location of the control enclosure and the location of any expansion enclosures. It is useful to label the enclosures themselves with the system name and the management IP addresses.

**Subscribe to support notifications**

Subscribe to support notifications so that you are aware of best practices and issues that might affect your system.

Subscribe to support notifications by visiting the IBM support page on the IBM website:

[www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000)

By subscribing, you are informed of new and updated support site information, such as publications, hints and tips, technical notes, product flashes (alerts), and downloads.

**Know your IBM warranty and maintenance agreement details**

If you have a warranty or maintenance agreement with IBM, know the details that must be supplied when you call for support.

Have the phone number of the support center available. When you call support, provide the machine type (always 2076) and the serial number of the enclosure that has the problem. If the problem does not relate to a specific enclosure, provide the control enclosure serial number. The serial numbers are on the labels on the enclosures.
Support personnel also ask for your customer number, machine location, contact details, and the details of the problem.
Chapter 3. Understanding the Storwize V7000 battery operation for the control enclosure

Storwize V7000 node canisters cache volume data and hold state information in volatile memory.

If the power fails, the cache and state data is written to a local solid-state drive (SSD) in the canister. The batteries within the control enclosure provide the power to write the cache and state data to a local drive.

Note: Storwize V7000 expansion canisters do not cache volume data or store state information in volatile memory. They, therefore, do not require battery power. If ac power to both power supplies in an expansion enclosure fails, the enclosure powers off. When ac power is restored to at least one of the power supplies, the controller restarts without operator intervention.

There are two power supply units in the control enclosure. Each one contains an integrated battery. Both power supply units and batteries provide power to both control canisters. Each battery has a sufficient charge to power both node canisters for the duration of saving critical data to the local drive. In a fully redundant system with two batteries and two canisters, there is enough charge in the batteries to support saving critical data from both canisters to a local drive twice. In a system with a failed battery, there is enough charge in the remaining battery to support saving critical data from both canisters to a local drive once.

If the ac power to a control enclosure is lost, the canisters do not start saving critical data to a local drive until approximately 10 seconds after the loss of ac power is first detected. If the power is restored within this period, the system continues to operate. This loss in power is called a brown out. As soon as the saving of the critical data starts, the system stops handling I/O requests from the host applications, and Metro Mirror and Global Mirror relationships go offline. The system powers off when the saving of the critical data completes.

If both node canisters shut down without writing the cache and state data to the local drive, the system is unable to restart without an extended service action. The system configuration must be restored. If any cache write data is lost, volumes must be restored from a backup. It is, therefore, important not to remove the canisters or the power supply units from the control enclosures unless directed to do so by the service procedures. Removing either of these components might prevent the node canister from writing its cache and state data to the local drive.

When the ac power is restored to the control enclosure, the system restarts without operator intervention. How quickly it restarts depends on whether there is a history of previous power failures.

When the ac power is restored after a power outage that causes both canisters to save their critical data, the system restarts only when the batteries have sufficient charge to power both canisters for the duration of saving the critical data again. In a fully redundant system with two batteries, this condition means that after one ac power outage and a saving of critical data, the system can restart as soon as the power is restored. If a second ac power outage occurs before the batteries have
completed charging, then the system starts in service state and does not permit I/O operations to be restarted until the batteries are half charged. The recharging takes approximately 30 minutes.

In a system with a failed battery, an ac power failure causes both canisters to save critical data and completely discharges the remaining battery. When the ac power is restored, the system starts in service state and does not permit I/O operations to be restarted until the remaining battery is fully charged. The recharging takes approximately 1 hour.

A battery is considered failed for the following conditions:
- When the system can communicate with it and it reports an error.
- When the system is unable to communicate with the battery. Failed communication exists because the power supply, which contains the battery, has been removed or because the power supply has failed in a manner that makes communication with the battery impossible.

There are conditions other than loss of ac power that can cause critical data to be saved and the nodes to go into service state and not permit I/O operations. The node canister saves critical data if they detect there is no longer sufficient battery charge to support a saving of critical data. This situation happens when, for example, both batteries have two-thirds of a charge. The total charge that is available in the enclosure is sufficient to support a saving of critical data once; therefore, both canisters are in active state and I/O operations are permitted. If one battery fails though, the remaining battery has only two-thirds of a charge, and the total charge that is available in the enclosure is now insufficient to perform a saving of the critical data if the ac power fails. Data protection cannot be guaranteed in this case. When the battery has sufficient charge, the system automatically restarts.

**Important:** Although Storwize V7000 is resilient to power failures and brownouts, always install Storwize V7000 in an environment where there is reliable and consistent ac power that meets the Storwize V7000 requirements. Consider uninterruptible power supply units to avoid extended interruptions to data access.

### Maintenance discharge cycles

Maintenance discharge cycles extend the lifetime of the batteries and ensure that the system can accurately measure the charge in the batteries. Discharge cycles guarantee that the batteries have sufficient charge to protect the Storwize V7000 system.

Maintenance discharge cycles are scheduled automatically by the system and involve fully discharging a battery and then recharging it again. Maintenance discharges are normally scheduled only when the system has two fully charged batteries. This condition ensures that for the duration of the maintenance cycle, the system still has sufficient charge to complete a save of the critical data if the ac power fails. This condition also ensures that I/O operations continue while the maintenance cycle is performed. It is usual for both batteries to require a maintenance discharge at the same time. In these circumstances, the system automatically schedules the maintenance of one battery. When the maintenance on that battery completes, the maintenance on the other battery starts.

Maintenance discharges are scheduled for the following situations:
A battery has been powered on for three months without a maintenance discharge.

A battery has provided protection for saving critical data at least twice.

A battery has provided protection for at least 10 brown outs, which lasted up to 10 seconds each.

A maintenance discharge takes approximately 10 hours to complete. If the ac power outage occurs during the maintenance cycle, the cycle must be restarted. The cycle is scheduled automatically when the battery is fully charged.

Under the following conditions, a battery is not considered when calculating whether there is sufficient charge to protect the system. This condition persists until a maintenance discharge cycle is completed.

- A battery is performing a maintenance discharge.
- A battery has provided protection for saving critical data at least four times without any intervening maintenance discharge.
- A battery has provided protection for at least 20 brown outs, which lasted up to 10 seconds each.
- A battery must restart a maintenance discharge because the previous maintenance cycle was disrupted by an ac power outage.

If a system suffers repeated ac power failures without a sufficient time interval in between the ac failures to complete battery conditioning, then neither battery is considered when calculating whether there is sufficient charge to protect the system. In these circumstances, the system enters service state and does not permit I/O operations to be restarted until the batteries have charged and one of the batteries has completed a maintenance discharge. This activity takes approximately 10 hours.

If one of the batteries in a system fails and is not replaced, it prevents the other battery from performing a maintenance discharge. Not only does this condition reduce the lifetime of the remaining battery, but it also prevents a maintenance discharge cycle from occurring after the battery has provided protection for at least 2 critical saves or 10 brown outs. Preventing this maintenance cycle from occurring increases the risk that the system accumulates a sufficient number of power outages to cause the remaining battery to be discounted when calculating whether there is sufficient charge to protect the system. This condition results in the system entering service state while the one remaining battery performs a maintenance discharge. I/O operations are not permitted during this process. This activity takes approximately 10 hours.
A storage system returns a medium error response to a host when it is unable to successfully read a block. The Storwize V7000 response to a host read follows this behavior.

The volume virtualization that is provided extends the time when a medium error is returned to a host. Because of this difference to non-virtualized systems, the Storwize V7000 uses the term *bad blocks* rather than medium errors.

The Storwize V7000 allocates volumes from the extents that are on the managed disks (MDisks). The MDisk can be a volume on an external storage controller or a RAID array that is created from internal drives. In either case, depending on the RAID level used, there is normally protection against a read error on a single drive. However, it is still possible to get a medium error on a read request if multiple drives have errors or if the drives are rebuilding or are offline due to other issues.

The Storwize V7000 provides migration facilities to move a volume from one underlying set of physical storage to another or to replicate a volume that uses FlashCopy or Metro Mirror or Global Mirror. In all these cases, the migrated volume or the replicated volume returns a medium error to the host when the logical block address on the original volume is read. The system maintains tables of bad blocks to record where the logical block addresses that cannot be read are. These tables are associated with the MDisks that are providing storage for the volumes.

The dumpmdiskbadblocks command and the dumpallmdiskbadblocks command are available to query the location of bad blocks.

**Important:** The dumpmdiskbadblocks only outputs the virtual medium errors that have been created, and not a list of the actual medium errors on MDisks or drives.

It is possible that the tables that are used to record bad block locations can fill up. The table can fill either on an MDisk or on the system as a whole. If a table does fill up, the migration or replication that was creating the bad block fails because it was not possible to create an exact image of the source volume.

The system creates alerts in the event log for the following situations:
- When it detects medium errors and creates a bad block
- When the bad block tables fill up

The following errors are identified:

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1840</td>
<td>The managed disk has bad blocks. On an external controller, this can only be a copied medium error.</td>
</tr>
<tr>
<td>1226</td>
<td>The system has failed to create a bad block because the MDisk already has the maximum number of allowed bad blocks.</td>
</tr>
</tbody>
</table>
Table 17. Bad block errors (continued)

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1225</td>
<td>The system has failed to create a bad block because the system already has the maximum number of allowed bad blocks.</td>
</tr>
</tbody>
</table>

The recommended actions for these alerts guide you in correcting the situation.

Clear bad blocks by deallocating the volume disk extent, by deleting the volume or by issuing write I/O to the block. It is good practice to correct bad blocks as soon as they are detected. This action prevents the bad block from being propagated when the volume is replicated or migrated. It is possible, however, for the bad block to be on part of the volume that is not used by the application. For example, it can be in part of a database that has not been initialized. These bad blocks are corrected when the application writes data to these areas. Before the correction happens, the bad block records continue to use up the available bad block space.
Chapter 5. Storwize V7000 user interfaces for servicing your system

Storwize V7000 provides a number of user interfaces to troubleshoot, recover, or maintain your system. The interfaces provide various sets of facilities to help resolve situations that you might encounter.

The interfaces for servicing your system connect through the 1 Gbps Ethernet ports that are accessible from port 1 of each canister. You cannot manage a system using the 10 Gbps Ethernet ports.

- Use the initialization tool to do the initial setup of your system.
- Use the management GUI to monitor and maintain the configuration of storage that is associated with your clustered systems.
- Perform service procedures from the service assistant.
- Use the command-line interface (CLI) to manage your system.

Management GUI interface

The management GUI is a browser-based GUI for configuring and managing all aspects of your system. It provides extensive facilities to help troubleshoot and correct problems.

About this task

You use the management GUI to manage and service your system. The Monitoring > Events panel provides access to problems that must be fixed and maintenance procedures that step you through the process of correcting the problem.

The information on the Events panel can be filtered three ways:

**Recommended actions (default)**

Shows only the alerts that require attention. Alerts are listed in priority order and should be fixed sequentially by using the available fix procedures. For each problem that is selected, you can:

- Run a fix procedure.
- View the properties.

**Unfixed messages and alerts**

Displays only the alerts and messages that are not fixed. For each entry that is selected, you can:

- Run a fix procedure.
- Mark an event as fixed.
- Filter the entries to show them by specific minutes, hours, or dates.
- Reset the date filter.
- View the properties.

**Show all**

Displays all event types whether they are fixed or unfixed. For each entry that is selected, you can:

- Run a fix procedure.
- Mark an event as fixed.
Filter the entries to show them by specific minutes, hours, or dates.
Reset the date filter.
View the properties.

Some events require a certain number of occurrences in 25 hours before they are displayed as unfixed. If they do not reach this threshold in 25 hours, they are flagged as expired. Monitoring events are below the coalesce threshold and are usually transient.

You can also sort events by time or error code. When you sort by error code, the most serious events, those with the lowest numbers, are displayed first. You can select any event that is listed and select Actions > Properties to view details about the event.

When to use the management GUI
The management GUI is the primary tool that is used to service your system.

Regularly monitor the status of the system using the management GUI. If you suspect a problem, use the management GUI first to diagnose and resolve the problem.

Use the views that are available in the management GUI to verify the status of the system, the hardware devices, the physical storage, and the available volumes. The Monitoring > Events panel provides access to all problems that exist on the system. Use the Recommended Actions filter to display the most important events that need to be resolved.

If there is a service error code for the alert, you can run a fix procedure that assists you in resolving the problem. These fix procedures analyze the system and provide more information about the problem. They suggest actions to take and step you through the actions that automatically manage the system where necessary. Finally, they check that the problem is resolved.

If there is an error that is reported, always use the fix procedures within the management GUI to resolve the problem. Always use the fix procedures for both system configuration problems and hardware failures. The fix procedures analyze the system to ensure that the required changes do not cause volumes to be inaccessible to the hosts. The fix procedures automatically perform configuration changes that are required to return the system to its optimum state.

Accessing the management GUI
This procedure describes how to access the management GUI.

About this task
You must use a supported web browser. Verify that you are using a supported web browser from the following website:

www.ibm.com/storage/support/storwize/v7000

You can use the management GUI to manage your system as soon as you have created a clustered system.
Procedure

1. Start a supported web browser and point the browser to the management IP address of your system.
   The management IP address is set when the clustered system is created. Up to four addresses can be configured for your use. There are two addresses for IPv4 access and two addresses for IPv6 access.
2. When the connection is successful, you see a login panel.
3. Log on by using your user name and password.
4. When you have logged on, select Monitoring > Events.
5. Ensure that the events log is filtered using Recommended actions.
6. Select the recommended action and run the fix procedure.
7. Continue to work through the alerts in the order suggested, if possible.

Results

After all the alerts are fixed, check the status of your system to ensure that it is operating as intended.

If you encounter problems logging on the management GUI or connecting to the management GUI, see “Problem: Unable to log on to the management GUI” on page 45 or “Problem: Unable to connect to the management GUI” on page 44.

Service assistant interface

The service assistant interface is a browser-based GUI that is used to service individual node canisters in the control enclosures.

You connect to the service assistant on one node canister through the service IP address. If there is a working communications path between the node canisters, you can view status information and perform service tasks on the other node canister by making the other node canister the current node. You do not have to reconnect to the other node.

When to use the service assistant

The primary use of the service assistant is when a node canister in the control enclosure is in service state. The node canister cannot be active as part of a system while it is in service state.

Attention: Perform service actions on node canisters only when directed to do so by the fix procedures. If used inappropriately, the service actions that are available through the service assistant can cause loss of access to data or even data loss.

The node canister might be in service state because it has a hardware issue, has corrupted data, or has lost its configuration data.

Use the service assistant in the following situations:

- When you cannot access the system from the management GUI and you cannot access the storage Storwize V7000 to run the recommended actions
- When the recommended action directs you to use the service assistant.

The storage system management GUI operates only when there is an online system. Use the service assistant if you are unable to create a system or if both node canisters in a control enclosure are in service state.
The service assistant does not provide any facilities to help you service expansion enclosures. Always service the expansion enclosures by using the management GUI.

The service assistant provides detailed status and error summaries, and the ability to modify the World Wide Node Name (WWN) for each node.

You can also perform the following service-related actions:

- Collect logs to create and download a package of files to send to support personnel.
- Remove the data for the system from a node.
- Recover a system if it fails.
- Install a code package from the support site or rescue the code from another node.
- Upgrade code on node canisters manually versus performing a standard upgrade procedure.
- Configure a control enclosure chassis after replacement.
- Change the service IP address that is assigned to Ethernet port 1 for the current node canister.
- Install a temporary SSH key if a key is not installed and CLI access is required.
- Restart the services used by the system.

A number of tasks that are performed by the service assistant cause the node canister to restart. It is not possible to maintain the service assistant connection to the node canister when it restarts. If the current node canister on which the tasks are performed is also the node canister that the browser is connected to and you lose your connection, reconnect and log on to the service assistant again after running the tasks.

**Accessing the service assistant**

The service assistant is a web application that helps troubleshoot and resolve problems on a node canister in a control enclosure.

**About this task**

You must use a supported web browser. Verify that you are using a supported and appropriately configured web browser from the following website:

[www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000)

To start the application, perform the following steps:

**Procedure**

1. Start a supported web browser and point your web browser to `<serviceaddress>/service` for the node canister that you want to work on.
   
   For example, if you set a service address of 11.22.33.44 for a node canister, point your browser to 11.22.33.44/service. If you are unable to connect to the service assistant, see "Problem: Cannot connect to the service assistant” on page 47.
2. Log on to the service assistant using the superuser password.
If you are accessing a new node canister, the default password is password. If the node canister is a member of a system or has been a member of a system, use the password for the superuser password.

If you do not know the current superuser password, reset the password. Go to "Procedure: Resetting superuser password" on page 51.

Results

Perform the service assistant actions on the correct node canister. If you did not connect to the node canister that you wanted to work on, access the Change Node panel from the home page to select a different current node.

Commands are run on the current node. The current node might not be the node canister that you connected to. The current node identification is shown on the left at the top of the service assistant screen. The identification includes the enclosure serial number, the slot location, and if it has one, the node name of the current node.

Cluster (system) command-line interface

Use the command-line interface (CLI) to manage a clustered system using the task commands and information commands.

For a full description of the commands and how to start an SSH command-line session, see the “Command-line interface” topic in the “Reference” section of the Storwize V7000 Information Center.

When to use the cluster (system) CLI

The cluster (system) CLI is intended for use by advanced users who are confident at using a command-line interface.

Nearly all of the flexibility that is offered by the CLI is available through the management GUI. However, the CLI does not provide the fix procedures that are available in the management GUI. Therefore, use the fix procedures in the management GUI to resolve the problems. Use the CLI when you require a configuration setting that is unavailable in the management GUI.

You might also find it useful to create command scripts using the CLI commands to monitor for certain conditions or to automate configuration changes that you make on a regular basis.

Accessing the cluster (system) CLI

Follow the steps that are described in the “Command-line interface” topic in the “Reference” section of the Storwize V7000 Information Center to initialize and use a CLI session.

Service command-line interface

Use the service command-line interface (CLI) to manage a node canister in a control enclosure using the task commands and information commands.

For a full description of the commands and how to start an SSH command-line session, see the “Command-line interface” topic in the “Reference” section of the Storwize V7000 Information Center.
When to use the service CLI

The service CLI is intended for use by advanced users who are confident at using a command-line interface.

To access a node canister directly, it is normally easier to use the service assistant with its graphical interface and extensive help facilities.

Accessing the service CLI

Follow the steps that are described in the “Command-line interface” topic in the “Reference” section of the Storwize V7000 Information Center to initialize and use a CLI session.

USB flash drive and Initialization tool interface

Use a USB flash drive to initialize a system and also to help service the node canisters in a control enclosure.

The initialization tool is a Windows application. Use the initialization tool to set up the USB flash drive to perform the most common tasks.

When a USB flash drive is inserted into one of the USB ports on a node canister in a control enclosure, the node canister searches for a control file on the USB flash drive and runs the command that is specified in the file. When the command completes, the command results and node status information are written to the USB flash drive.

When to use the USB flash drive

The USB flash drive is normally used to initialize the configuration after installing a new system.

Using the USB flash drive is required in the following situations:

- When you cannot connect to a node canister in a control enclosure using the service assistant and you want to see the status of the node.
- When you do not know, or cannot use, the service IP address for the node canister in the control enclosure and must set the address.
- When you have forgotten the superuser password and must reset the password.

Using a USB flash drive

Use any USB flash drive that is formatted with a FAT32 file system on its first partition.

About this task

When a USB flash drive is plugged into a node canister, the node canister code searches for a text file named satask.txt in the root directory. If the code finds the file, it attempts to run a command that is specified in the file. When the command completes, a file called satask_result.html is written to the root directory of the USB flash drive. If this file does not exist, it is created. If it exists, the data is inserted at the start of the file. The file contains the details and results of the command that was run and the status and the configuration information from the node canister. The status and configuration information matches the detail that is shown on the service assistant home page panels.
The satask.txt file can be created on any workstation by using a text editor. If a Microsoft Windows workstation is being used, the initialization tool can be used to create the commands that are most often used.

The fault LED on the node canister flashes when the USB service action is being performed. When the fault LED stops flashing, it is safe to remove the USB flash drive.

**Results**

The USB flash drive can then be plugged into a workstation and the satask_result.html file viewed in a web browser.

To protect from accidentally running the same command again, the satask.txt file is deleted after it has been read.

If no satask.txt file is found on the USB flash drive, the result file is still created, if necessary, and the status and configuration data is written to it.

**Using the initialization tool**

The initialization tool is a graphical user interface (GUI) application. You must have Microsoft Windows XP Professional or higher to run the application.

**About this task**

The initialization tool is available on the USB flash drive that is shipped with the control enclosures. The name of the application file is InitTool.exe. If you cannot locate the USB flash drive, you can download the application from the support website (search for initialization tool):

[www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000)

If you download the initialization tool, you must copy the file onto the USB flash drive that you are going to use.

To start the initialization tool, insert the USB flash drive that contains the program into a USB slot on a suitable personal computer. Run the InitTool.exe program from the USB drive.

The initialization tool is used to create the satask.txt file on a USB flash drive. After the satask.txt file is created, follow the instructions in "Using a USB flash drive" on page 36 to run the commands on the node.

The initialization tool prompts you for the task that you want to perform and for the parameters that are relevant to that task. It prompts you when to put it in the node canister on the control enclosure. When the commands have run, return the USB flash drive to your personal computer and start the tool again to see the results.

**Results**

By using the initialization tool, you can set the USB flash drive to run one of the following tasks:
- Create a new system.
- Reset the superuser password.
• Set or reset the service IP address on the node canister on the control enclosure.

For any other tasks that you want to perform on a node canister on the control enclosure, you must create the `satask.txt` file using a text editor.

**satask.txt commands**

This topic identifies the commands that can be run from a USB flash drive.

If you are creating the `satask.txt` command file by using a text editor, the file must contain a single command on a single line in the file. The commands that you use are the same as the service CLI commands except where noted. Not all service CLI commands can be run from the USB flash drive. The `satask.txt` commands always run on the node that the USB flash drive is plugged into.

**Reset service IP address and superuser password command**

Use this command to obtain service assistant access to a node canister even if the current state of the node canister is unknown. The physical access to the node canister is required and is used to authenticate the action.

**Syntax**

```bash
satask chserviceip -serviceip ipv4 -gw ipv4 -mask ipv4 -resetpassword
```

```bash
satask chserviceip -serviceip_6 ipv6 -gw_6 ipv6 -prefix_6 int -resetpassword
```

```bash
satask chserviceip --default -resetpassword
```

**Parameters**

- `-serviceip`
  
  (Optional) The IPv4 address for the service assistant.

- `-gw`
  
  (Optional) The IPv4 gateway for the service assistant.

- `-mask`
  
  (Optional) The IPv4 subnet for the service assistant.

- `-serviceip_6`
  
  (Optional) The IPv6 address for the service assistant.

- `-gw_6`
  
  (Optional) The IPv6 gateway for the service assistant.

- `-default`
  
  (Optional) Resets to the default IPv4 address.

- `-prefix_6`
  
  (Optional) The IPv6 prefix for the service assistant.

- `-resetpassword`
  
  (Optional) Sets the service assistant password to the default value.
Description

This command resets the service assistant IP address to the default value. If the command is run on the upper canister, the default value is 192.168.70.121 subnet mask: 255.255.255.0. If the command is run on the lower canister, the default value is 192.168.70.122 subnet mask: 255.255.255.0. If the node canister is active in a system, the superuser password for the system is reset; otherwise, the superuser password is reset on the node canister.

If the node canister becomes active in a system, the superuser password is reset to that of the system. You can configure the system to disable resetting the superuser password. If you disable that function, this action fails.

This action calls the satask chserviceip command and the satask resetpassword command.

Reset service assistant password command

Use this command when you are unable to logon to the system because you have forgotten the superuser password, and you wish to reset it.

Syntax

```
>>> satask — resetpassword —
```

Parameters

None.

Description

This command resets the service assistant password to the default value password. If the node canister is active in a system, the superuser password for the system is reset; otherwise, the superuser password is reset on the node canister.

If the node canister becomes active in a system, the superuser password is reset to that of the system. You can configure the system to disable resetting the superuser password. If you disable that function, this action fails.

This command calls the satask resetpassword command.

Snap command

Use this command to collect diagnostic information from the node canister and to write the output to a USB flash drive.

Syntax

```
>>> satask — snap — —options—
```

Parameters

- `—options`  
  (Optional) Specifies which diagnostic information to collect.
Description

This command moves a snap file to a USB flash drive.

This command calls the `satask snap` command.

Apply software command

Use this command to install a specific upgrade package on the node canister.

Syntax

```
>>> satask --installsoftware --file filename --ignore
```

Parameters

- `-file` (Required) The file name of upgrade package.

- `-ignore` (Optional) Overrides prerequisite checking and forces installation of the upgrade package.

Description

This command copies the file from the USB flash drive to the upgrade directory on the node canister and then installs the upgrade package.

This command calls the `satask installsoftware` command.

Create cluster command

Use this command to create a storage system.

Syntax

```
>>> satask --mkcluster --clusterip ipv4 --gw ipv4 --mask ipv4 --name cluster_name
```

```
>>> satask --mkcluster --clusterip_6 ipv6 --gw_6 ipv6 --prefix_6 int --name --cluster_name
```

Parameters

- `-clusterip` (Optional) The IPv4 address for Ethernet port 1 on the system.

- `-gw` (Optional) The IPv4 gateway for Ethernet port 1 on the system.

- `-mask` (Optional) The IPv4 subnet for Ethernet port 1 on the system.

- `-clusterip_6` (Optional) The IPv6 address for Ethernet port 1 on the system.

- `-gw_6` (Optional) The IPv6 gateway for Ethernet port 1 on the system.
-prefix_6
  (Optional) The IPv6 prefix for Ethernet port 1 on the system.
-name
  (Optional) The name of the new system.

Description
This command creates a storage system.
This command calls the satask mkcluster command.

Query status command
Use this command to determine the current service state of the node canister.

Syntax

```
        sainfo - getstatus
```

Parameters
None.

Description
This command writes the output from each node canister to the USB flash drive.
This command calls the sainfo lsservicenodes command, the sainfo lsservicestatus command, and the sainfo lsservicerecommendation command.
Chapter 6. Resolving a problem

Described here are some procedures to help resolve fault conditions that might exist on your system and which assume a basic understanding of the Storwize V7000 system concepts.

The following procedures are often used to find and resolve problems:
- Procedures that involve data collection and system configuration
- Procedures that are used for hardware replacement.

Always use the recommended actions on the Events panel of the management GUI as the starting point to diagnose and resolve a problem.

The following topics describe a type of problem that you might experience, that is not resolved by using the management GUI. In those situations, review the symptoms and follow the actions that are provided here.

The “Start here: Use the management GUI recommended actions” topic gives the starting point for any service action. The situations covered in this section are the cases where you cannot start the management GUI or the node canisters in the control enclosure are unable to run the system software.

Note: After you have created your clustered system, remove hardware components only when directed to do so by the fix procedures. Failure to follow the procedures can result in loss of access to data or loss of data. Follow the fix procedures when servicing a control enclosure.

Start here: Use the management GUI recommended actions

The management GUI provides extensive facilities to help you troubleshoot and correct problems on your system.

You can connect to and manage a Storwize V7000 system using the management GUI as soon as you have created a clustered system. If you cannot create a clustered system, see the problem that contains information about what to do if you cannot create one. Go to “Problem: Cannot create a clustered storage system” on page 46.

To run the management GUI, start a supported web browser and point it to the management IP address of your system. Up to four addresses can be configured for your use. There are two addresses for IPv4 access, and two addresses for IPv6 access. If you do not know the system management IP address, go to “Problem: Management IP address unknown” on page 44. After the connection is successful, you see a login panel. If you are unable to access the login panel, go to “Problem: Unable to connect to the management GUI” on page 44.

Log on using your user name and password. If you are unable to log on, go to “Problem: Unable to log on to the management GUI” on page 45.
When you have logged on, select **Monitoring > Events**. Depending on how you choose to filter alerts, you might see only the alerts that require attention, alerts and messages that are not fixed, or all event types whether they are fixed or unfixed.

Select the recommended alert, or any other alert, and run the fix procedure. The fix procedure steps you through the process of troubleshooting and correcting the problem. The fix procedure displays information that is relevant to the problem and provides various options to correct the problem. Where it is possible, the fix procedure runs the commands that are required to reconfigure the system.

Always use the recommended action for an alert because these actions ensure that all required steps are taken. Use the recommended actions even in cases where the service action seems obvious, such as a drive showing a fault. In this case, the drive must be replaced and reconfiguration must be performed. The fix procedure performs the reconfiguration for you.

The fix procedure also checks that another existing problem does not result in a fix procedure that causes volume data to be lost. For example, if a power supply unit in a node enclosure must be replaced, the fix procedure checks and warns you if the integrated battery in the other power supply unit is not sufficiently charged to protect the system.

If possible, fix the alerts in the order shown to resolve the most serious issues first. Often, other alerts are fixed automatically because they were the result of a more serious issue.

After all the alerts are fixed, go to "Procedure: Checking the status of your system" on page 52.

---

**Problem: Management IP address unknown**

This topic helps you if you are not able to run the management GUI because you do not know the IP address. This address is also known as the management IP address.

The management IP address is set when the clustered system is created. An address for port 2 can be added after the clustered system is created.

If you do not know the management IP address, it is part of the data that is shown in the service assistant home panel or the data that is returned by the USB flash drive. If you know the service address of a node canister, go to "Procedure: Getting node canister and system information using the service assistant" on page 53.

---

**Problem: Unable to connect to the management GUI**

If you are unable to connect to the management GUI from your web browser and received a **Page not found** or similar error, this information might help you resolve the issue.

Consider the following possibilities if you are unable to connect to the management GUI:

- You cannot connect if the system is not operational with at least one node online. If you know the service address of a node canister, go to "Procedure:
Getting node canister and system information using the service assistant” on page 53, otherwise, go to “Procedure: Getting node canister and system information using a USB flash drive” on page 53 and obtain the state of each of the node canisters from the data that is returned. If there is not a node canister with a state of active, resolve the reason why it is not in active state. If the state of both node canisters is candidate, then there is not a clustered system to connect to. If the node state is service, go to “Procedure: Fixing node errors” on page 60.

- Ensure that you are using the correct system IP address. If you know the service address of a node canister, go to “Procedure: Getting node canister and system information using the service assistant” on page 53, otherwise, go to “Procedure: Getting node canister and system information using a USB flash drive” on page 53, and obtain the management IP address from the data that is returned.

- Ensure that all node canisters have an Ethernet cable that is connected to port 1 and that the port is working. To understand the port status, go to “Procedure: Finding the status of the Ethernet connections” on page 59.

- Ping the management address to see if the Ethernet network permits the connection. If the ping fails, check the Ethernet network configuration to see if there is a routing or a firewall issue. Ensure that the Ethernet network configuration is compatible with the gateway and subnet or prefix settings. Ensure that you have not used the Ethernet address of another device as the management address. If necessary, modify your network settings to establish a connection.

- If the system IP address settings are incorrect for your environment, take these steps:
  1. Determine the service address of the configuration node canister. You can determine this if you can access the service assistant on any node canister, alternatively use the summary data returned, when a USB flash drive is plugged into a node canister.
  2. You can temporarily run the management GUI on the service address of the configuration node. Point your browser to service address/gui. For example, if the service address of the configuration node is 11.22.33.44, point your browser to 11.22.33.44/gui.
  3. Use the options in the settings > network panel to change the management IP settings.
  4. As an alternative to using the management GUI, you can use the chsystemip CLI command to correct the system IP address settings by using ssh to the service IP of the configuration node.

---

**Problem: Unable to log on to the management GUI**

This topic assists you when you can see the management GUI login screen but cannot log on.

Log on using your user name and password. Follow the suggested actions when you encounter a specific situation:

- If you are not logging on as superuser, contact your system administrator who can verify your user name and reset your account password.

- If the user name that you are using is authenticated through a remote authentication server, verify that the server is available. If the authentication server is unavailable, you can log on as user name superuser. This user is always authenticated locally.
**Problem: Cannot create a clustered storage system**

This topic helps if your attempt to create a clustered storage system has failed.

The failure is reported regardless of the method that you used to create a clustered storage system:
- USB flash drive
- management console
- Service assistant
- Service command line

The create clustered-system function protects the system from loss of volume data.

If you create a clustered system on a control enclosure that was previously used, you lose all of the volumes that you previously had. To determine if there is an existing system, use data that is returned by the create clustered-system function.

- The node canister that you are attempting to create a clustered system on is in candidate state. The node canister is in candidate state if it is a new canister.
- The partner node canister in the control enclosure is not in active state.
- The latest system ID of the control enclosure is 0.

If the create function failed because there is an existing system, fix the existing clustered system; do not re-create a new clustered system. If you want to create a clustered system and do not want to use any data from the volumes used in the previous clustered system, go to “Procedure: Deleting a system completely” on page 60, and then run the create function again.

You might not be able to create a cluster if the node canister (the one on which you are attempting to create the clustered system) is in service state. Check whether the node canister is in service state by using the data returned by the create clustered-system function.

- If the node is in service state, fix the reported node errors. For more information, go to “Procedure: Fixing node errors” on page 60. After the node error is corrected, attempt to create a clustered storage system again.

---

**Problem: Node canister service IP address unknown**

This topic describes the methods that you can use to determine the service address of a node canister.

If you are able to access the management GUI, the service IP addresses of the node canisters are shown by selecting a node and port at Settings > Network > Service IP Addresses.

If you are unable to access the management GUI but you know the management IP address of the system, you can use the address to log into the service assistant that is running on the configuration node.
1. Point your browser at the /service directory of the management IP address of the system. If your management IP address is 11.22.33.44, point your web browser to 11.22.33.44/service.

2. Log into the service assistant.

3. The service assistant home page lists the node canister that can communicate with the node.

4. If the service address of the node canister that you are looking for is listed in the Change Node window, make the node the current node. Its service address is listed under the Access tab of the node details.

If you know the service IP address of any node canister in the system, you can log into the service assistant of that node. Follow the previous instructions for using the service assistant, but at step 1, point your browser at the /service directory of the service IP address you know. If you know a service IP address is 11.22.33.56, point your web browser to 11.22.33.56/service.

Some types of errors can prevent nodes from communicating with each other; in that event, it might be necessary to point your browser directly at the service assistant of the node that requires administering, rather than change the current node in the service assistant.

If you are unable to find the service address of the node using the management GUI or service assistant, you can also use a USB flash drive to find it. For more information, see "Procedure: Getting node canister and system information using a USB flash drive" on page 53.

---

Problem: Cannot connect to the service assistant

This topic provides assistance if you are unable to display the service assistant on your browser.

You might encounter a number of situations when you cannot connect to the service assistant.

- Check that you have entered the "/service" path after the service IP address. Point your web browser to <control enclosure management IP address>/service for the node that you want to work on. For example, if you set a service address of 11.22.33.44 for a node canister, point your browser to 11.22.33.44/service.

- Check that you are using the correct service address for the node canister. To find the IPv4 and IPv6 addresses that are configured on the node, go to "Problem: Node canister service IP address unknown" on page 46. Try accessing the service assistant through these addresses. Verify that the IP address, subnet, and gateway are specified correctly for IPv4 addresses. Verify that the IP address, prefix, and gateway are specified for the IPv6 addresses. If any of the values are incorrect, see "Procedure: Changing the service IP address of a node canister" on page 61.

- You cannot connect to the service assistant if the node canister is not able to start the Storwize V7000 code. To verify that the LEDs indicate that the code is active, see "Procedure: Understanding the system status using the LEDs" on page 54.

- The service assistant is configured on Ethernet port 1 of a node canister. Verify that an Ethernet cable is connected to this port and to an active port on your Ethernet network. See "Procedure: Finding the status of the Ethernet connections" on page 59 for details.
• Ping the management address to see if the Ethernet network permits the connection. If the ping fails, check the Ethernet network configuration to see if there is a routing or a firewall issue. Check that the Ethernet network configuration is compatible with the gateway and subnet or prefix settings. Check that you have not used an address that is used by another device on your Ethernet network. If necessary, change the network configuration or see “Procedure: Changing the service IP address of a node canister” on page 61 to change the service IP address of a node.

• A default service address is initially assigned to each node canister. The service IP address 192.168.70.121 subnet mask 255.255.255.0 is preconfigured on Ethernet port 1 of the upper canister, canister 1. The service IP address 192.168.70.122 subnet mask 255.255.255.0 is preconfigured on Ethernet port 2 of the lower canister, canister 2.

You might not be able to access these addresses because of the following conditions:
- These addresses are the same as the addresses that are used by other devices on the network.
- These addresses cannot be accessed on your network.
- There are other reasons why they are not suitable for use on your network.

If the previous conditions apply, see “Procedure: Changing the service IP address of a node canister” on page 61 to change the service IP address to one that works in your environment.

If you are unable to change the service address, for example, because you cannot use a USB flash drive in the environment, see “Procedure: Accessing a canister using a directly attached Ethernet cable” on page 64.

### Problem: Management GUI or service assistant does not display correctly

This topic provides assistance if the Management GUI or the service assistant does not display correctly.

You must use a supported web browser. Verify that you are using a supported web browser from the following website:

www.ibm.com/storage/support/storwize/v7000

Switch to using a supported web browser. If the problem continues, contact IBM Support.

### Problem: A node canister has a location node error

The node error that is listed on the service assistant home page or in the event log can indicate a location error.

The node error, that is listed on the service assistant home page, can be classified as a location error. This indicates that the node canister, or the enclosure midplane has been moved or changed. This is normally due to a service action not being completed or not being implemented correctly.

There are a number of different conditions that report as a location error. Each condition is indicated by different node error. To find out how to resolve the node error, go to “Procedure: Fixing node errors” on page 60.
Be aware that after a node canister has been used in a system, the node canister must not be moved to a different location, either within the same enclosure or in a different enclosure because this might compromise its access to storage, or a host application’s access to volumes. Do not move the canister from its original location unless directed to do so by a service action.

Problem: SAS cabling not valid

This topic provides information to be aware of if you receive errors that indicate the SAS cabling is not valid.

Check the following items:

• No more than five expansion enclosures can be chained to port 1 (below the control enclosure). The connecting sequence from port 1 of the node canister is called chain 1.
• No more than four expansion enclosures can be chained to port 2 (above the control enclosure). The connecting sequence from port 2 of the node canister is called chain 2.
• Do not connect a SAS cable between a port on an upper canister and a port on a lower canister.
• In any enclosure, the same ports must be used on both canisters.
• No SAS cable can be connected between ports in the same enclosure.
• For any enclosure, the cables that are connected to SAS port 1 on each canister must attach to the same enclosure. Similarly, for any enclosure, the cables that are connected to SAS port 2 on each canister must attach to the same enclosure. Cable attachments for SAS port 1 and cable attachments for SAS port 2 do not go to the same enclosure.
• For cables connected between expansion enclosures, one end is connected to port 1 while the other end is connected to port 2.
• For cables that are connected between a control enclosure and expansion enclosures, port 1 must be used on the expansion enclosures.
• The last enclosure in a chain must not have cables in port 2 of canister 1 and port 2 of canister 2.
• Ensure that each SAS cable is fully inserted.

Problem: New expansion enclosure not detected

This topic helps you resolve why a newly installed expansion enclosure was not detected by the system.

When installing a new expansion enclosure, follow the management GUI Add Enclosure wizard, which is available from the Manage Devices Actions menu.

If the expansion enclosure is not detected, perform the following verifications:

• Verify the status of the LEDs at the back of the expansion enclosure. At least one power supply unit must be on with no faults shown. At least one canister must be active, with no fault LED on, and all the serial-attached SCSI (SAS) port 1 LEDs must be on. For details about the LED status, see "Procedure: Understanding the system status using the LEDs" on page 54.
• Verify that the SAS cabling to the expansion enclosure is correctly installed. To review the requirements, see "Problem: SAS cabling not valid."
Problem: Control enclosure not detected

If a control enclosure is not detected by the system, this procedure may help you resolve the problem.

When installing a new control enclosure, follow the management GUI Add Control and Expansion Enclosures wizard, which is available from the Monitoring > System Details menu. After selecting the control enclosure from the navigation tree, click the Actions menu, and then select Add Enclosures > Control and Expansions.

If the control enclosure is not detected, check the following items:
- The enclosure is powered on.
- The enclosure is not part of another system.
- At least one node is in candidate state.
- The Fibre Channel cables are connected and zoning is set up according to the zoning rules defined in the SAN configuration and zoning rules summary topic. There must be a zone that includes all ports from all node canisters.
- The existing system and the nodes in the enclosure that are not detected have Storwize V7000 6.2 or later installed.

Problem: Mirrored volume copies no longer identical

The management GUI provides options to either check copies that are identical or to check that the copies are identical and to process any differences that are found.

To confirm that the two copies of a mirrored volume are still identical, choose the volume view that works best for you. Select one of the volume copies in the volume that you want to check. From the Actions menu, select the Validate Volume Copies option.

You have the following choices:
- Validate that the volume copies are identical.
- Validate that the volume copies are identical, mark, and repair any differences that are found.

If you want to resolve any differences, you have the following options:
- Consider that one volume is correct and make the other volume copy match the other copy if any differences are found. The primary volume copy is the copy that is considered correct.
- Do not assume that either volume copy is correct. If a difference is found, the sector is marked. A media error is returned if the volume is read by a host application.

Problem: Command file not processed from USB flash drive

This information assists you in determining why the command file is not being processed, when using a USB flash drive.

You might encounter this problem during initial setup or when running commands if you are using your own USB flash drive rather than the USB flash drive that was packaged with your order.
If you encounter this situation, verify the following items:

- That an `satask_result.html` file is in the root directory on the USB flash drive. If the file does not exist, then the following problems are possible:
  - The USB flash drive is not formatted with the correct file system type. Use any USB flash drive that is formatted with FAT32 file system on its first partition; for example, NTFS is not a supported type. Reformat the key or use a different key.
  - The USB port is not working. Try the key in the other USB port.
  - The node is not operational. Check the node status using the LEDs. See "Procedure: Understanding the system status using the LEDs" on page 54.

- If there is a `satask_result.html` file, check the first entry in the file. If there is no entry that matches the time the USB flash drive was used, it is possible that the USB port is not working or the node is not operational. Check the node status using the LEDs. See "Procedure: Understanding the system status using the LEDs" on page 54.

- If there is a status output for the time the USB flash drive was used, then the `satask.txt` file was not found. Check that the file was named correctly. The `satask.txt` file is automatically deleted after it has been processed.

---

**Procedure: Resetting superuser password**

You can reset the superuser password to the default password of `password` by using a USB flash drive command action.

**About this task**

You can use this procedure to reset the superuser password if you have forgotten the password. This command runs differently depending on whether you run it on a node canister that is active in a clustered system.

**Note:** If a node canister is not in active state, the superuser password is still required to log on to the service assistant.

It is possible to configure your system so that resetting the superuser password with the USB flash drive command action is not permitted. If your system is configured this way, there is no work-around. Contact the person who knows the password.

To use a USB flash drive to reset the superuser password, see "USB flash drive and initialization tool interface" on page 36.

See also "Problem: Unable to log on to the management GUI" on page 45.

**Results**

If the node canister is active in a clustered system, the password for superuser is changed on the clustered system. If the node canister is not in active state, the superuser password for the node canister is changed. If the node canister joins a clustered system later, the superuser password is reset to that of the clustered system.

---

**Procedure: Identifying which enclosure or canister to service**

Use this procedure to identify which enclosure or canister must be serviced.
About this task

Procedure

Use the following options to identify an enclosure. An enclosure is identified by its ID and serial number.

- The ID is shown on the LCD panel on the front left of the enclosure. The serial number is also found on the front left end cap of the enclosure and is repeated on the rear left flange of the enclosure. The enclosure ID is unique within a Storwize V7000 system. However, if you have more than one Storwize V7000 system, the same ID can be used within more than one system. The serial number is always unique.

Note: Use the Manage Device options from the management GUI to change the ID of an enclosure. Use this option to set a unique ID on all your enclosures.

- Within an enclosure, a canister is identified by its slot location. Slot 1 is the upper canister. Slot 2 is the lower canister. A canister is uniquely identified by the enclosure that it is in and the slot location. The ID can be shown as E-C or E|C where E is the enclosure ID and C is the canister location. On the service assistant, the ID is known as the Panel.

Note: When a node canister is added to a clustered system as a node, it is given a node name and a node ID. The default node name is nodeN, where N is an integer number. This number does not represent the slot location of the node. Similarly, the node ID does not indicate the slot location. The Manage Device > Canister panel from the management GUI shows both the node name and the canister location. The service assistant home page also shows both the node name and the canister location. If you have only the node name, use these panels to determine the node canister location.

- Use the service assistant to identify a node canister by turning on the identify LED of the containing enclosure. This option is at the upper left of the service assistant page. It is a good practice to identify a node in this way before performing any service action. Performing a service action on the wrong canister can lead to loss of access to data or loss of data.

Procedure: Checking the status of your system

Use this procedure to verify the status of objects in your system using the management GUI. If the status of the object is not online, view the alerts and run the recommended fix procedures.

About this task

Volumes normally show offline because another object is offline. A volume is offline if one of the MDisks that makes up the storage pool that it is in is offline. You do not see an alert that relates to the volume; instead, the alert relates to the MDisk. Performing the fix procedures for the MDisk enables the volume to go online.

Procedure

Use the following management GUI functions to find a more detailed status:

- Monitoring > System Details
- Pools > MDisks by Pools
Volumes > Volumes
Monitoring > Events, and then use the filtering options to display alerts, messages, or event types.

Procedure: Getting node canister and system information using the service assistant

This procedure explains how to view information about the node canisters and system using the service assistant.

About this task

To obtain the information:
1. Log on to the service assistant, as described in “Accessing the service assistant” on page 34
2. View the information about the node canister to which you connected or the other node canister in the enclosure. To change which node’s information is shown, select the node in the Change Node table of the Home page.

The Home page shows a table of node errors that exist on the node canister and a table of node details for the current node. The node errors are shown in priority order.

The node details are divided into several sections. Each section has a tab. Examine the data that is reported in each tab for the information that you want.
- The Node tab shows general information about the node canister that includes the node state and whether it is a configuration node.
- The Hardware tab shows information about the hardware.
- The Access tab shows the management IP addresses and the service addresses for this node.
- The Location tab identifies the enclosure in which the node canister is located.
- The Ports tab shows information about the I/O ports.

Procedure: Getting node canister and system information using a USB flash drive

This procedure explains how to view information about the node canister and system using a USB flash drive.

About this task

Use any USB flash drive with a FAT32 file system on its first partition.
1. Ensure that the USB flash drive does not contain a file named satask.txt in the root directory.

If satask.txt does exist in the directory, the node attempts to run the command that is specified in the file. The information that is returned is appended to the satask_result.html file. Delete this file if you no longer want the previous output.

Procedure
1. Insert the USB flash drive in one of the USB ports of the node canister from which you want to collect data.
Procedure: Understanding the system status using the LEDs

This procedure helps you determine the system status using the LED indicators on the system.

About this task

The LEDs provide a general idea of the system status. You can obtain more detail from the management GUI and the service assistant. Examine the LEDs when you are not able to access the management GUI or the service assistant, or when the system is not showing any information about a device. For information about the LEDs, go to “Power supply unit and battery for the control enclosure” on page 6, “Power supply unit for the expansion enclosure” on page 7, “Fibre Channel ports and indicators” on page 8, “Ethernet ports and indicators” on page 11, “Node canister SAS ports and indicators” on page 13, “Node canister LEDs” on page 14, “Expansion canister SAS ports and indicators” on page 15, and “Expansion canister LEDs” on page 16.

The procedure shows the status for the enclosure chassis, power supply units and batteries, and canisters. It does not show the status for the drives.

The first step is to determine the state of the control enclosure, which includes its power supply units, batteries, and node canisters. Your control enclosure is operational if you can manage the system using the management GUI. You might also want to view the status of the individual power supply units, batteries, or node canisters.

Find the control enclosure for the system that you are troubleshooting. There is one control enclosure in a system. If you are unsure which one is the control enclosure, go to “Procedure: Identifying which enclosure or canister to service” on page 51.

Procedure

1. Use the state of the ac power failure, power supply OK, fan failure, and dc power failure LEDs on each power supply unit in the enclosure to determine if there is power to the system, or if there are power problems. Figure 21 on page 55 shows the LEDs on the power supply unit for the 2076-112 or 2076-124. The LEDs on the power supply units for the 2076-312 and 2076-324 are similar, but they are not shown here.
### Table 18. Power-supply unit LEDs

<table>
<thead>
<tr>
<th>Power supply</th>
<th>ac failure</th>
<th>Fan failure</th>
<th>dc failure</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>Communication failure between the power supply unit and the enclosure chassis</td>
<td>Replace the power supply unit. If failure is still present, replace the enclosure chassis.</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>No ac power to the enclosure.</td>
<td>Turn on power.</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>The ac power is on but power supply unit is not seated correctly in the enclosure.</td>
<td>Seat the power supply unit correctly in the enclosure.</td>
</tr>
</tbody>
</table>

*Figure 21. LEDs on the power supply units of the control enclosure*
### Table 18. Power-supply unit LEDs (continued)

<table>
<thead>
<tr>
<th>Power supply</th>
<th>ac failure</th>
<th>Fan failure</th>
<th>dc failure</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
</table>
| Off          | On         | Off         | On         | No ac power to this power supply | 1. Check that the switch on the power supply unit is on.  
2. Check that the ac power is on.  
3. Reseat and replace the power cable. |
| On           | Off        | Off         | Off        | Power supply is on and operational. | No actions |
| Off          | Off        | On          | Off        | Fan failure | Replace the power supply unit. |
| Off          | On         | On          | On         | Communication failure and power supply problem | Replace the power supply unit. If replacing the power supply unit does not fix the problem, replace the enclosure chassis. |
| Flashing     | X          | X           | X          | No canister is operational. | Both canisters are either off or not seated correctly. Turn off the switch on both power supply units and then turn on both switches. If this action does not resolve the problem, remove both canisters slightly and then push the canisters back in. |
| Off          | Flashing   | Flashing    | Flashing   | Firmware is downloading. | No actions. Do not remove ac power.  
**Note:** In this case, if there is a battery in a power supply unit, its LEDs also flash. |

2. At least one power supply in the enclosure must indicate **Power supply OK** or **Power supply firmware downloading** for the node canisters to operate. For this situation, review the three canister status LEDs on each of the node canisters. Start with the power LED.

### Table 19. Power LEDs

<table>
<thead>
<tr>
<th>Power LED status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>There is no power to the canister. Try reseating the canister. Go to &quot;Procedure: Reseating a node canister&quot; on page 65. If the state persists, follow the hardware replacement procedures for the parts in the following order: node canister, enclosure chassis.</td>
</tr>
</tbody>
</table>
Table 19. Power LEDs (continued)

<table>
<thead>
<tr>
<th>Power LED status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow flashing (1 Hz)</td>
<td>Power is available, but the canister is in standby mode. Try to start the node canister by reseating it. Go to “Procedure: Reseating a node canister” on page 65.</td>
</tr>
<tr>
<td>Fast flashing (2 Hz)</td>
<td>The canister is running its power-on self-test (POST). Wait for the test to complete. If the canister remains in this state for more than 10 minutes, try reseating the canister. Go to “Procedure: Reseating a node canister” on page 65. If the state persists, follow the hardware replacement procedure for the node canister.</td>
</tr>
</tbody>
</table>

Figure 22 shows the LEDs on the node canister.

Figure 22. LEDs on the node canisters

3. If the power LED is on, consider the states of the clustered-system status and fault LEDs.

Table 20. System status and fault LEDs

<table>
<thead>
<tr>
<th>System status LED</th>
<th>Fault LED</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Off</td>
<td>Code is not active.</td>
<td>• Follow procedures for reviewing power LEDs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If the power LEDs show green, reseat the node canister. See “Procedure: Reseating a node canister” on page 65. If the LED status does not change, see “Replacing a node canister” on page 85.</td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>Code is not active. The BIOS or the service processor has detected a hardware fault.</td>
<td>Follow the hardware replacement procedures for the node canister.</td>
</tr>
<tr>
<td>On</td>
<td>Off</td>
<td>Code is active. Node state is active.</td>
<td>No action. The node canister is part of a clustered system and can be managed by the management GUI.</td>
</tr>
</tbody>
</table>
Table 20. System status and fault LEDs (continued)

<table>
<thead>
<tr>
<th>System status LED</th>
<th>Fault LED</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>On</td>
<td>Code is active and is in starting state. However, it does not have enough resources to form the clustered system. The node canister cannot become active in a clustered system. There are no detected problems on the node canister itself. However, it cannot connect to enough resources to safely form a clustered system. Follow the procedure to fix the node errors. Go to “Procedure: Fixing node errors” on page 60.</td>
<td></td>
</tr>
<tr>
<td>Flashing</td>
<td>Off</td>
<td>Code is active. Node state is candidate. Create a clustered system on the node canister, or add the node canister to the clustered system. If the other node canister in the enclosure is in active state, it automatically adds this node canister into the clustered system. A node canister in this state can be managed using the service assistant.</td>
<td></td>
</tr>
<tr>
<td>Flashing</td>
<td>On</td>
<td>Code is active. Node state is service. The node canister cannot become active in a clustered system. Several problems can exist: hardware problem, a problem with the environment or its location, or problems with the code or data on the canister. Follow the procedure to fix the node errors. Go to “Procedure: Fixing node errors” on page 60.</td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>Flashing</td>
<td>The node canister is being identified so that you can locate it. The fix procedures in the management GUI might have identified the component because it requires servicing. Continue to follow the fix procedures. The service assistant has a function to identify node canisters. If the identification LED is on in error, use the service assistant node actions to turn off the LED.</td>
<td></td>
</tr>
</tbody>
</table>

Results

To review the status of the control enclosure batteries, see Table 21.

Table 21. Control enclosure battery LEDs

<table>
<thead>
<tr>
<th>Battery Good LED</th>
<th>Battery Fault LED</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Off</td>
<td>Battery is good and fully charged.</td>
<td>None</td>
</tr>
<tr>
<td>Flashing</td>
<td>off</td>
<td>Battery is good but not fully charged. The battery is either charging or a maintenance discharge is being performed.</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 21. Control enclosure battery LEDs (continued)

<table>
<thead>
<tr>
<th>Battery Good</th>
<th>Battery Fault</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>On</td>
<td>Nonrecoverable battery fault.</td>
<td>Replace the battery. If replacing the battery does not fix the issue, replace the power supply unit.</td>
</tr>
<tr>
<td>Off</td>
<td>Flashing</td>
<td>Recoverable battery fault.</td>
<td>None</td>
</tr>
<tr>
<td>Flashing</td>
<td>Flashing</td>
<td>The battery cannot be used because the firmware for the power supply unit is being downloaded.</td>
<td>None</td>
</tr>
</tbody>
</table>

### Procedure: Finding the status of the Ethernet connections

This procedure explains how to find the status of the Ethernet connections when you cannot connect.

**About this task**

Ensure that the software is active on the node before you begin this procedure. Go to “Procedure: Understanding the system status using the LEDs” on page 54. Ethernet port 1 must be connected to an active port on your Ethernet network.

Determine the state of the Ethernet LEDs by using one of the following methods:

- Use the USB flash drive to obtain the most comprehensive information for the node status. Go to “Procedure: Getting node canister and system information using a USB flash drive” on page 53.
  The status, speed, and MAC address are returned for each port. Information is returned that identifies whether the node is the configuration node and if any node errors were reported.
- Examine the LEDs of the Ethernet ports. For the status of the LEDs, go to “Ethernet ports and indicators” on page 11.

If your link is not connected, perform the following actions to check the port status each time until it is corrected or connected:

**Procedure**

1. Verify that each end of the cable is securely connected.
2. Verify that the port on the Ethernet switch or hub is configured correctly.
3. Connect the cable to a different port on your Ethernet network.
4. If the status is obtained using the USB flash drive, review all the node errors that are reported.
5. Replace the Ethernet cable.

### Procedure: Removing system data from a node canister

This procedure guides you through the process to remove system information from a node canister. The information that is removed includes configuration data, cache data, and location data.
About this task

Attention: If the enclosure reaches a point where the system data is not available on any node canister in the system, you have to perform a system recovery. This recovery is an extended service action and might not be able to recover all of your volumes. Do not perform this action to remove the system data from a node unless there is a node canister with saved system information in the enclosure. Do not remove the system data from a node unless instructed to do so by a service procedure.

Procedure
1. Start the service assistant on the node canister.
2. Use the service assistant node action to hold the node in service state.
3. Use the Manage System option to remove the system data from the node.

Results

The node restarts in service state. When you want the node canister to be active again, use the service assistant home page action to leave service state.

Procedure: Deleting a system completely

This procedure guides you through the process of completely removing all system information. When the procedure is finished, the system performs like a new installation.

About this task

Attention: This procedure makes all the volume data that you have on your system inaccessible. You cannot recover the data. This procedure affects all volumes that are managed by your system.

Do not continue unless you are certain that you want to remove all the volume data and configuration data from your system. This procedure is not used as part of any recovery action.

There are two stages to this procedure. First, the node canisters are reset. Second, the enclosure data is reset.

Procedure
1. Start the service assistant on one of the node canisters.
2. Use the service assistant node action to hold the node in service state.
3. Use the Manage System option to remove the system data from the node.
4. Perform the previous steps on the second node canister in the enclosure.
5. On one node, open the service assistant Configure Enclosure and select the Reset System ID option. This action causes the system to reset.

Procedure: Fixing node errors

To fix a node error that is detected on one of the node canisters in your system, use this procedure.
**About this task**

Node errors are reported when there is an error that is detected that affects a specific node canister.

**Procedure**

1. Use the service assistant to view the current node errors on any node.
2. If available, use the management GUI to run the recommended action for the alert.
3. Follow the fix procedure instructions.
4. If the recommended action does not provide sufficient information to determine the service action, review the node error descriptions and service actions. Go to "Error code range" on page 138.
   
   See the node error descriptions if you cannot access the management GUI or if the management GUI is not reporting an alert because it cannot connect to the node. When you cannot connect to the management GUI, follow the procedure for getting node canister and clustered-system information using the service assistant. Go to "Procedure: Getting node canister and system information using the service assistant" on page 53. Start with the node that displays an error. The home page shows the node errors on the current node in the priority that you must service them. Start with the node error with the highest priority.
5. Select a different node in the system to see the node errors on that node.
6. Attempt to service the node errors in the priority order that they are listed.
7. Use the error number as an index when reviewing the node error descriptions. The service actions for each error are listed with the error code. Go to "Error code range" on page 138.

---

**Procedure: Changing the service IP address of a node canister**

This procedure identifies many methods that you can use to change the service IP address of a node canister.

**About this task**

When you change an IPv4 address, you change the IP address, the subnet, mask, and gateway. When you change an IPv6 address, you change the IP address, prefix, and gateway.

Which method to use depends on the status of the system and the other node canisters in the system. Follow the methods in the order shown until you are successful in setting the IP address to the required value.

You can set an IPv4 address, an IPv6 address, or both, as the service address of a node. Enter the required address correctly. If you set the address to 0.0.0.0 or 0000:0000:0000:0000:0000:0000:0000:0000, you disable the access to the port on that protocol.

**Procedure**

Change the service IP address.

- Use the control enclosure management GUI when the system is operating and the system is able to connect to the node with the service IP address that you want to change.
1. Select **Settings > Network** from the navigation.
2. Select **Service IP Addresses**.
3. Complete the panel. Be sure to select the correct node to configure.
   - Use the service assistant when you can connect to the service assistant on either the node canister that you want to configure or on a node canister that can connect to the node canister that you want to configure:
     1. Make the node canister that you want to configure the current node.
     2. Select **Change Service IP** from the menu.
     3. Complete the panel.
   - Use one of the following procedures if you cannot connect to the node canister from another node:
     - Use the initialization tool to write the correct command file to the USB flash drive. Go to "Using the initialization tool" on page 37.
     - Use a text editor to create the command file on the USB flash drive. Go to "Using a USB flash drive" on page 36.

---

**Procedure: Initializing a clustered system with a USB flash drive without using the initialization tool**

Use this procedure to initialize a clustered system using a USB flash drive when you do not have a Microsoft Windows workstation to run the initialization tool or you do not have a copy of the tool.

**About this task**

In these situations, you must manually create an satask.txt file on a USB flash drive to initialize your clustered system. Use the USB flash drive that was supplied with your system or any USB flash drive that is formatted with a FAT32 file system on its first partition.

**Procedure**

1. Open a file editor that can create ASCII text files.
2. Create a file called satask.txt.
3. Add a single line of command text to the file.
   - If you are creating a clustered system with an IPv4 address, the command line is like the following string:
     ```
     ```
     where you must replace `aaa.aaa.aaa.aaa` with the management IP address, `ggg.ggg.ggg.ggg` with the network gateway address, and `mmm.mmm.mmm.mmm` with the subnet mask address.
   - If you are creating a clustered system with an IPv6 address, the command line is like the following string:
     ```
     ```
4. Save the file to a USB flash drive.
5. Plug the USB flash drive into a USB port on a control canister.

6. The system detects the USB flash drive, reads the satask.txt file, runs the command, and writes the results to the USB flash drive. The satask.txt file is deleted after the command is run.

7. Wait for the fault LED on the node canister to stop flashing before removing the USB flash drive.

8. Remove the USB flash drive and insert it into your workstation to view the results.

9. Use a web browser to view the results file, satask_result.html. Check that there were no errors returned by the command. If there is insufficient battery charge to protect the system, the clustered system creates successfully, but it does not start immediately. In the results, look for the time_to_charge field for the battery. The results provide an estimate of the time, in minutes, before the system can start. If the time is not 0, wait for the required time. Check that the node canister that you inserted the USB flash drive into has its clustered-state LED on permanently. For additional information, see “Procedure: Understanding the system status using the LEDs” on page 54.

10. If the initialization was successful and the batteries are sufficiently charged, point a supported browser to the management IP address that you specified to start the management GUI. You see the management GUI logon panel.

11. Log on as superuser. Use password for the password.

12. Follow the on-screen instructions.

Results

For more information about using the USB flash drive, see “USB flash drive and initialization tool interface” on page 36.

Procedure: Initializing a clustered system using the service assistant

To initialize a clustered system using the service assistant rather than the USB flash drive, use this procedure.

About this task

Note: The service assistant gives you the option to create a clustered system only if the node state is candidate.

To initialize a clustered system using the service assistant, perform the following steps:

Procedure

1. Point your web browser to the service assistant address of a node canister. It is best to use node canister in slot 1; when viewed from the rear of the control enclosure, the left node canister. The default service address for this canister is 192.168.70.121/service.

2. Log on with the superuser password. The default password is password.

   If you are unable to connect, see “Problem: Cannot connect to the service assistant” on page 47.

3. Select Manage System.

4. Enter the system name and the management IP address.
5. Click Create System.

Results

Attention: Without a USB flash drive to service the system, it is not possible to reset the superuser password or to change the system IP addresses in the event of a fault that prevents access to the management interface. It is essential that you take steps to record this information for use in the event of a failure.

Procedure: Accessing a canister using a directly attached Ethernet cable

If you need to use a direct Ethernet connection to attach a personal computer to a node canister to run the service assistant or to use the service CLI, use this procedure.

About this task

Perform this procedure if you are not authorized to use a USB flash drive in your data center and when the service address of your nodes cannot be accessed over your Ethernet network. This situation might occur for a new installation where the default service IP addresses cannot be accessed on your network. The default service addresses are listed in “Problem: Cannot connect to the service assistant” on page 47.

Note: Do not attempt to use a directly attached Ethernet cable to a canister that is active in a clustered system. You might disrupt access from host applications or the management GUI. If the node is active, go to Settings > Network in the management GUI to set the service IP address to one that is accessible on the network.

Perform the following steps to access a canister using a directly attached Ethernet cable:

Procedure

1. Connect one end of an Ethernet cable to Ethernet port 1 of a node canister in the control enclosure.

   Note: A cross-over Ethernet cable is not required.

2. Connect the other end of the Ethernet cable directly to the Ethernet port on a personal computer that has a web browser installed.

3. Use the operating system tools on the computer to set the IP address of the Ethernet port that is used in the previous step to 192.168.70.10.

4. Point the web browser to the service IP address for the node canister attached at step 1. If the service IP address has not been changed at any time, use the default service IP addresses listed in “Problem: Cannot connect to the service assistant” on page 47.

5. Log on with the superuser password. The default password is passw0rd.

6. After the action completes, disconnect your personal computer, and reconnect the node canister to the Ethernet network.

7. Set the service address of the canister to one that can be accessed on the network as soon as possible.
Procedure: Reseating a node canister

Use this procedure to reseat a canister that is in service state or because a service action has directed you.

About this task

Verify that you are reseating the correct node canister and that you use the correct canister handle for the node that you are reseating. Handles for the node canisters are located next to each other. The handle on the right operates the upper canister. The handle on the left operates the lower canister.

Procedure

1. Verify the clustered-system status LED on the node canister. If it is permanently on, the node is active. If the node is active, no reseating is required.
2. Verify that you have selected the correct node canister and verify why you are reseating it. Go to “Procedure: Identifying which enclosure or canister to service” on page 51.
   - If you reseat a node that is active, it cannot store its state data and cannot restart without other service actions.
   - If the other node canister in the enclosure is not active, reseating the node canister while it is active results in loss of the data on your volumes and the system is unavailable to hosts.
3. Grasp the handle between the thumb and forefinger.
4. Squeeze them together to release the handle.
5. Pull out the handle to its full extension.
6. Grasp the canister and pull it out 2 or 3 inches.
7. Push the canister back into the slot until the handle starts to move.
8. Finish inserting the canister by closing the handle until the locking catch clicks into place.
9. Verify that the cables were not displaced.
10. Verify that the LEDs are on.

Results

Procedure: Powering off your system

Use this procedure to power off your Storwize V7000 system when it must be serviced or to permit other maintenance actions in your data center.

About this task

To power off your Storwize V7000 system, use the following steps:
1. Stop hosts.
2. Shut down the system by using the management GUI. Click Monitoring > System Details. From the Actions menu, select Shut Down System.
3. Wait for the power LED on both node canisters in all control enclosures to start flashing, which indicates that the shutdown operation has completed.
   - The following figure shows the LEDs on the node canisters. The power LED is the LED on the left when the canister is top-side up.
4. Using the power switches, power off the control enclosures.
5. Using the power switches, power off the expansion enclosures.
6. (Optional) Shut down external storage systems.
7. (Optional) Shut down Fibre Channel switches.

**Procedure: Collecting information for support**

IBM support might ask you to collect trace files and dump files from your system to help them resolve a problem.

**About this task**

The management GUI and the service assistant have features to assist you in collecting the required information. The management GUI collects information from all the components in the system. The service assistant collects information from a single node canister. When the information that is collected is packaged together in a single file, the file is called a snap.

Special tools that are only available to the support teams are required to interpret the contents of the support package. The files are not designed for customer use.

**Procedure**

Always follow the instructions that are given by the support team to determine whether to collect the package by using the management GUI or the service assistant. Instruction is also given for which package content option is required.

- If you are collecting the package by using the management GUI, select **Settings > Support**. Click **Download Support Package**. Follow the instructions to download the appropriate log files.
- If you are collecting the package by using the service assistant, ensure that the node that you want to collect logs from is the current node. Select the **Collect Logs** option from the navigation. You can collect a support package or copy an individual file from the node canister. Follow the instructions to collect the information.
**Procedure: Rescuing node canister software from another node (node rescue)**

Use this procedure to perform a node rescue.

**About this task**

A failure has indicated that the node software is damaged and must be reinstalled.

**Procedure**

1. Ensure that the node you want to reinstall the code on is the current node. Go to “Accessing the service assistant” on page 34.
2. Select Reinstall Machine Code from the navigation.
3. Select Rescue from another node.

**Results**

---

**Procedure: FCoE host-link**

**About this task**

If you are having problems attaching to the FCoE hosts, your problem might be related to the network, the Storwize V7000 system, or the host.

**Procedure**

1. If you are seeing error code 705 on the node, this means Fibre Channel I/O port is inactive. Note that FCoE uses Fibre Channel as a protocol and an Ethernet as an interconnect. If you are dealing with an FCoE enabled port that means either the Fibre Channel Forwarder (FCF) is not seen or the FCoE feature is not configured on the switch:
   a. Check that the FCoE feature is enabled on the FCF.
   b. Check the remote port (switch port) properties on the FCF.
2. If you connecting the host through a Converged Enhanced Ethernet (CEE) switch, for network problems, you can attempt any of the following actions:
   a. Test your connectivity between the host and CEE switch.
   b. Ask the Ethernet network administrator to check the firewall and router settings.
3. Please run `svcinfo lsfabric` and check that the host is seen as a remote port in the output. If not, then do the following tasks in order:
   a. Verify that Storwize V7000 and host get an fcid on FCF. If not, check the VLAN configuration.
   b. Verify that Storwize V7000 and host port are part of a zone and that zone is currently in force.
   c. Verify the volumes are mapped to the host and that they are online. See `lshostvdiskmap` and `lsvdisk` in the CLI configuration guide for more information.
4. If you still have FCoE problems, you can attempt the following action:
   a. Verify that the host adapter is in good state. You can unload and load the device driver and see the operating system utilities to verify that the device driver is installed, loaded, and operating correctly.
SAN problem determination

About this task

SAN failures might cause Storwize V7000 volumes to be inaccessible to host systems. Failures can be caused by SAN configuration changes or by hardware failures in SAN components.

The following list identifies some of the hardware that might cause failures:

- Power, fan, or cooling switch
- Application-specific integrated circuits
- Installed small form-factor pluggable (SFP) transceiver
- Fiber-optic cables

Perform the following steps if you were sent here from the error codes:

Procedure

1. Verify that the power is turned on to all switches and storage controllers that the Storwize V7000 system uses, and that they are not reporting any hardware failures. If problems are found, resolve those problems before proceeding further.
2. Verify that the Fibre Channel cables that connect the systems to the switches are securely connected.
3. If you have a SAN management tool, use that tool to view the SAN topology and isolate the failing component.

Fibre Channel link failures

When a failure occurs on a single Fibre Channel link, the small form-factor pluggable (SFP) transceiver might need to be replaced.

Before you begin

The following items can indicate that a single Fibre Channel link has failed:

- The Fibre Channel status LEDs at the rear of the node canister
- An error that indicates a single port has failed

Attempt each of these actions, in the following order, until the failure is fixed:

1. Ensure that the Fibre Channel cable is securely connected at each end.
2. Replace the Fibre Channel cable.
3. Replace the SFP transceiver for the failing port on the Storwize V7000 Storwize V7000 node.

Note: Storwize V7000 nodes are supported with both longwave SFP transceivers and shortwave SFP transceivers. You must replace an SFP transceiver with the same type of SFP transceiver. If the SFP transceiver to replace is a longwave SFP transceiver, for example, you must provide a suitable replacement. Removing the wrong SFP transceiver could result in loss of data access.

4. Perform the Fibre Channel switch service procedures for a failing Fibre Channel link. This might involve replacing the SFP transceiver at the switch.
5. Contact IBM Support for assistance in replacing the node canister.
Servicing storage systems

Storage systems that are supported for attachment to the Storwize V7000 system are designed with redundant components and access paths to enable concurrent maintenance. Hosts have continuous access to their data during component failure and replacement.
This topic describes these recovery procedures: recover a system and back up and restore a system configuration.

Recover system procedure

The recover system procedure recovers the entire system if the block cluster state has been lost from all nodes. The recover system procedure recovers the entire storage system if the data has been lost from all control enclosure node canisters. The procedure re-creates the storage system by using saved configuration data. The recovery might not be able to restore all volume data. This procedure is also known as Tier 3 (T3) recovery.

Attention: Perform service actions only when directed by the fix procedures. If used inappropriately, service actions can cause loss of access to data or even data loss. Before attempting to recover a storage system, investigate the cause of the failure and attempt to resolve those issues by using other fix procedures. Read and understand all of the instructions before performing any action.

Attention: Do not attempt the recovery procedure unless the following conditions are met:

- All hardware errors are fixed.
- All node canisters have candidate status.
- All node canisters must be at the same level of code that the storage system had before the system failure. If any node canisters were modified or replaced, use the service assistant to verify the levels of code, and where necessary, to upgrade or downgrade the level of code.

The system recovery procedure is one of several tasks that must be performed. The following list is an overview of the tasks and the order in which they must be performed:

1. Preparing for system recovery
   a. Review the information regarding when to run the recover system procedure
   b. Fix your hardware errors
   c. Remove the system information for node canisters with error code 550 or error code 578 by using the service assistant.

2. Performing the system recovery. After you prepared the system for recovery and met all the pre-conditions, run the system recovery.

   Note: Run the procedure on one system in a fabric at a time. Do not perform the procedure on different node canisters in the same system. This restriction also applies to remote systems.

3. Performing actions to get your environment operational
   a. Recovering from offline VDisks (volumes) by using the CLI
   b. Checking your system, for example, to ensure that all mapped volumes can access the host.
When to run the recover system procedure

A recover procedure must be attempted only after a complete and thorough investigation of the cause of the system failure. Attempt to resolve those issues by using other service procedures.

**Attention:** If you experience failures at any time while you are running the recover system procedure, call the IBM Support Center. Do not attempt to do further recovery actions because these actions might prevent IBM Support from restoring the system to an operational status.

Certain conditions must be met before you run the recovery procedure. Use the following items to help you determine when to run the recovery procedure:

**Note:** It is important that you know the number of control enclosures in the system, and when the instructions indicate that every node is checked, you must check the status of both nodes in every control enclosure. For some system problems or Fibre Channel network problems, you must run the service assistant directly on the node to get its status.

- Check to see if any node in the system has a node status of active. This status means that the system is still available. In this case, recovery is not necessary.
- Do not recover the system if the management IP address is available from another node. Ensure that all service procedures have been run.
- Check the node status of every node canister that is part of this system. Resolve all hardware errors except node error 578 or node error 550.
  - All nodes must be reporting either a node error 578 or a node error 550. These error codes indicate that the system has lost its configuration data. If any nodes report anything other than these error codes, do not perform a recovery. You can encounter situations where non-configuration nodes report other node errors, such as a 550 node error. The 550 error can also indicate that a node is not able to join a system.
  - If any nodes show a node error 550, record the error data that is associated with the 550 error from the service assistant.

  - In addition to the node error 550, the report can show data that is separated by spaces in one of the following forms:
    - Node identifiers in the format: `<enclosure_serial>---<canister slot ID>` (7 characters, hyphen, 1 number), for example, 01234A6-2
    - Quorum drive identifiers in the format: `<enclosure_serial>:<drive slot ID>:<drive slot ID>[<drive 11S serial number>]` (7 characters, colon, 1 or 2 numbers, open square bracket, 22 characters, close square bracket), for example, 012349:21[1151234567890123456789]
    - Quorum MDisk identifier in the format: WWPN/LUN (16 hexadecimal digits followed by a forward slash and a decimal number), for example, 1234567890123456/12
  - If the error data contains a node identifier, ensure that the node that is referred to by the ID is showing node error 578. If the node is showing a node error 550, ensure that the two nodes can communicate with each other. Verify the SAN connectivity, and if the 550 error is still present, restart one of the two nodes by clicking **Restart Node** from the service assistant.
  - If the error data contains a quorum drive identifier, locate the enclosure with the reported serial number. Verify that the enclosure is powered on and that the drive in the reported slot is powered on and functioning. If the node canister that is reporting the fault is in the I/O group of the listed...
enclosure, ensure that it has SAS connectivity to the listed enclosure. If the node canister that is reporting the fault is in a different I/O group from the listed enclosure, ensure that the listed enclosure has SAS connectivity to both node canisters in the control enclosure in its I/O group. After verifying these things, restart the node by clicking Restart Node from the service assistant.

- If the error data contains a quorum MDisk identifier, verify the SAN connectivity between this node and that WWPN. Check the storage controller to ensure that the LUN referred to is online. After verifying these things, if the 550 error is still present, restart the node by clicking Restart Node from the service assistant.

- If there is no error data, the error is because there are insufficient connections between nodes over the Fibre Channel network. Each node must have at least two independent Fibre Channel logical connections, or logins, to every node that is not in the same enclosure. An independent connection is one where both physical ports are different. In this case, there is a connection between the nodes, but there is not a redundant connection. If there is no error data, wait 3 minutes for the SAN to initialize. Next check that the following items:
  • That there are at least two Fibre Channel ports that are operational and connected on every node.
  • That the SAN zoning allows every port to connect to every port on every other node.
  • If redundant SANs are being used, that all of them are operational.

After verifying these things, if the 550 error is still present, restart the node by clicking Restart Node from the service assistant.

Note: If after resolving all these scenarios, half or greater than half of the nodes are reporting node error 578, it is appropriate to run the recovery procedure. You can also call IBM Support for further assistance.

- For any nodes that are reporting a node error 550, ensure that all the missing hardware that is identified by these errors is powered on and connected without faults. If you cannot contact the service assistant from any node, isolate the problems by using the LED indicators.

- If you have not been able to restart the system and if any node other than the current node is reporting node error 550 or 578, you must remove system data from those nodes. This action acknowledges the data loss and puts the nodes into the required candidate state.

  • Do not attempt to recover the system if you have been able to restart it.
  • If back-end MDisks are removed from the configuration, those volumes that depended on that hardware cannot be recovered. All previously configured back-end hardware must be present for a successful recovery.
  • Any nodes that were replaced must have the same WWNN as the nodes that they replaced.
  • If any of the node canisters were replaced, they must not have participated in any other system. You can resolve this issue by performing a node rescue on the affected canister by using the service assistant. Do not perform this action on any of the other node canisters.
  • The configuration backup file must be up to date. If any configuration changes had been made since the backup was taken, the data is inconsistent and further investigation is needed. Manual changes are required after the system is recovered.
Any data that was in the cache at the point of failure is lost. The loss of data can result in data corruption on the affected volumes. If the volumes are corrupted, call the IBM Support Center.

Fix hardware errors

Before you can run a system recovery procedure, it is important that the root cause of the hardware issues be identified and fixed.

Obtain a basic understanding about the hardware failure. In most situations when there is no clustered system, a power issue is the cause. For example, both power supplies might have been removed.

Removing system information for node canisters with error code 550 or error code 578 using the service assistant

The system recovery procedure works only when all node canisters are in candidate status. If there are any node canisters that display error code 550 or error code 578, you must remove their data.

About this task

Before performing this task, ensure that you have read the introductory information in the overall recover system procedure.

To remove system information from a node canister with an error 550 or 578, follow this procedure using the service assistant:

Procedure

1. Point your browser to the service IP address of one of the nodes, for example, https://node_service_ip_address/service/.
   If you do not know the IP address or if it has not been configured, you must assign an IP address using the initialization tool.
2. Log on to the service assistant.
3. Select Manage System.
4. Click Remove System Data.
5. Confirm that you want to remove the system data when prompted.
6. Remove the system data for the other nodes that display a 550 or a 578 error.
   All nodes previously in this system must have a node status of Candidate and have no errors listed against them.
7. Resolve any hardware errors until the error condition for all nodes in the system is None.
8. Ensure that all nodes in the system display a status of candidate.

Results

When all nodes display a status of candidate and all error conditions are None, you can run the recovery procedure.

Performing system recovery using the service assistant

Start recovery when all node canisters that were members of the system are online and have candidate status. If any nodes display error code 550 or 578, remove their system data to place them into candidate status. Do not run the recovery procedure on different node canisters in the same system.
About this task

All node canisters must be at the original level of code, prior to the system failure. If any node canisters were modified or replaced, use the service assistant to verify the levels of code, and where necessary, to upgrade or downgrade the level of code.

Attention: This service action has serious implications if not performed properly. If at any time an error is encountered not covered by this procedure, stop and call IBM Support.

Note: The web browser must not block pop-up windows, otherwise progress windows cannot open.

Any one of the following categories of messages may be displayed:

- **T3 successful**
  
  The volumes are back online. Use the final checks to get your environment operational again.

- **T3 recovery completed with errors**
  
  T3 recovery completed with errors: One or more of the volumes are offline because there was fast write data in the cache. To bring the volumes online, see “Recovering from offline VDisks using the CLI” on page 76 for details.

- **T3 failed**
  
  Call IBM Support. Do not attempt any further action.

Run the recovery from any node canisters in the system; the node canisters must not have participated in any other system.

Note: Each individual stage of the recovery procedure might take significant time to complete, dependant upon the specific configuration.

Before performing this procedure, read the recover system procedure introductory information; see “Recover system procedure” on page 71.

Procedure

1. Point your browser to the service IP address of one of the node canisters.
   
   If the IP address is unknown or has not been configured, assign an IP address using the initialization tool; see “Procedure: Changing the service IP address of a node canister” on page 61.

2. Log on to the service assistant.

3. Check that all node canisters that were members of the system are online and have candidate status.
   
   If any nodes display error code 550 or 578, remove their system data to place them into candidate status; see “Procedure: Removing system data from a node canister” on page 59.

4. Select **Recover System** from the navigation.

5. Follow the online instructions to complete the recovery procedure.
   
   a. Verify the date and time of the last quorum time. The time stamp must be less than 30 minutes before the failure. The time stamp format is **YYYYMMDD hh:mm**, where **YYYY** is the year, **MM** is the month, **DD** is the day, **hh** is the hour, and **mm** is the minute.
Attention: If the time stamp is not less than 30 minutes before the failure, call IBM Support.

a. Verify the date and time of the last backup date. The time stamp must be less than 24 hours before the failure. The time stamp format is YYYYMMDD hh:mm, where YYYY is the year, MM is the month, DD is the day, hh is the hour, and mm is the minute.

Attention: If the time stamp is not less than 24 hours before the failure, call IBM Support. Changes made after the time of this backup date might not be restored.

Results

Verify the environment is operational by performing the checks provided in “What to check after running the system recovery” on page 77.

If any errors are logged in the error log after the system recovery procedure completes, use the fix procedures to resolve these errors, especially the errors related to offline arrays.

If the recovery completes with offline volumes, go to “Recovering from offline VDisks using the CLI.”

Recovering from offline VDisks using the CLI

If a Tier 3 recovery procedure completes with offline volumes, then it is likely that the data which was in the write-cache of the node canisters was lost during the failure that caused all of the node canisters to lose the block storage system cluster state. You can use the command-line interface (CLI) to acknowledge that was lost data lost from the write-cache and bring the volume back online so that you can attempt to deal with the data loss.

About this task

If you have performed the recovery procedure, and it has completed successfully but there are offline volumes, you can perform the following steps to bring the volumes back online. Any volumes that are offline and are not thin-provisioned (or compressed) volumes are offline because of the loss of write-cache data during the event that led all node canisters to lose their cluster state. Any data lost from the write-cache cannot be recovered. These volumes might need additional recovery steps after the volume is brought back online.

Note: If you encounter errors in the error log after running the recovery procedure that are related to offline arrays, use the fix procedures to resolve the offline array errors before fixing the offline volume (VDisk) errors.

Example

Perform the following steps to recover an offline volume after the recovery procedure has completed:
1. Delete all IBM FlashCopy® function mappings and Metro Mirror or Global Mirror relationships that use the offline volumes.
2. Run the recovervdisk or recovervdiskbysystem command. (This will only bring the volume back online so that you can attempt to deal with the data loss.)
3. Refer to “What to check after running the system recovery” for what to do with volumes that have been corrupted by the loss of data from the write-cache.

4. Recreate all FlashCopy mappings and Metro Mirror or Global Mirror relationships that use the volumes.

**What to check after running the system recovery**

Several tasks must be performed before you use the system.

The recovery procedure performs a recreation of the old system from the quorum data. However, some things cannot be restored, such as cached data or system data managing in-flight I/O. This latter loss of state affects RAID arrays managing internal storage. The detailed map about where data is out of synchronization has been lost, meaning that all parity information must be restored, and mirrored pairs must be brought back into synchronization. Normally this results in either old or stale data being used, so only writes in flight are affected. However, if the array had lost redundancy (such as syncing, or degraded or critical RAID status) prior to the error requiring system recovery, then the situation is more severe. Under this situation you need to check the internal storage:

- Parity arrays will likely be syncing to restore parity; they do not have redundancy when this operation proceeds.
- Because there is no redundancy in this process, bad blocks may have been created where data is not accessible.
- Parity arrays could be marked as corrupt. This indicates that the extent of lost data is wider than in-flight IO, and in order to bring the array online, the data loss must be acknowledged.
- Raid-6 arrays that were actually degraded prior the system recovery may require a full restore from backup. For this reason, it is important to have at least a capacity match spare available.

Be aware of the following differences regarding the recovered configuration:

- FlashCopy mappings are restored as “idle_or_copied” with 0% progress. Both volumes must have been restored to their original I/O groups.
- The management ID is different. Any scripts or associated programs that refer to the system-management ID of the clustered system must be changed.
- Any FlashCopy mappings that were not in the “idle_or_copied” state with 100% progress at the point of disaster have inconsistent data on their target disks. These mappings must be restarted.
- Intersystem remote copy partnerships and relationships are not restored and must be re-created manually.
- Consistency groups are not restored and must be re-created manually.
- Intrasystem remote copy relationships are restored if all dependencies were successfully restored to their original I/O groups.
- The system time zone might not have been restored.

Before using the volumes, perform the following tasks:

- Start the host systems.
- Manual actions might be necessary on the hosts to trigger them to rescan for devices. You can perform this task by disconnecting and reconnecting the Fibre Channel cables to each host bus adapter (HBA) port.
- Verify that all mapped volumes can be accessed by the hosts.
- Run file system consistency checks.
- Run the application consistency checks.

**Backing up and restoring the system configuration**

You can back up and restore the configuration data for the system after preliminary tasks are completed.

Configuration data for the system provides information about your system and the objects that are defined in it. The backup and restore functions of the `svcconfig` command can back up and restore only your configuration data for the Storwize V7000 system. You must regularly back up your application data by using the appropriate backup methods.

You can maintain your configuration data for the system by completing the following tasks:
- Backing up the configuration data
- Restoring the configuration data
- Deleting unwanted backup configuration data files

Before you back up your configuration data, the following prerequisites must be met:
- No independent operations that change the configuration for the system can be running while the backup command is running.
- No object name can begin with an underscore character (_).

**Note:**
- The default object names for controllers, I/O groups, and managed disks (MDisks) do not restore correctly if the ID of the object is different from what is recorded in the current configuration data file.
- All other objects with default names are renamed during the restore process. The new names appear in the format `name_r` where `name` is the name of the object in your system.

Before you restore your configuration data, the following prerequisites must be met:
- You have the Security Administrator role associated with your user name and password.
- You have a copy of your backup configuration files on a server that is accessible to the system.
- You have a backup copy of your application data that is ready to load on your system after the restore configuration operation is complete.
- You know the current license settings for your system.
- You did not remove any hardware since the last backup of your configuration.
- No zoning changes were made on the Fibre Channel fabric which would prevent communication between the Storwize V7000 and any storage controllers which are present in the configuration.
- For configurations with more than one I/O group, if a new system is created on which the configuration data is to be restored, the I/O groups for the other control enclosures must be added.

Use the following steps to determine how to achieve an ideal T4 recovery:
Open the appropriate svc.config.backup.xml (or svc.config.cron.xml) file with a suitable text editor or browser and navigate to the node section of the file.

For each node entry, make a note of the value of following properties:
  IO_group_id, canister_id, enclosure_serial_number.

Use the CLI sainfo lsservicenodes command and the adata to determine which node canisters previously belonged in each IO group.

Restoring the system configuration should be performed via one of the nodes previously in IO group zero. For example, property name="IO_group_id" value="0". The remaining enclosures should be added, as required, in the appropriate order based on the previous IO_group_id of its node canisters.

Note: It is not currently possible to determine which canister within the identified enclosure was previously used for cluster creation. Typically the restoration should be performed via canister 1.

The Storwize V7000 analyzes the backup configuration data file and the system to verify that the required disk controller system nodes are available.

Before you begin, hardware recovery must be complete. The following hardware must be operational: hosts, Storwize V7000, drives, the Ethernet network, and the SAN fabric.

### Backing up the system configuration using the CLI

You can back up your configuration data using the command-line interface (CLI).

#### Before you begin

Before you back up your configuration data, the following prerequisites must be met:

- No independent operations that change the configuration can be running while the backup command is running.
- No object name can begin with an underscore character (_).

#### About this task

The backup feature of the svcconfig CLI command is designed to back up information about your system configuration, such as volumes, local Metro Mirror information, local Global Mirror information, managed disk (MDisk) groups, and nodes. All other data that you wrote to the volumes is not backed up. Any application that uses the volumes on the system as storage, must back up its application data using the appropriate backup methods.

You must regularly back up your configuration data and your application data to avoid data loss. It is recommended that this is performed after any significant changes in configuration have been made to the system. Note that the system automatically creates a backup of the configuration data each day at 1AM. This is known as a cron backup and is written to /dumps/svc.config.cron.xml_<serial#> on the configuration node. A manual backup can be generated at any time using the instructions in this task. If a severe failure occurs, both the configuration of the system and application data may be lost. The backup of the configuration data can be used to restore the system configuration to the exact state it was in before the failure. In some cases it may be possible to automatically recover the application data. This can be attempted via the <Recover System Procedure> also known as a Tier 3 (T3) procedure. Restoring the system configuration without attempting to...
recover the application data is performed via the <Restoring the System Configuration> procedure also known as a Tier 4 (T4) recovery. Both of these procedures require a recent backup of the configuration data.

Perform the following steps to back up your configuration data:

**Procedure**

1. Back up all of the application data that you stored on your volumes using your preferred backup method.
2. Issue the following CLI command to remove any temporary working files created by a previous configuration backup or restore attempt:
   ```
   svcconfig clear -all
   ```
3. Issue the following CLI command to back up your configuration:
   ```
   svcconfig backup
   ```
   The following output is an example of the messages that may be displayed during the backup process:
   ```
   CMMVC6112W io_grp io_grp1 has a default name
   CMMVC6112W io_grp io_grp2 has a default name
   CMMVC6112W mdisk mdisk14 ...
   CMMVC6112W node node1 ...
   CMMVC6112W node node2 ...
   ....................................................
   ```

   The `svcconfig backup` CLI command creates three files that provide information about the backup process and the configuration. These files are created in the `/dumps` directory of the configuration node canister.

   The following table describes the three files that are created by the backup process:

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>svc.config.backup.xml_&lt;serial#&gt;</code></td>
<td>This file that contains your configuration data.</td>
</tr>
<tr>
<td><code>svc.config.backup.sh_&lt;serial#&gt;</code></td>
<td>This file that contains the names of the commands that were issued to create the backup of the system.</td>
</tr>
<tr>
<td><code>svc.config.backup.log_&lt;serial#&gt;</code></td>
<td>This file contains details about the backup, including any reported errors or warnings.</td>
</tr>
</tbody>
</table>

4. Check that the `svcconfig backup` command completes successfully, and examine the command output for any warnings or errors. The following output is an example of the message that is displayed when the backup process is successful:
   ```
   CMMVC6155I SVCCONFIG processing completed successfully.
   ```

   If the process fails, resolve the errors, and run the command again.

5. It is recommended to keep backup copies of the files above outside the system to protect them against a system hardware failure. Copy the backup files off the system to a secure location using either the management GUI or scp command line. For example:
   ```
   pscp superuser@cluster_ip:/dumps/svc.config.backup.* /offclusterstorage/
   ```
The cluster_ip is the IP address or DNS name of the system and offclusterstorage is the location where you want to store the backup files.

Tip: To maintain controlled access to your configuration data, copy the backup files to a location that is password-protected.

**Restoring the system configuration**

Use this procedure in the following situations: only if the recover procedure has failed or if the data that is stored on the volumes is not required. For directions on the recover procedure, see “Recover system procedure” on page 71.

**Before you begin**

This configuration restore procedure is designed to restore information about your configuration, such as volumes, local Metro Mirror information, local Global Mirror information, storage pools, and nodes. All the data that you have written to the volumes is not restored. To restore the data on the volumes, you must restore application data from any application that uses the volumes on the clustered system as storage separately. Therefore, you must have a backup of this data before you follow the configuration recovery process.

**About this task**

You must regularly back up your configuration data and your application data to avoid data loss. If a system is lost after a severe failure occurs, both configuration for the system and application data is lost. You must reinstate the system to the exact state it was in before the failure, and then recover the application data.

**Important:** There are two phases during the restore process: prepare and execute. You must not change the fabric or system between these two phases.

If you do not understand the instructions to run the CLI commands, see the command-line interface reference information.

To restore your configuration data, follow these steps:

**Procedure**

1. Verify that all nodes are available as candidate nodes before you run this recovery procedure. You must remove errors 550 or 578 to put the node in candidate state. For all nodes that display these errors, perform the following steps:
   a. Point your browser to the service IP address of one of the nodes, for example, https://node_service_ip_address/service/.
   b. Log on to the service assistant.
   c. From the Home page, put the node into service state if it is not already in that state.
   d. Select Manage System.
   e. Click Remove System Data.
   f. Confirm that you want to remove the system data when prompted.
   g. Exit service state from the Home page. The 550 or 578 errors are removed, and the node appears as a candidate node.
   h. Remove the system data for the other nodes that display a 550 or a 578 error.
All nodes previously in this system must have a node status of Candidate and have no errors listed against them.

Note: A node that is powered off might not show up in this list of nodes for the system. Diagnose hardware problems directly on the node using the service assistant IP address and by physically verifying the LEDs for the hardware components.

2. Verify that all nodes are available as candidate nodes with blank system fields. Perform the following steps on one node in each control enclosure:
   a. Connect to the service assistant on either of the nodes in the control enclosure.
   b. Select Configure Enclosure.
   c. Select the Reset the system ID option. Do not make any other changes on the panel.
   d. Click Modify to make the changes.

3. Use the initialization tool that is available on the USB flash drive to create a new Storwize V7000 system. Select the Initialize a new Storwize V7000 (block system only) option from the Welcome panel of the initialization tool.

4. In a supported browser, enter the IP address that you used to initialize the system and the default superuser password (password).

5. At this point the setup wizard is shown. Be aware of the following items:
   a. Accept the license agreements.
   b. Set the values for the system name, data and time settings, and the system licensing. The original settings are restored during the configuration restore process.
   c. Verify the hardware. Only the control enclosure on which the clustered system was created and directly attached expansion enclosures are displayed. Any other control enclosures and expansion enclosures in other I/O groups will be added to the system.
   d. On the Configure Storage panel, deselect Yes, automatically configure internal storage now. Any internal storage configuration is recovered after the system is restored.

6. Optional: From the management GUI, click Access > Users and configure an SSH key for the superuser.

7. By default, the newly initialized system is created in the storage layer. The layer of the system is not restored automatically from the configuration backup XML file, so if the system you are restoring was previously configured in the replication layer, you must change the layer manually now. Refer to Metro Mirror and Global Mirror partnerships located under Product overview, in the IBM Storwize V7000 Information Center for more information.

8. For configurations with more than one I/O group add the rest of the control enclosures into the clustered system.
   a. From the management GUI, select Monitoring > System Details.
   b. Select the system name in the tree.
   c. Go to Actions > Add Enclosures > Control and Expansions .
   d. Continue to follow the on-screen instructions to add the control enclosures. Decline the offer to configure storage for the new enclosures when asked if you want to do so.

9. Identify the configuration backup file that you want to restore from.
The file can be either a local copy of the configuration backup XML file that you saved when backing up the configuration or an up-to-date file on one of the nodes.

Configuration data is automatically backed up daily at 01:00 system time on the configuration node.

Download and check the configuration backup files on all nodes that were previously in the system to identify the one containing the most recent complete backup.

For each node in the system:

a. From the management GUI, click **Settings > Support**.
b. Click **Show full log listing**.
c. Select the node to operate on from the selection box at the top of the table.
d. Find the file name that begins with `svc.config.cron.xml`.
e. Double-click the file to download the file to your computer.

The XML files contain a date and time that can be used to identify the most recent backup. After you identify the backup XML file that is to be used when you restore the system, rename the file to `svc.config.backup.xml`.

10. Issue the following CLI command to remove all of the existing backup and restore configuration files that are located on your configuration node in the `/tmp` directory: `svcconfig clear -all`

11. Copy the XML backup file that you wish to restore from back onto the system.

```
pscp full_path_to_identified_svc.config.backup.xml
superuser@cluster_ip:/tmp/
```

12. Issue the following CLI command to compare the current configuration with the backup configuration data file:

```
svcconfig restore -prepare
```

This CLI command creates a log file in the `/tmp` directory of the configuration node. The name of the log file is `svc.config.restore.prepare.log`.

**Note:** It can take up to a minute for each 256-MDisk batch to be discovered. If you receive error message `CMMVC6200W` for an MDisk after you enter this command, all the managed disks (MDisks) might not have been discovered yet. Allow a suitable time to elapse and try the `svcconfig restore -prepare` command again.

13. Issue the following command to copy the log file to another server that is accessible to the system:

```
pscp superuser@cluster_ip:/tmp/svc.config.restore.prepare.log
full_path_for_where_to_copy_log_files
```

14. Open the log file from the server where the copy is now stored.

15. Check the log file for errors.

   - If there are errors, correct the condition that caused the errors and reissue the command. You must correct all errors before you can proceed to step 16.
   - If an error indicates that the system layer will not be restored, then return to 7 on page 82 configure the layer setting correctly, and then continue the restore process from 10.
   - If you need assistance, contact the IBM Support Center.

16. Issue the following CLI command to restore the configuration:

```
svcconfig restore -execute
```

This CLI command creates a log file in the `/tmp` directory of the configuration node. The name of the log file is `svc.config.restore.execute.log`. 
17. Issue the following command to copy the log file to another server that is accessible to the system:

```
pscp superuser@cluster_ip:/tmp/svc.config.restore.execute.log
full_path_for_where_to_copy_log_files
```

18. Open the log file from the server where the copy is now stored.

19. Check the log file to ensure that no errors or warnings have occurred.

**Note:** You might receive a warning stating that a licensed feature is not enabled. This message means that after the recovery process, the current license settings do not match the previous license settings. The recovery process continues normally and you can enter the correct license settings in the management GUI at a later time.

When you log into the CLI again over SSH, you see this output:

```
IBM_2076:your_cluster_name:superuser>
```

20. After the configuration is restored, verify that the quorum disks are restored to the MDisks that you want by using the `lsquorum` command. To restore the quorum disks to the correct MDisks, issue the appropriate `chquorum` CLI commands.

**What to do next**

You can remove any unwanted configuration backup and restore files from the `/tmp` directory on your configuration by issuing the following CLI command:

```
svcconfig clear -all
```

**Deleting backup configuration files using the CLI**

You can use the command-line interface (CLI) to delete backup configuration files.

**About this task**

Perform the following steps to delete backup configuration files:

**Procedure**

1. Issue the following command to log on to the system:

```
plink -i ssh_private_key_file superuser@cluster_ip
```

where `ssh_private_key_file` is the name of the SSH private key file for the superuser and `cluster_ip` is the IP address or DNS name of the clustered system from which you want to delete the configuration.

2. Issue the following CLI command to erase all of the files that are stored in the `/tmp` directory:

```
svconfig clear -all
```
Chapter 8. Removing and replacing parts

You can remove and replace customer-replaceable units (CRUs) from the control enclosure or the expansion enclosure.

Attention: If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.

Even though many of these procedures are hot-swappable, they are intended to be used only when your system is not up and running and performing I/O operations. If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Each replaceable unit has its own removal procedure. Sometimes you can find that a step within a procedure might refer you to a different remove and replace procedure. You might want to complete the new procedure before you continue with the first procedure that you started.

Remove or replace parts only when you are directed to do so.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Preparing to remove and replace parts

Before you remove and replace parts, you must be aware of all safety issues.

Before you begin

First, read the safety precautions in the IBM Systems Safety Notices. These guidelines help you safely work with the Storwize V7000.

Replacing a node canister

This topic describes how to replace a node canister.

About this task

Attention: If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.
**Attention:** Do not replace one type of node canister with another type. For example, do not replace a model 2076-112 node canister with a model 2076-312 node canister.

Be aware of the following canister LED states:

- If both the power LED and system status LED are on, do not remove a node canister unless directed to do so by a service procedure.
- If the system status is off, it is acceptable to remove a node canister. However, do not remove a node canister unless directed to do so by a service procedure.
- If the power LED is flashing or off, it is safe to remove a node canister. However, do not remove a node canister unless directed to do so by a service procedure.

**Attention:** Even if a node canister is powered off, it is still possible to lose data. Do not remove a node canister unless directed to do so by a service procedure.

To replace the node canister, perform the following steps:

**Procedure**

1. Read the safety information to which “Preparing to remove and replace parts” on page 85 refers.
2. Confirm that you know which canister to replace. Go to “Procedure: Identifying which enclosure or canister to service” on page 51.
3. Record which data cables are plugged into the specific ports of the node canister. The cables must be inserted back into the same ports after the replacement is complete; otherwise, the system cannot function properly.
4. Disconnect the data cables for each canister.
5. Grasp the handle between the thumb and forefinger.

**Note:** Ensure that you are opening the correct handle. The handle locations for the node canisters and expansion canisters are slightly different.

Handles for the node canisters are located in close proximity to each other. The handle with the finger grip on the right removes the upper canister (1), and the handle with the finger grip on the left removes the lower canister (2).

![Image](Figure%2024.%20Rear%20of%20node%20canisters%20that%20shows%20the%20handles.)

6. Squeeze them together to release the handle.
7. Pull out the handle to its full extension.
8. Grasp canister and pull it out.
9. Insert the new canister into the slot with the handle pointing towards the center of the slot. Insert the unit in the same orientation as the one that you removed.
10. Push the canister back into the slot until the handle starts to move.
11. Finish inserting the canister by closing the handle until the locking catch clicks into place.
   If the enclosure is powered on, the canister starts automatically.
12. Reattach the data cables.

Replacing an expansion canister

This topic describes how to replace an expansion canister.

About this task

Attention: If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.

Even though many of these procedures are hot-swappable, they are intended to be used only when your system is not up and running and performing I/O operations. If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.
Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Be aware of the following canister LED states:

- If the power LED is on, do not remove an expansion canister unless directed to do so by a service procedure.
- If the power LED is flashing or off, it is safe to remove an expansion canister. However, do not remove an expansion canister unless directed to do so by a service procedure.

**Attention:** Even if an expansion canister is powered off, it is still possible to lose data. Do not remove an expansion canister unless directed to do so by a service procedure.

To replace an expansion canister, perform the following steps:

**Procedure**

1. Read the safety information to which “Preparing to remove and replace parts” on page 85 refers.
2. Record which SAS cables are plugged into the specific ports of the expansion canister. The cables must be inserted back into the same ports after the replacement is complete; otherwise, the system cannot function properly.
3. Disconnect the SAS cables for each canister.
4. Grasp the handle between the thumb and forefinger.

   **Note:** Ensure that you are opening the correct handle. The handle locations for the node canisters and expansion canisters are slightly different. Handles for the upper and lower expansion canisters overlap each other. The handle with the finger grip on the left removes the upper canister (1). The handle with the finger grip on the right removes the lower canister (2).

5. Squeeze them together to release the handle.
6. Pull out the handle to its full extension.
7. Grasp canister and pull it out.
8. Insert the new canister into the slot with the handle pointing towards the center of the slot. Insert the unit in the same orientation as the one that you removed.
9. Push the canister back into the slot until the handle starts to move.
10. Finish inserting the canister by closing the handle until the locking catch clicks into place.
11. Reattach the SAS cables.

Replacing an SFP transceiver

When a failure occurs on a single link, the SFP transceiver might need to be replaced.

Before you begin

Even though many of these procedures are hot-swappable, they are intended to be used only when your system is not up and running and performing I/O operations. If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.
CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode.
Note the following information: laser radiation when open. Do not stare into the
beam, do not view directly with optical instruments, and avoid direct exposure
to the beam. (C030)

About this task
Perform the following steps to remove and then replace an SFP transceiver:

Procedure
1. Carefully determine the failing physical port connection.

   Important: The Fibre Channel links in the enclosures are supported with both
   longwave SFP transceivers and shortwave SFP transceivers. A longwave SFP
   transceiver has some blue components that are visible even when the SFP
   transceiver is plugged in. You must replace an SFP transceiver with the same
   type of SFP transceiver that you are replacing. If the SFP transceiver to replace
   is a longwave SFP transceiver, for example, you must replace with another
   longwave SFP transceiver. Removing the wrong SFP transceiver might result in
   loss of data access.

2. Remove the optical cable by pressing the release tab and pulling the cable out.
   Be careful to exert pressure only on the connector and do not pull on the
   optical cables.

3. Remove the SFP transceiver. There are a number of different handling or
   locking mechanisms that are used on the SFP transceivers. Some SFP
   transceivers might have a plastic tag. If so, pull the tag to remove the SFP
   transceiver.

   Important: Always check that the SFP transceiver that you replace matches the
   SFP transceiver that you remove.

4. Push the new SFP transceiver into the aperture and ensure that it is securely
   pushed home. The SFP transceiver usually locks into place without having to
   swing the release handle until it locks flush with the SFP transceiver. Figure 28
   illustrates an SFP transceiver and its release handle.

5. Reconnect the optical cable.

6. Confirm that the error is now fixed. Either mark the error as fixed or restart the
   node depending on the failure indication that you originally noted.
Replacing a power supply unit for a control enclosure

You can replace either of the two 764 watt hot-swap redundant power supplies in the control enclosure. These redundant power supplies operate in parallel, one continuing to power the canister if the other fails.

Before you begin

DANGER

When working on or around the system, observe the following precautions:

- Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:
  - Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
  - Do not open or service any power supply assembly.
  - Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
  - The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
  - Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
  - Connect any equipment that will be attached to this product to properly wired outlets.
  - When possible, use one hand only to connect or disconnect signal cables.
  - Never turn on any equipment when there is evidence of fire, water, or structural damage.
  - Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.

- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:

1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:

1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.
Attention: If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.

Attention: A powered-on enclosure must not have a power supply removed for more than five minutes because the cooling does not function correctly with an empty slot. Ensure that you have read and understood all these instructions and have the replacement available, and unpacked, before you remove the existing power supply.

Even though many of these procedures are hot-swappable, they are intended to be used only when your system is not up and running and performing I/O operations. If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Attention: In some instances, it might not be advisable to remove a power supply unit when a system is performing I/O. For example, the charge in the backup battery might not be sufficient enough within the partner power-supply unit to continue operations without causing a loss of access to the data. Wait until the partner battery is 100% charged before replacing the power supply unit.

Ensure that you are aware of the procedures for handling static-sensitive devices before you replace the power supply.

About this task

A replacement power supply unit is not shipped with a battery; therefore, transfer the battery from the existing power supply unit to the replacement unit. To transfer a battery, go to “Replacing a battery in a power supply unit” on page 98.

To replace the power supply, perform the following steps:

Procedure

1. Read the safety information to which “Preparing to remove and replace parts” on page 85 refers.
2. Examine the Identify LED that is lit on the front of the enclosure to identify the correct enclosure.
3. Turn off the power to the power supply units using the switches at the back of the units.
4. Disconnect the cable retention bracket and the power cord from the power supply that you are replacing.
5. Remove the power supply unit. Record the orientation of the power supply unit. Power supply unit 1 is top side up, and power supply unit 2 is inverted.
   a. Depress the black locking catch from the side with the colored sticker as shown in Figure 29 on page 93.
6. Grip the handle to pull the power supply out of the enclosure as shown in Figure 30.

6. Insert the replacement power supply unit into the enclosure with the handle pointing towards the center of the enclosure. Insert the unit in the same orientation as the one that you removed.
7. Push the power supply unit back into the enclosure until the handle starts to move.
8. Finish inserting the power supply unit into the enclosure by closing the handle until the locking catch clicks into place.
9. Reattach the power cable and cable retention bracket.
10. Turn on the power switch to the power supply unit.

What to do next

If required, return the power supply. Follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Replacing a power supply unit for an expansion enclosure

You can replace either of the two 580 watt hot-swap redundant power supplies in the expansion enclosure. These redundant power supplies operate in parallel, one continuing to power the canister if the other fails.
Before you begin

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:
1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:
1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.

Attention: If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.
Attention: A powered-on enclosure must not have a power supply removed for more than five minutes because the cooling does not function correctly with an empty slot. Ensure that you have read and understood all these instructions and have the replacement available, and unpacked, before you remove the existing power supply.

Even though many of these procedures are hot-swappable, they are intended to be used only when your system is not up and running and performing I/O operations. If your system is powered on and performing I/O operations, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Ensure that you are aware of the procedures for handling static-sensitive devices before you replace the power supply.

About this task

To replace the power supply unit in an expansion enclosure, perform the following steps:

Procedure

1. Read the safety information to which “Preparing to remove and replace parts” on page 85 refers.
2. Examine the Identify LED that is lit on the front of the enclosure to identify the correct enclosure.
3. Turn off the power to the power supply units using the switches at the back of the units.
4. Disconnect the cable retention bracket and the power cord from the power supply that you are replacing.
5. Remove the power supply unit. Record the orientation of the power supply unit. Power supply unit 1 is top side up, and power supply unit 2 is inverted.
   a. Depress the black locking catch from the side with the colored sticker as shown in Figure 31 on page 97.
b. Grip the handle to pull the power supply out of the enclosure as shown in Figure 32.

6. Insert the replacement power supply unit into the enclosure with the handle pointing towards the center of the enclosure. Insert the unit in the same orientation as the one that you removed.
7. Push the power supply unit back into the enclosure until the handle starts to move.
8. Finish inserting the power supply unit in the enclosure by closing the handle until the locking catch clicks into place.
9. Reattach the power cable and cable retention bracket.
10. Turn on the power switch to the power supply unit.

What to do next

If required, return the power supply. Follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Replacing a battery in a power supply unit

This topic describes how to replace the battery in the control enclosure power-supply unit.
Before you begin

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:
1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:
1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.
CAUTION:
The battery is a lithium ion battery. To avoid possible explosion, do not burn.
Exchange only with the IBM-approved part. Recycle or discard the battery as
instructed by local regulations. In the United States, IBM has a process for the
collection of this battery. For information, call 1-800-426-4333. Have the IBM part
number for the battery unit available when you call. (C007)

Attention: If your system is powered on and performing I/O operations, go to
the management GUI and follow the fix procedures. Performing the replacement
actions without the assistance of the fix procedures can result in loss of data or
access to data.

Even though many of these procedures are hot-swappable, they are intended to be
used only when your system is not up and running and performing I/O
operations. If your system is powered on and performing I/O operations, go to the
management GUI and follow the fix procedures. Performing the replacement
actions without the assistance of the fix procedures can result in loss of data or loss
of access to data.

Be careful when you are replacing the hardware components that are located in the
back of the system that you do not inadvertently disturb or remove any cables that
you are not instructed to remove.

About this task

Each power supply unit in a control enclosure contains an integrated battery that
is used during temporary short-term power outages. You must replace the battery
with the exact same model.

To replace the battery in the power supply unit of the control enclosure, perform
the following steps:

Procedure
1. Read the safety information to which “Preparing to remove and replace parts”
on page 85 refers.
2. Follow the removing steps of the replacing a power-supply unit procedure. Go
to “Replacing a power supply unit for a control enclosure” on page 91.
3. Remove the battery, as shown in Figure 33 on page 101.
a. Press the catch to release the handle 1.
b. Lift the handle on the battery 2.
c. Lift the battery out of the power supply unit 3.

4. Install the replacement battery.
   
   **Attention:** The replacement battery has protective end caps that must be removed prior to use.
   
   a. Remove the battery from the packaging.
   b. Remove the end caps.
   c. Attach the end caps to both ends of the battery that you removed and place the battery in the original packaging.
d. Place the replacement battery in the opening on top of the power supply in its proper orientation.

e. Press the battery to seat the connector.

f. Place the handle in its downward location

5. Push the power supply unit back into the enclosure until the handle starts to move.

6. Finish inserting the power supply unit into the enclosure by closing the handle until the locking catch clicks into place.

7. Reattach the power cable and cable retention bracket.

8. Turn on the power switch to the power supply unit.

What to do next

If required, return the battery. Follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Releasing the cable retention bracket

This topic provides instructions for releasing the cable retention bracket when removing the power cords from the power supply unit.

About this task

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Each cable retention bracket comes attached to the back of the power supply unit by the power cord plug-in.

To release a cable retention bracket, perform these steps:

Procedure

1. Unlock the cable retention bracket that is around the end of the power cord.

2. Pull the lever next to the black plastic loop slightly towards the center of the canister.

3. Continue to pull the lever towards you as you slide the cable retention bracket away from the end of the cable.

Replacing a 3.5" drive assembly or blank carrier

This topic describes how to replace a 3.5" drive assembly or blank carrier.

About this task

Attention: If your drive is configured for use, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures results in loss of data or access to data.

Attention: Do not leave a drive slot empty. Do not remove a drive or drive assembly before you have a replacement available.
The drives can be distinguished from the blank carriers by the color-coded striping on the drive. The drives are marked with an orange striping. The blank carriers are marked with a blue striping.

To replace the drive assembly or blank carrier, perform the following steps:

**Procedure**

1. Read the safety information to which "Preparing to remove and replace parts" on page 85 refers.
2. Unlock the assembly by squeezing together the tabs on the side.
3. Open the handle to the full extension.

*Figure 34. Unlocking the 3.5" drive*
Replacing a 2.5" drive assembly or blank carrier

This topic describes how to remove a 2.5" drive assembly or blank carrier.

About this task

Attention: If your drive is configured for use, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures results in loss of data or access to data.

Attention: Do not leave a drive slot empty. Do not remove a drive or drive assembly before you have a replacement available.

To replace the drive assembly or blank carrier, perform the following steps:

Procedure

1. Read the safety information to which "Preparing to remove and replace parts" on page 85 refers.
2. Unlock the module by squeezing together the tabs at the top.
3. Open the handle to the full extension.

4. Pull out the drive.

5. Push the new drive back into the slot until the handle starts to move.

6. Finish inserting the drive by closing the handle until the locking catch clicks into place.
Replacing enclosure end caps

To replace enclosure end caps, use this procedure.

About this task

To remove either the left or right end cap, complete the following steps:

Procedure

1. If the enclosure is on a table or other flat surface, elevate the enclosure front slightly or carefully extend the front over the table edge.
2. Grasp the end cap by the blue touch point and pull it until the bottom edge of the end cap is clear of the bottom tab on the chassis flange.
3. Lift the end cap off the chassis flange.

To install either the left or right end cap, complete the following steps:

4. Fit the slot that is on the top of the end cap over the tab on the top of the chassis flange.
5. Rotate the end cap down until it snaps into place. Make sure that the inside surface of the end cap is flush with the chassis.

Attention:

The left end cap is printed with information that helps identify the enclosure.
- machine type and model
- enclosure serial number
- its machine part number

The information on the end cap should always match the information printed on the rear of the enclosure, and it should also match the information that is stored on the enclosure midplane.

Replacing a SAS cable

This topic describes how to replace a SAS cable.

About this task

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

To replace a SAS cable, perform the following steps:

Procedure

1. Record which SAS cable is plugged into the specific port of the expansion canister. The cable must be inserted back into the same port after the replacement is complete; otherwise, the system cannot function properly.

   Note: If you are replacing a single cable, this step is not necessary.

2. Pull the tab with the arrow away from the connector.
3. Plug the replacement cable into the specific port.
4. Ensure that the SAS cable is fully inserted. A click is heard when the cable is successfully inserted.

Replacing a control enclosure chassis

This topic describes how to replace a control enclosure chassis.

Before you begin

Note: Ensure that you know the type of enclosure chassis that you are replacing. The procedures for replacing a control enclosure chassis are different from those procedures for replacing an expansion enclosure chassis. For information about replacing an expansion enclosure chassis, see “Replacing an expansion enclosure chassis” on page 112.
DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:
1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:
1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.
- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.

(D005)
Attention: Perform this procedure only if instructed to do so by a service action or the IBM support center. If you have a single control enclosure, this procedure requires that you shut down your system to replace the control enclosure. If you have more than one control enclosure, you can keep part of the system running, but you lose access to the volumes that are on the affected I/O group and any volumes that are in other I/O groups that depend on the drives that are in the affected I/O group. If the system is still performing I/O requests in all the I/O groups, schedule the replacement during a maintenance period or other time when the I/O can be stopped.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Ensure that you are aware of the procedures for handling static-sensitive devices before you remove the enclosure.

About this task

To replace a control enclosure chassis, perform the following steps:

Procedure

1. If you are able to access either of the node canisters with the service assistant, record the machine type and model of the enclosure, the serial number of the enclosure, and the two WWNNs for the enclosure.
   - From the service assistant home page, open the location data for the node. Record the machine type and model (MTM), the serial number, WWNN 1 and WWNN 2 from the enclosure column.
   - If you are replacing the enclosure because neither node canister can start, retrieve this information after you have completed the replacement.
     a. Start the service assistant on one of the canisters.
     b. Go to the node location data on the home page.
     c. Record the machine type and model, the serial number, WWNN 1 and WWNN 2 from the node copy column.
        The machine type and model and the serial number are also shown on the labels at the front and back of the enclosure.

2. If the enclosure is still active, shut down the host I/O and the Metro Mirror and Global Mirror activity to all the volumes that depend on the affected enclosure.
   This statement applies to all volumes in the I/O group that are managed by this enclosure plus any volumes in other I/O groups that depend on the drives in the affected I/O group.

3. If your system contains a single I/O group and if the clustered system is still online, shut the system down by using the management GUI.
   a. From the management GUI, go to Monitoring > Manage Device.
   b. Select Shut Down System from the Actions menu.
   c. Wait for the shutdown to complete.

4. If your system contains more than one I/O group and if this I/O group is still online, shut down the I/O group by using the CLI.
   a. Identify the two nodes in the I/O group.
   b. To shut down each node, issue the following CLI command once for each of the two node canisters:
stopsystem -force -node <node ID>

c. Wait for the shutdown to complete.

5. Verify that it is safe to remove the power from the enclosure.
   For each of the canisters, verify the status of the system status LED. If the LED is lit on either of the canisters, do not continue because the system is still online. Determine why the node canisters did not shut down in step 3 on page 109 or step 4 on page 109.

   **Note:** If you continue while the system is still active, you risk losing the clustered system configuration and volume cache data that is stored in the canister.

6. Turn off the power to the enclosure using the switches on the power supply units.

7. Record which data cables are plugged into the specific ports. The cables must be inserted back into the same ports after the replacement is complete; otherwise, the system cannot function properly.

8. Disconnect the cable retention brackets and the power cords from the power supply units.

9. Disconnect the data cables for each canister.

10. Remove the power supply units from the enclosure.

11. Remove the canisters from the enclosure. Record the location of each canister. They must be inserted back into the same location in the new enclosure.

12. Remove all the drives and blank drive assemblies from the enclosure. Record the location for each drive. They must be inserted back into the same location in the new enclosure.

13. Remove both enclosure end caps from the enclosure. Keep the left end cap because it is used again.

14. Remove the clamping screws that attached the enclosure to the rack cabinet.

15. Remove the enclosure chassis from the front of the rack cabinet and take the chassis to a work area.

16. Install the new enclosure chassis in the rack cabinet.

17. Remove the end caps from the new enclosure and install the clamping screws that attach the enclosure to the rack cabinet.

18. Replace the end caps. Use the new right end cap and use the left end cap that you removed in step 13. Using the left end cap that you removed preserves the model and serial number identification.

19. Reinstall the drives in the new enclosure. The drives must be inserted back into the same location from which they were removed on the old enclosure.

20. Reinstall the canisters in the enclosure. The canisters must be inserted back into the same location from which they were removed on the old enclosure.

21. Install the power supply units.

22. Reattach the data cables to each canister using the information that you recorded previously.

   **Note:** The cables must be inserted back into the same ports from which they were removed on the old enclosure; otherwise, the system cannot function properly.

23. Attach the power cords and the cable retention brackets to the power supply units.
24. Write the old enclosure machine type and model (MTM) and serial number on the repair identification (RID) tag that is supplied. Attach the tag to the left flange at the back of the enclosure.

25. Turn on the power to the enclosure using the switches on the power supply units.

The node canisters boot up. The fault LEDs are on because the new enclosure has not been set with the identity of the old enclosure. The node canisters report that they are in the wrong location.

a. Connect to the service assistant on one of the node canisters to configure the machine type and model, serial number, and WWNNs that are stored in the enclosure. If you have replaced a node canister, connect to the canister that has not been replaced.

You can connect using the previous service address. However, it is not always possible to maintain this address. If you cannot connect through the original service address, attempt to connect using the default service address. If you still cannot access the system, see “Problem: Cannot connect to the service assistant” on page 47.

b. Use the Configure enclosure panel.

c. Select the options to Update WWNN 1, Update WWNN 2, Update the machine type and model, and Update the serial number. Do not update the system ID. Use the node copy data for each of the values. Check that these values match the values that you recorded in step 1 on page 109.

If you were not able to record the values, use the node copy values only if none of them have all zeroes as their value. If any of the node copy values are all zeroes, connect the service assistant to the other node canister and configure the enclosure there. If you still do not have a full set of values, contact IBM support.

After you modify the configuration, the node attempts to restart.

Note: There are situations where the canisters restart and report critical node error 508. If the node canisters fail to become active after they restart when the enclosure is updated, check their status by using the service assistant. If both node canisters show critical node error 508, use the service assistant to restart the nodes. For any other node error, see “Procedure: Fixing node errors” on page 60. To restart a node from the service assistant, perform the following steps:

1) Log on to the service assistant.
2) From the home page, select the node that you want to restart from the Changed Node List.
3) Select Actions > Restart.

d. The system starts and can handle I/O requests from the host systems.

Note: The configuration changes that are described in the following steps must be performed to ensure that the system is operating correctly. If you do not perform these steps, the system is unable to report certain errors.

26. Start the management GUI and select Monitoring > System Details. You see an additional enclosure in the system list because the system has detected the replacement control enclosure. The original control enclosure is still listed in its configuration. The original enclosure is listed with its original enclosure ID. It is offline and managed. The new enclosure has a new enclosure ID. It is online and unmanaged.

27. Select the original enclosure in the tree view.
Verify that it is offline and managed and that the serial number is correct.

28. From the Actions menu, select Remove enclosure and confirm the action. The physical hardware has already been removed. You can ignore the messages about removing the hardware. Verify that the original enclosure is no longer listed in the tree view.

29. Add the new enclosure to the system.
   a. Select the enclosure from the tree view.
   b. From the Actions menu, select Add Control and Expansion Enclosures.
   c. Because you have already added the hardware, select Next on the first panel that asks you to install the hardware. The next panel shows the unmanaged new enclosure.
   d. Follow the steps in the wizard. The wizard changes the control enclosure to Managed.
   e. Select the enclosure and add it to the system.

30. Select the new enclosure in the tree view and verify that it is now online and managed.

31. Change the enclosure ID of the replaced enclosure to that of the original enclosure. From the Enclosure ID field, select the ID value of the original enclosure.

32. Check the status of all volumes and physical storage to ensure everything is online.

33. Restart the host application and any FlashCopy activities, Global Mirror activities, or Metro Mirror activities that were stopped.

**Results**

**Replacing an expansion enclosure chassis**

This topic describes how to replace an expansion enclosure chassis.

**Before you begin**

**Note:** Ensure that you know the type of enclosure chassis that you are replacing. The procedures for replacing an expansion enclosure chassis are different from those procedures for replacing a control enclosure chassis. For information about replacing a control enclosure chassis, see “Replacing a control enclosure chassis” on page 107.
DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To disconnect:
1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices.

To connect:
1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.

(D005)
**Attention:** If your system is powered on and performing I/O operations, go the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures can result in loss of data or access to data.

Even though many of these procedures are hot-swappable, these procedures are intended to be used only when your system is not up and running and performing I/O operations. Unless your system is offline, go to the management GUI and follow the fix procedures.

Be careful when you are replacing the hardware components that are located in the back of the system that you do not inadvertently disturb or remove any cables that you are not instructed to remove.

Ensure that you are aware of the procedures for handling static-sensitive devices before you remove the enclosure.

**About this task**

**Note:** If your system is online, replacing an expansion enclosure can cause one or more of your volumes to go offline or your quorum disks to be inaccessible. Before you proceed with these procedures, verify which volumes might go offline. From the management GUI, go to **Home > Manage Devices.** Select the enclosure that you want to replace. Then select **Show Dependent Volumes** in the **Actions** menu.

To replace an expansion enclosure chassis, perform the following steps:

**Procedure**

1. Shut down the I/O activity to the enclosure, which includes host access, FlashCopy, Metro Mirror and Global Mirror access.
2. Turn off the power to the enclosure by using the switches on the power supply units.
3. Record which data cables are plugged into the specific ports. The cables must be inserted back into the same ports after the replacement is complete; otherwise, the system cannot function properly.
4. Disconnect the cable retention brackets and the power cords from the power supply units.
5. Disconnect the data cables for each canister.
6. Remove the power supply units from the enclosure.
7. Remove the canisters from the enclosure.
8. Remove all the drives and blank drive assemblies from the enclosure. Record the location for each drive. They must be inserted back into the same location in the new enclosure.
9. Remove both enclosure end caps from the enclosure. Keep the left end cap because it is used again.
10. Remove the clamping screws that attached the enclosure to the rack cabinet.
11. Remove the enclosure chassis from the front of the rack cabinet and take the chassis to a work area.
12. Install the new enclosure chassis in the rack cabinet.
13. Remove the end caps from the new enclosure and install the clamping screws that attach the enclosure to the rack cabinet.
14. Replace the end caps. Use the new right end cap and use the left end cap that you removed in step 7 on page 114.
   Using the left end cap that you removed preserves the model and serial number identification.
15. Reinstall the drives in the new enclosure. The drives must be inserted back into the same location from which they were removed on the old enclosure.
16. Reinstall the canisters in the enclosure.
17. Install the power supply units.
18. Reattach the data cables to each canister by using the information that you recorded previously.

   Note: The cables must be inserted back into the same ports from which they were removed on the old enclosure; otherwise, the system cannot function properly.
19. Attach the power cords and the cable retention brackets to the power supply units.
20. Write the old enclosure machine type and model (MTM) and serial number on the repair identification (RID) tag that is supplied. Attach the tag to the left flange at the back of the enclosure.
21. Turn on the power to the enclosure by using the switches on the power supply units.

Results

The system records an error that indicates that an enclosure FRU replacement was detected. Go to the management GUI to use the fix procedure to change the machine type and model and serial number in the expansion enclosure.

Replacing the support rails

This topic describes how to replace the support rails.

About this task

Perform the following steps to replace the support rails:

Procedure

1. Remove the enclosure.
2. Record the location of the rail assembly in the rack cabinet.
3. Working from the back of the rack cabinet, remove the clamping screw from the rail assembly on both sides of the rack cabinet.
4. Working from the front of the rack cabinet, remove the clamping screw from the rail assembly on both sides of the rack cabinet.

5. From one side of the rack cabinet, grip the rail and slide the rail pieces together to shorten the rail.

6. Disengage the rail location pins.

7. From the other side the rack cabinet, grip the rail and slide the rail pieces together to shorten the rail.

8. Disengage the rail location pins.

9. Starting from the location of the previous rail assembly, align the bottom of the rail with the bottom of the two rack units. Insert the rail location pins through the holes in the rack cabinet.

10. Insert a clamping screw into the upper mounting hole between the rail location pins.

11. Tighten the screw to secure the rail to the rack.

12. Working from the rear of the rack cabinet, extend the rail that you secured to the front to align the bottom of the rail with the bottom of the two rack units.

   **Note:** Ensure that the rail is level between the front and the back.

13. Insert the rail location pins through the holes in the rack cabinet.

14. Insert a clamping screw into the upper mounting hole between the rail location pins.

15. Tighten the screw to secure the rail to the rack from the back side.

16. Repeat the steps to secure the opposite rail to the rack cabinet.

---

**Storwize V7000 replaceable units**

The Storwize V7000 consists of several replaceable units. Generic replaceable units are cables, SFP transceivers, canisters, power supply units, battery assemblies, and enclosure chassis.

[Table 22 on page 117](#) provides a brief description of each replaceable unit.
<table>
<thead>
<tr>
<th>Part</th>
<th>Part number</th>
<th>Applicable models</th>
<th>FRU or customer replaced</th>
</tr>
</thead>
<tbody>
<tr>
<td>2U24 enclosure chassis (empty chassis)</td>
<td>85Y5897</td>
<td>124, 224, 324</td>
<td>FRU</td>
</tr>
<tr>
<td>2U12 enclosure chassis (empty chassis)</td>
<td>85Y5896</td>
<td>112, 212, 312</td>
<td>FRU</td>
</tr>
<tr>
<td>Type 100 node canister</td>
<td>85Y5899</td>
<td>112, 124</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Type 300 node canister with 10 Gbps Ethernet ports</td>
<td>85Y6116</td>
<td>312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Expansion canister</td>
<td>85Y5850</td>
<td>212, 224</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>764 W power supply unit</td>
<td>85Y5847</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>580 W power supply unit</td>
<td>85Y5846</td>
<td>212, 224</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Battery backup unit</td>
<td>85Y5898</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>1 m SAS cable</td>
<td>44V4041</td>
<td>212, 224</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>3 m SAS cable</td>
<td>44V4163</td>
<td>212, 224</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>6 m SAS cable</td>
<td>44V4164</td>
<td>212, 224</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>1 m Fibre Channel cable</td>
<td>39M5699</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>5 m Fibre Channel cable</td>
<td>39M5700</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>25 m Fibre Channel cable</td>
<td>39M5701</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>1.8 m power cord (Chicago)</td>
<td>39M5080</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (EMEA)</td>
<td>39M5151</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Australia)</td>
<td>39M5102</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Africa)</td>
<td>39M5123</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Denmark)</td>
<td>39M5130</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (South Africa)</td>
<td>39M5144</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Switzerland)</td>
<td>39M5158</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Chile)</td>
<td>39M5165</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Israel)</td>
<td>39M5172</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Part</td>
<td>Part number</td>
<td>Applicable models</td>
<td>FRU or customer replaced</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>2.8 m power cord (Group 1 including the United States)</td>
<td>39M5081</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Argentina)</td>
<td>39M5068</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (China)</td>
<td>39M5206</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Taiwan)</td>
<td>39M5247</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Brazil)</td>
<td>39M5233</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.0 m jumper cable</td>
<td>39M5376</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (India)</td>
<td>39M5226</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>4.3 m power cord (Japan)</td>
<td>39M5200</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.8 m power cord (Korea)</td>
<td>39M5219</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” SSD, 300 GB, in carrier assembly</td>
<td>85Y5861</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 300 GB, in carrier assembly</td>
<td>85Y5862</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 450 GB, in carrier assembly</td>
<td>85Y5863</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 600 GB, in carrier assembly</td>
<td>85Y5864</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>3.5” 7.2 K nearline SAS - 2 TB in carrier assembly</td>
<td>85Y5869</td>
<td>112, 212, 312</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Blank 2.5” carrier</td>
<td>85Y5893</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Blank 3.5” carrier</td>
<td>85Y5894</td>
<td>112, 212, 312</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Fibre Channel shortwave small form-factor pluggable (SFP)</td>
<td>85Y5958</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Fibre Channel longwave small form-factor pluggable (SFP)</td>
<td>85Y5957</td>
<td>112, 124, 312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Ethernet small form-factor pluggable (SFP)</td>
<td>31P1549</td>
<td>312, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Rail kit</td>
<td>85Y5855</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Left enclosure cap including RID tag but no black MTM label</td>
<td>85Y5901</td>
<td>All</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Right enclosure cap (2U12)</td>
<td>85Y5903</td>
<td>112, 212, 312</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Right enclosure cap (2U24)</td>
<td>85Y5904</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
</tbody>
</table>
Chapter 9. Event reporting

Events that are detected are saved in an event log. As soon as an entry is made in this event log, the condition is analyzed. If any service activity is required, a notification is sent.

Event reporting process

The following methods are used to notify you and the IBM Support Center of a new event:

- If you enabled Simple Network Management Protocol (SNMP), an SNMP trap is sent to an SNMP manager that is configured by the customer.
- If enabled, log messages can be forwarded from a sender to a receiver on an IP network by using the syslog protocol.
- If enabled, event notifications can be forwarded from a sender to a receiver through Call Home email.
- If Call Home is enabled, critical faults generate a problem management record (PMR) that is sent directly to the appropriate IBM Support Center.

Understanding events

When a significant change in status is detected, an event is logged in the event log.

Error data

Events are classified as either alerts or messages:

- An alert is logged when the event requires some action. Some alerts have an associated error code that defines the service action that is required. The service actions are automated through the fix procedures. If the alert does not have an error code, the alert represents an unexpected change in state. This situation must be investigated to see if it is expected or represents a failure. Investigate an alert and resolve it as soon as it is reported.
- A message is logged when a change that is expected is reported, for instance, an IBM FlashCopy operation completes.

Viewing the event log

You can view the event log by using the management GUI or the command-line interface (CLI).

About this task

You can view the event log by using the Monitoring > Events options in the management GUI. The event log contains many entries. You can, however, select only the type of information that you need.

You can also view the event log by using the command-line interface (ls-eventlog). See the “Command-line interface” topic for the command details.
Managing the event log

The event log has a limited size. After it is full, newer entries replace entries that are no longer required.

To avoid having a repeated event that fills the event log, some records in the event log refer to multiple occurrences of the same event. When event log entries are coalesced in this way, the time stamp of the first occurrence and the last occurrence of the problem is saved in the log entry. A count of the number of times that the error condition has occurred is also saved in the log entry. Other data refers to the last occurrence of the event.

Describing the fields in the event log

The event log includes fields with information that you can use to diagnose problems.

Table 23 describes some of the fields that are available to assist you in diagnosing problems.

<table>
<thead>
<tr>
<th>Data field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>This number precisely identifies why the event was logged.</td>
</tr>
<tr>
<td>Error code</td>
<td>This number describes the service action that should be followed to resolve an error condition. Not all events have error codes that are associated with them. Many event IDs can have the same error code because the service action is the same for all the events.</td>
</tr>
<tr>
<td>Sequence number</td>
<td>A number that identifies the event.</td>
</tr>
<tr>
<td>Event count</td>
<td>The number of events coalesced into this event log record.</td>
</tr>
<tr>
<td>Object type</td>
<td>The object type to which the event log relates.</td>
</tr>
<tr>
<td>Object ID</td>
<td>A number that uniquely identifies the instance of the object.</td>
</tr>
<tr>
<td>Fixed</td>
<td>When an alert is shown for an error condition, it indicates if the reason for the event was resolved. In many cases, the system automatically marks the events fixed when appropriate. There are some events that must be manually marked as fixed. If the event is a message, this field indicates that you have read and performed the action. The message must be marked as read.</td>
</tr>
<tr>
<td>First time</td>
<td>The time when this error event was reported. If events of a similar type are being coalesced together, so that one event log record represents more than one event, this field is the time the first error event was logged.</td>
</tr>
<tr>
<td>Last time</td>
<td>The time when the last instance of this error event was recorded in the log.</td>
</tr>
<tr>
<td>Root sequence number</td>
<td>If set, this number is the sequence number of an event that represents an error that probably caused this event to be reported. Resolve the root event first.</td>
</tr>
<tr>
<td>Sense data</td>
<td>Additional data that gives the details of the condition that caused the event to be logged.</td>
</tr>
</tbody>
</table>
Event notifications

The SAN Volume Controller product can use Simple Network Management Protocol (SNMP) traps, syslog messages, emails and Call Homes notify you and the IBM(r) Remote Technical Support Center when significant events are detected. Any combination of these notification methods can be used simultaneously. Notifications are normally sent immediately after an event is raised. However, there are some events that might occur because of service actions that are being performed. If a recommended service action is active, these events are notified only if they are still unfixed when the service action completes.

Only events recorded in the event log can be notified. Most CLI messages in response to some CLI commands are not recorded in the event log so do not cause an event notification.

Table 24 describes the levels of event notifications.

<table>
<thead>
<tr>
<th>Notification level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Critical notification is sent to indicate a problem that must be corrected as soon as possible. This notification indicates a serious problem with the Storwize V7000. For example, the event that is being reported could indicate a loss of redundancy in the system, and it is possible that another failure could result in loss of access to data. The most typical reason that this type of notification is sent is because of a hardware failure, but some configuration errors or fabric errors also are included in this notification level. Critical notifications can be configured to be sent as a Call Home to the IBM Remote Technical Support.</td>
</tr>
<tr>
<td>Warning</td>
<td>A warning notification is sent to indicate a problem or unexpected condition with the Storwize V7000. Always immediately investigate this type of notification to determine the effect that it might have on your operation, and make any necessary corrections. A warning notification does not require any replacement parts and therefore should not require IBM Support Center involvement. The allocation of notification type Warning does not imply that the event is less serious than one that has notification level Critical.</td>
</tr>
<tr>
<td>Information</td>
<td>An informational notification is sent to indicate that an expected event has occurred: for example, a FlashCopy operation has completed. No remedial action is required when these notifications are sent.</td>
</tr>
</tbody>
</table>

Power-on self-test

When you turn on the system, the node canisters perform self-tests.

A series of tests is performed to check the operation of components and some of the options that have been installed when the units are first turned on. This series of tests is called the power-on self-test (POST).

If a critical failure is detected during the POST, the software is not loaded and the fault LED is illuminated. To determine if there is a POST error on a canister, go to “Procedure: Understanding the system status using the LEDs” on page 54.
When the code is loaded, additional testing takes place, which ensures that all of the required hardware and code components are installed and functioning correctly.

**Understanding the error codes**

Error codes are generated by the event-log analysis and system configuration code.

Error codes help you to identify the cause of a problem, the failing field-replaceable units (FRUs), and the service actions that might be needed to solve the problem.

**Event IDs**

The Storwize V7000 software generates events, such as informational events and error events. An event ID or number is associated with the event and indicates the reason for the event.

Informational events provide information about the status of an operation. Informational events are recorded in the event log, and depending on the configuration, can be notified through email, SNMP, or syslog.

Error events are generated when a service action is required. An error event maps to an alert with an associated error code. Depending on the configuration, error events can be notified through email, SNMP, or syslog.

**Informational events**

The informational events provide information about the status of an operation.

Informational events are recorded in the event log and, depending on the configuration, can be notified through email, SNMP, or syslog.

Informational events can be either notification type I (information) or notification type W (warning). An informational event report of type (W) might require user attention. Table 25 provides a list of informational events, the notification type, and the reason for the event.

**Table 25. Informational events**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>980221</td>
<td>I</td>
<td>The error log is cleared.</td>
</tr>
<tr>
<td>980230</td>
<td>I</td>
<td>The SSH key was discarded for the service login user.</td>
</tr>
<tr>
<td>980231</td>
<td>I</td>
<td>User name has changed.</td>
</tr>
<tr>
<td>980301</td>
<td>I</td>
<td>Degraded or offline managed disk is now online.</td>
</tr>
<tr>
<td>980310</td>
<td>I</td>
<td>A degraded or offline storage pool is now online.</td>
</tr>
<tr>
<td>980320</td>
<td>I</td>
<td>Offline volume is now online.</td>
</tr>
<tr>
<td>980321</td>
<td>W</td>
<td>Volume is offline because of degraded or offline storage pool.</td>
</tr>
<tr>
<td>980330</td>
<td>I</td>
<td>All nodes can see the port.</td>
</tr>
<tr>
<td>980340</td>
<td>I</td>
<td>All ports in this host are now logged in.</td>
</tr>
<tr>
<td>980341</td>
<td>W</td>
<td>One or more ports in this host is now degraded.</td>
</tr>
<tr>
<td>980342</td>
<td>W</td>
<td>One or more ports in this host is now offline.</td>
</tr>
</tbody>
</table>
### Table 25. Informational events (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>980343</td>
<td>W</td>
<td>All ports in this host are now offline.</td>
</tr>
<tr>
<td>980349</td>
<td>I</td>
<td>A node has been successfully added to the cluster (system).</td>
</tr>
<tr>
<td>980350</td>
<td>I</td>
<td>The node is now a functional member of the cluster (system).</td>
</tr>
<tr>
<td>980351</td>
<td>I</td>
<td>A noncritical hardware error occurred.</td>
</tr>
<tr>
<td>980352</td>
<td>I</td>
<td>Attempt to automatically recover offline node starting.</td>
</tr>
<tr>
<td>980370</td>
<td>I</td>
<td>Both nodes in the I/O group are available.</td>
</tr>
<tr>
<td>980371</td>
<td>I</td>
<td>One node in the I/O group is unavailable.</td>
</tr>
<tr>
<td>980372</td>
<td>W</td>
<td>Both nodes in the I/O group are unavailable.</td>
</tr>
<tr>
<td>980380</td>
<td>I</td>
<td>Maintenance mode was started.</td>
</tr>
<tr>
<td>980381</td>
<td>I</td>
<td>Maintenance mode has ended.</td>
</tr>
<tr>
<td>980392</td>
<td>I</td>
<td>Cluster (system) recovery completed.</td>
</tr>
<tr>
<td>980435</td>
<td>W</td>
<td>Failed to obtain directory listing from remote node.</td>
</tr>
<tr>
<td>980440</td>
<td>W</td>
<td>Failed to transfer file from remote node.</td>
</tr>
<tr>
<td>980445</td>
<td>I</td>
<td>The migration is complete.</td>
</tr>
<tr>
<td>980446</td>
<td>I</td>
<td>The secure delete is complete.</td>
</tr>
<tr>
<td>980501</td>
<td>W</td>
<td>The virtualization amount is close to the limit that is licensed.</td>
</tr>
<tr>
<td>980502</td>
<td>W</td>
<td>The FlashCopy feature is close to the limit that is licensed.</td>
</tr>
<tr>
<td>980503</td>
<td>W</td>
<td>The Metro Mirror or Global Mirror feature is close to the limit that is licensed.</td>
</tr>
<tr>
<td>980504</td>
<td>I</td>
<td>The limit was reached for the external virtualization feature.</td>
</tr>
<tr>
<td>980505</td>
<td>I</td>
<td>The limit was reached for the compression feature license.</td>
</tr>
<tr>
<td>981002</td>
<td>I</td>
<td>Fibre Channel discovery occurred; configuration changes are pending.</td>
</tr>
<tr>
<td>981003</td>
<td>I</td>
<td>Fibre Channel discovery occurred; configuration changes are complete.</td>
</tr>
<tr>
<td>981004</td>
<td>I</td>
<td>Fibre Channel discovery occurred; no configuration changes were detected.</td>
</tr>
<tr>
<td>981007</td>
<td>W</td>
<td>The managed disk is not on the preferred path.</td>
</tr>
<tr>
<td>981009</td>
<td>W</td>
<td>The initialization for the managed disk failed.</td>
</tr>
<tr>
<td>981014</td>
<td>W</td>
<td>The LUN discovery has failed. The cluster (system) has a connection to a device through this node but this node cannot discover the unmanaged or managed disk that is associated with this LUN.</td>
</tr>
<tr>
<td>981015</td>
<td>W</td>
<td>The LUN capacity equals or exceeds the maximum. Only part of the disk can be accessed.</td>
</tr>
<tr>
<td>981020</td>
<td>W</td>
<td>The managed disk error count warning threshold has been met.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>981022</td>
<td>I</td>
<td>Managed disk offline imminent, offline prevention started</td>
</tr>
<tr>
<td>981025</td>
<td>I</td>
<td>Drive firmware download started</td>
</tr>
<tr>
<td>981026</td>
<td>I</td>
<td>Drive FPGA download started</td>
</tr>
<tr>
<td>981101</td>
<td>I</td>
<td>SAS discovery occurred; no configuration changes were detected.</td>
</tr>
<tr>
<td>981102</td>
<td>I</td>
<td>SAS discovery occurred; configuration changes are pending.</td>
</tr>
<tr>
<td>981103</td>
<td>I</td>
<td>SAS discovery occurred; configuration changes are complete.</td>
</tr>
<tr>
<td>981104</td>
<td>W</td>
<td>The LUN capacity equals or exceeds the maximum capacity. Only the first 1 PB of disk will be accessed.</td>
</tr>
<tr>
<td>981105</td>
<td>I</td>
<td>The drive format has started.</td>
</tr>
<tr>
<td>981106</td>
<td>I</td>
<td>The drive recovery was started.</td>
</tr>
<tr>
<td>982003</td>
<td>W</td>
<td>Insufficient virtual extents.</td>
</tr>
<tr>
<td>982004</td>
<td>W</td>
<td>The migration suspended because of insufficient virtual extents or too many media errors on the source managed disk.</td>
</tr>
<tr>
<td>982007</td>
<td>W</td>
<td>Migration has stopped.</td>
</tr>
<tr>
<td>982009</td>
<td>I</td>
<td>Migration is complete.</td>
</tr>
<tr>
<td>982010</td>
<td>W</td>
<td>Copied disk I/O medium error.</td>
</tr>
<tr>
<td>983001</td>
<td>I</td>
<td>The FlashCopy operation is prepared.</td>
</tr>
<tr>
<td>983002</td>
<td>I</td>
<td>The FlashCopy operation is complete.</td>
</tr>
<tr>
<td>983003</td>
<td>W</td>
<td>The FlashCopy operation has stopped.</td>
</tr>
<tr>
<td>984001</td>
<td>W</td>
<td>First customer data being pinned in a virtual disk working set.</td>
</tr>
<tr>
<td>984002</td>
<td>I</td>
<td>All customer data in a virtual disk working set is now unpinned.</td>
</tr>
<tr>
<td>984003</td>
<td>W</td>
<td>The volume working set cache mode is in the process of changing to synchronous destage because the volume working set has too much pinned data.</td>
</tr>
<tr>
<td>984004</td>
<td>I</td>
<td>Volume working set cache mode updated to allow asynchronous destage because enough customer data has been unpinned for the volume working set.</td>
</tr>
<tr>
<td>984501</td>
<td>I</td>
<td>The firmware level of an enclosure component is being updated.</td>
</tr>
<tr>
<td>984502</td>
<td>I</td>
<td>The firmware level updated has completed.</td>
</tr>
<tr>
<td>984503</td>
<td>I</td>
<td>The battery conditioning completed.</td>
</tr>
<tr>
<td>984504</td>
<td>I</td>
<td>The battery conditioning started.</td>
</tr>
<tr>
<td>984505</td>
<td>I</td>
<td>The statesave information for the enclosure was collected.</td>
</tr>
<tr>
<td>984506</td>
<td>I</td>
<td>The debug from an IERR was extracted to disk.</td>
</tr>
<tr>
<td>984507</td>
<td>I</td>
<td>An attempt was made to power on the slots.</td>
</tr>
<tr>
<td>984508</td>
<td>I</td>
<td>All the expanders on the strand were reset.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>984509</td>
<td>I</td>
<td>The component firmware update paused to allow the battery charging to finish.</td>
</tr>
<tr>
<td>984511</td>
<td>I</td>
<td>The update for the component firmware paused because the system was put into maintenance mode.</td>
</tr>
<tr>
<td>984512</td>
<td>I</td>
<td>A component firmware update is needed but is prevented from running.</td>
</tr>
<tr>
<td>985001</td>
<td>I</td>
<td>The Metro Mirror or Global Mirror background copy is complete.</td>
</tr>
<tr>
<td>985002</td>
<td>I</td>
<td>The Metro Mirror or Global Mirror is ready to restart.</td>
</tr>
<tr>
<td>985003</td>
<td>W</td>
<td>Unable to find path to disk in the remote cluster (system) within the timeout period.</td>
</tr>
<tr>
<td>986001</td>
<td>W</td>
<td>The thin-provisioned volume copy data in a node is pinned.</td>
</tr>
<tr>
<td>986002</td>
<td>I</td>
<td>All thin-provisioned volume copy data in a node is unpinned.</td>
</tr>
<tr>
<td>986010</td>
<td>I</td>
<td>The thin-provisioned volume copy import has failed and the new volume is offline; either upgrade the Storwize V7000 software to the required version or delete the volume.</td>
</tr>
<tr>
<td>986011</td>
<td>I</td>
<td>The thin-provisioned volume copy import is successful.</td>
</tr>
<tr>
<td>986020</td>
<td>W</td>
<td>A thin-provisioned volume copy space warning has occurred.</td>
</tr>
<tr>
<td>986030</td>
<td>I</td>
<td>A thin-provisioned volume copy repair has started.</td>
</tr>
<tr>
<td>986031</td>
<td>I</td>
<td>A thin-provisioned volume copy repair is successful.</td>
</tr>
<tr>
<td>986032</td>
<td>I</td>
<td>A thin-provisioned volume copy validation is started.</td>
</tr>
<tr>
<td>986033</td>
<td>I</td>
<td>A thin-provisioned volume copy validation is successful.</td>
</tr>
<tr>
<td>986034</td>
<td>I</td>
<td>The import of the compressed-virtual volume copy was successful.</td>
</tr>
<tr>
<td>986035</td>
<td>W</td>
<td>A compressed-virtual volume copy space warning has occurred.</td>
</tr>
<tr>
<td>986036</td>
<td>I</td>
<td>A compressed-virtual volume copy repair has started.</td>
</tr>
<tr>
<td>986037</td>
<td>I</td>
<td>A compressed-virtual volume copy repair is successful.</td>
</tr>
<tr>
<td>986038</td>
<td>I</td>
<td>A compressed-virtual volume copy has too many bad blocks.</td>
</tr>
<tr>
<td>986201</td>
<td>I</td>
<td>A medium error has been repaired for the mirrored copy.</td>
</tr>
<tr>
<td>986203</td>
<td>W</td>
<td>A mirror copy repair, using the validate option cannot complete.</td>
</tr>
<tr>
<td>986204</td>
<td>I</td>
<td>A mirror disk repair is complete and no differences are found.</td>
</tr>
<tr>
<td>986205</td>
<td>I</td>
<td>A mirror disk repair is complete and the differences are resolved.</td>
</tr>
</tbody>
</table>
Table 25. Informational events (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>986206</td>
<td>W</td>
<td>A mirror disk repair is complete and the differences are marked as medium errors.</td>
</tr>
<tr>
<td>986207</td>
<td>I</td>
<td>The mirror disk repair has been started.</td>
</tr>
<tr>
<td>986208</td>
<td>W</td>
<td>A mirror copy repair, using the set medium error option, cannot complete.</td>
</tr>
<tr>
<td>986209</td>
<td>W</td>
<td>A mirror copy repair, using the resync option, cannot complete.</td>
</tr>
<tr>
<td>987102</td>
<td>W</td>
<td>Node coldstarted.</td>
</tr>
<tr>
<td>987103</td>
<td>W</td>
<td>A node power-off has been requested from the power switch.</td>
</tr>
<tr>
<td>987104</td>
<td>I</td>
<td>Additional Fibre Channel ports were connected.</td>
</tr>
<tr>
<td>987301</td>
<td>W</td>
<td>The connection to a configured remote cluster (system) has been lost.</td>
</tr>
<tr>
<td>987400</td>
<td>W</td>
<td>The node unexpectedly lost power but has now been restored to the cluster (system).</td>
</tr>
<tr>
<td>988100</td>
<td>W</td>
<td>An overnight maintenance procedure has failed to complete. Resolve any hardware and configuration problems that you are experiencing on the cluster (system). If the problem persists, contact your IBM service representative for assistance.</td>
</tr>
<tr>
<td>988300</td>
<td>W</td>
<td>An array MDisk is offline because it has too many missing members.</td>
</tr>
<tr>
<td>988301</td>
<td>I</td>
<td>The rebuild for an array MDisk was started.</td>
</tr>
<tr>
<td>988302</td>
<td>I</td>
<td>The rebuild for an array MDisk has finished.</td>
</tr>
<tr>
<td>988304</td>
<td>I</td>
<td>A RAID array has started exchanging an array member.</td>
</tr>
<tr>
<td>988305</td>
<td>I</td>
<td>A RAID array has completed exchanging an array member.</td>
</tr>
<tr>
<td>988306</td>
<td>I</td>
<td>A RAID array needs resynchronization.</td>
</tr>
<tr>
<td>989001</td>
<td>W</td>
<td>A managed disk group space warning has occurred.</td>
</tr>
</tbody>
</table>

Error event IDs and error codes

Error codes describe a service procedure that must be followed. Each event ID that requires service has an associated error code.

Error codes can be either notification type E (error) or notification type W (warning). Table 26 lists the event IDs and corresponding error codes, the notification type, and the condition of the event.

Table 26. Error event IDs and error codes

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>009020</td>
<td>E</td>
<td>An automatic system recovery has started. All configuration commands are blocked.</td>
<td>1001</td>
</tr>
<tr>
<td>009040</td>
<td>E</td>
<td>The error event log is full.</td>
<td>1002</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Condition</td>
<td>Error code</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| 009052  | W                | The following causes are possible:  
• The node is missing.  
• The node is no longer a functional member of the system. | 1196       |
<p>| 009053  | E                | A node has been missing for 30 minutes.                                                                                                     | 1195       |
| 009100  | W                | The software install process has failed.                                                                                                     | 2010       |
| 009101  | W                | The software upgrade package delivery has failed.                                                                                             | 2010       |
| 009150  | W                | Unable to connect to the SMTP (email) server                                                                                                | 2600       |
| 009151  | W                | Unable to send mail through the SMTP (email) server                                                                                           | 2601       |
| 009170  | W                | The Metro Mirror or Global Mirror feature capacity is not set.                                                                                | 3030       |
| 009171  | W                | The FlashCopy feature capacity is not set.                                                                                                   | 3031       |
| 009172  | W                | The Virtualization feature has exceeded the amount that is licensed.                                                                        | 3032       |
| 009173  | W                | The FlashCopy feature has exceeded the amount that is licensed.                                                                               | 3032       |
| 009174  | W                | The Metro Mirror or Global Mirror feature has exceeded the amount that is licensed.                                                          | 3032       |
| 009175  | W                | The usage for the thin-provisioned volume is not licensed.                                                                                     | 3033       |
| 009176  | W                | The value set for the virtualization feature capacity is not valid.                                                                           | 3029       |
| 009177  | E                | A physical disk FlashCopy feature license is required.                                                                                         | 3035       |
| 009178  | E                | A physical disk Metro Mirror and Global Mirror feature license is required.                                                                    | 3036       |
| 009179  | E                | A virtualization feature license is required.                                                                                                | 3025       |
| 009180  | E                | Automatic recovery of offline node failed.                                                                                                   | 1194       |
| 009181  | W                | Unable to send email to any of the configured email servers.                                                                                   | 3081       |
| 009182  | W                | The external virtualization feature license limit was exceeded.                                                                             | 3032       |
| 009183  | W                | Unable to connect to LDAP server.                                                                                                            | 2251       |
| 009184  | W                | The LDAP configuration is not valid.                                                                                                          | 2250       |
| 009185  | E                | The limit for the compression feature license was exceeded.                                                                                  | 3032       |
| 009186  | E                | The limit for the compression feature license was exceeded.                                                                                  | 3032       |
| 010002  | E                | The node ran out of base event sources. As a result, the node has stopped and exited the system.                                               | 2030       |
| 010003  | W                | The number of device logins has reduced.                                                                                                      | 1630       |
| 010006  | E                | A software error has occurred.                                                                                                               | 2030       |
| 010008  | E                | The block size is invalid, the capacity or LUN identity has changed during the managed disk initialization.                                      | 1660       |</p>
<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>010010 E</td>
<td>E</td>
<td>The managed disk is excluded because of excessive errors.</td>
<td>1310</td>
</tr>
<tr>
<td>010011 E</td>
<td>E</td>
<td>The remote port is excluded for a managed disk and node.</td>
<td>1220</td>
</tr>
<tr>
<td>010012 E</td>
<td>E</td>
<td>The local port is excluded.</td>
<td>1210</td>
</tr>
<tr>
<td>010013 E</td>
<td>E</td>
<td>The login is excluded.</td>
<td>1230</td>
</tr>
<tr>
<td>010014 E</td>
<td>E</td>
<td>The local port is excluded.</td>
<td>1211</td>
</tr>
<tr>
<td>010017 E</td>
<td>E</td>
<td>A timeout has occurred as a result of excessive processing time.</td>
<td>1340</td>
</tr>
<tr>
<td>010018 E</td>
<td>E</td>
<td>An error recovery procedure has occurred.</td>
<td>1370</td>
</tr>
<tr>
<td>010019 E</td>
<td>E</td>
<td>A managed disk I/O error has occurred.</td>
<td>1310</td>
</tr>
<tr>
<td>010020 E</td>
<td>E</td>
<td>The managed disk error count threshold has exceeded.</td>
<td>1310</td>
</tr>
<tr>
<td>010021 W</td>
<td>W</td>
<td>There are too many devices presented to the cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010022 W</td>
<td>W</td>
<td>There are too many managed disks presented to the cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010023 W</td>
<td>W</td>
<td>There are too many LUNs presented to a node.</td>
<td>1200</td>
</tr>
<tr>
<td>010024 W</td>
<td>W</td>
<td>There are too many drives presented to a cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010025 W</td>
<td>W</td>
<td>A disk I/O medium error has occurred.</td>
<td>1320</td>
</tr>
<tr>
<td>010026 W</td>
<td>W</td>
<td>A suitable MDisk or drive for use as a quorum disk was not found.</td>
<td>1330</td>
</tr>
<tr>
<td>010027 W</td>
<td>W</td>
<td>The quorum disk is not available.</td>
<td>1335</td>
</tr>
<tr>
<td>010028 W</td>
<td>W</td>
<td>A controller configuration is not supported.</td>
<td>1625</td>
</tr>
<tr>
<td>010029 E</td>
<td>E</td>
<td>A login transport fault has occurred.</td>
<td>1360</td>
</tr>
<tr>
<td>010030 E</td>
<td>E</td>
<td>A managed disk error recovery procedure (ERP) has occurred. The node or controller reported the following: • Sense • Key • Code • Qualifier</td>
<td>1370</td>
</tr>
<tr>
<td>010031 E</td>
<td>E</td>
<td>One or more MDisks on a controller are degraded.</td>
<td>1623</td>
</tr>
<tr>
<td>010032 W</td>
<td>W</td>
<td>The controller configuration limits failover.</td>
<td>1625</td>
</tr>
<tr>
<td>010033 E</td>
<td>E</td>
<td>The controller configuration uses the RDAC mode; this is not supported.</td>
<td>1624</td>
</tr>
<tr>
<td>010034 E</td>
<td>E</td>
<td>Persistent unsupported controller configuration.</td>
<td>1695</td>
</tr>
<tr>
<td>010040 E</td>
<td>E</td>
<td>The controller system device is only connected to the node through a single initiator port.</td>
<td>1627</td>
</tr>
<tr>
<td>010041 E</td>
<td>E</td>
<td>The controller system device is only connected to the node through a single target port.</td>
<td>1627</td>
</tr>
<tr>
<td>010042 E</td>
<td>E</td>
<td>The controller system device is only connected to the cluster (system) nodes through a single target port.</td>
<td>1627</td>
</tr>
</tbody>
</table>
### Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>010043</td>
<td>E</td>
<td>The controller system device is only connected to the cluster (system) nodes through half of the expected target ports.</td>
<td>1627</td>
</tr>
<tr>
<td>010044</td>
<td>E</td>
<td>The controller system device has disconnected all target ports to the cluster (system) nodes.</td>
<td>1627</td>
</tr>
<tr>
<td>010050</td>
<td>W</td>
<td>A solid-state drive (SSD) failed. A rebuild is required.</td>
<td>1201</td>
</tr>
<tr>
<td>010051</td>
<td>E</td>
<td>A solid-state drive (SSD) is missing.</td>
<td>1202</td>
</tr>
<tr>
<td>010052</td>
<td>E</td>
<td>A solid-state drive (SSD) is offline as a result of a drive hardware error.</td>
<td>1205</td>
</tr>
<tr>
<td>010053</td>
<td>E</td>
<td>A solid-state drive (SSD) is reporting a predictive failure analysis (PFA).</td>
<td>1215</td>
</tr>
<tr>
<td>010054</td>
<td>E</td>
<td>A solid-state drive (SSD) is reporting too many errors.</td>
<td>1215</td>
</tr>
<tr>
<td>010055</td>
<td>W</td>
<td>An unrecognized SAS device.</td>
<td>1665</td>
</tr>
<tr>
<td>010056</td>
<td>E</td>
<td>SAS error counts exceeded the warning thresholds.</td>
<td>1216</td>
</tr>
<tr>
<td>010057</td>
<td>E</td>
<td>SAS errors exceeded critical thresholds.</td>
<td>1216</td>
</tr>
<tr>
<td>010058</td>
<td>E</td>
<td>The drive initialization failed because of an unknown block size or a block size that is not valid; an unknown capacity or a capacity that is not valid; or was not able to set the required mode pages.</td>
<td>1661</td>
</tr>
<tr>
<td>010059</td>
<td>E</td>
<td>A solid-state drive (SSD) is offline due to excessive errors.</td>
<td>1311</td>
</tr>
<tr>
<td>010060</td>
<td>E</td>
<td>A solid-state drive (SSD) exceeded the warning temperature threshold.</td>
<td>1217</td>
</tr>
<tr>
<td>010061</td>
<td>E</td>
<td>A solid-state drive (SSD) exceeded the offline temperature threshold.</td>
<td>1218</td>
</tr>
<tr>
<td>010062</td>
<td>E</td>
<td>A drive exceeded the warning temperature threshold.</td>
<td>1217</td>
</tr>
<tr>
<td>010063</td>
<td>W</td>
<td>Drive medium error.</td>
<td>1321</td>
</tr>
<tr>
<td>010066</td>
<td>W</td>
<td>Controller indicates that it does not support descriptor sense for LUNs that are greater than 2 TBs.</td>
<td>1625</td>
</tr>
<tr>
<td>010067</td>
<td>W</td>
<td>Too many enclosures were presented to a cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010068</td>
<td>E</td>
<td>The solid-state drive (SSD) format was corrupted.</td>
<td>1204</td>
</tr>
<tr>
<td>010069</td>
<td>E</td>
<td>The block size for the solid-state drive (SSD) was incorrect.</td>
<td>1204</td>
</tr>
<tr>
<td>010070</td>
<td>W</td>
<td>Too many controller target ports were presented to the cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010071</td>
<td>W</td>
<td>Too many target ports were presented to the cluster (system) from a single controller.</td>
<td>1200</td>
</tr>
<tr>
<td>010072</td>
<td>E</td>
<td>The drive is offline as a result of a drive hardware error.</td>
<td>1680</td>
</tr>
<tr>
<td>010073</td>
<td>E</td>
<td>The drive is reporting predictive failure analysis (PFA) errors.</td>
<td>1680</td>
</tr>
<tr>
<td>010080</td>
<td>E</td>
<td>The drive is reporting too many errors.</td>
<td>1680</td>
</tr>
<tr>
<td>010081</td>
<td>E</td>
<td>The drive format is corrupted.</td>
<td>1206</td>
</tr>
<tr>
<td>010082</td>
<td>E</td>
<td>The block size for the drive was incorrect.</td>
<td>1206</td>
</tr>
</tbody>
</table>
Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>010083</td>
<td>E</td>
<td>The drive is offline due to excessive errors.</td>
<td>1680</td>
</tr>
<tr>
<td>010084</td>
<td>E</td>
<td>The error counts for the SAS drive exceeded the warning thresholds.</td>
<td>1285</td>
</tr>
<tr>
<td>010085</td>
<td>W</td>
<td>The SAS device was not recognized.</td>
<td>1666</td>
</tr>
<tr>
<td>010086</td>
<td>W</td>
<td>The SAS enclosure was not recognized.</td>
<td>1666</td>
</tr>
<tr>
<td>010087</td>
<td>W</td>
<td>The SAS device was not able to be identified.</td>
<td>1666</td>
</tr>
<tr>
<td>010088</td>
<td>E</td>
<td>There were excessive medium errors on the drive.</td>
<td>1680</td>
</tr>
<tr>
<td>010089</td>
<td>E</td>
<td>There were excessive overall timeout errors on the drive.</td>
<td>1680</td>
</tr>
<tr>
<td>010090</td>
<td>E</td>
<td>There were excessive times when the drive stopped.</td>
<td>1680</td>
</tr>
<tr>
<td>010091</td>
<td>E</td>
<td>A drive failed validation testing.</td>
<td>1680</td>
</tr>
<tr>
<td>010092</td>
<td>E</td>
<td>There were excessive medium errors on the solid-state drive (SSD).</td>
<td>1215</td>
</tr>
<tr>
<td>010093</td>
<td>E</td>
<td>There were excessive overall timeout errors on the solid-state drive (SSD)</td>
<td>1204</td>
</tr>
<tr>
<td>010094</td>
<td>E</td>
<td>Login excluded.</td>
<td>1231</td>
</tr>
<tr>
<td>010095</td>
<td>E</td>
<td>Drive failed.</td>
<td>1687</td>
</tr>
<tr>
<td>010096</td>
<td>E</td>
<td>The drive initialization failed because of an unknown block size or a block size that is not valid; an unknown capacity or a capacity that is not valid; or was not able to set the required mode pages.</td>
<td>1680</td>
</tr>
<tr>
<td>010097</td>
<td>E</td>
<td>A drive is reporting excessive errors.</td>
<td>1685</td>
</tr>
<tr>
<td>010098</td>
<td>W</td>
<td>There are too many drives presented to a cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>020001</td>
<td>E</td>
<td>There are too many medium errors on the managed disk.</td>
<td>1610</td>
</tr>
<tr>
<td>020002</td>
<td>E</td>
<td>A managed disk group is offline.</td>
<td>1620</td>
</tr>
<tr>
<td>020003</td>
<td>W</td>
<td>There are insufficient virtual extents.</td>
<td>2030</td>
</tr>
<tr>
<td>029001</td>
<td>W</td>
<td>The managed disk has bad blocks. On an external controller, this can only be a copied medium error.</td>
<td>1840</td>
</tr>
<tr>
<td>029002</td>
<td>E</td>
<td>The system failed to create a bad block because MDisk already has the maximum number of allowed bad blocks.</td>
<td>1226</td>
</tr>
<tr>
<td>029003</td>
<td>E</td>
<td>The system failed to create a bad block because the clustered system already has the maximum number of allowed bad blocks.</td>
<td>1225</td>
</tr>
<tr>
<td>030000</td>
<td>W</td>
<td>The trigger prepare command has failed because of a cache flush failure.</td>
<td>1900</td>
</tr>
<tr>
<td>030010</td>
<td>W</td>
<td>The mapping is stopped because of the error that is indicated in the data.</td>
<td>1910</td>
</tr>
<tr>
<td>030020</td>
<td>W</td>
<td>The mapping is stopped because of a clustered system or complete I/O group failure, and the current state of the relationship could not be recovered.</td>
<td>1895</td>
</tr>
<tr>
<td>045001</td>
<td>E</td>
<td>One or more power supply unit fans have failed.</td>
<td>1124</td>
</tr>
<tr>
<td>045002</td>
<td>E</td>
<td>A fan is operating outside the expected range.</td>
<td>1126</td>
</tr>
<tr>
<td>045003</td>
<td>E</td>
<td>There was a fan status communications failure.</td>
<td>1126</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Condition</td>
<td>Error code</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>045004</td>
<td>E</td>
<td>The power supply unit is not installed.</td>
<td>1128</td>
</tr>
<tr>
<td>045005</td>
<td>W</td>
<td>The power supply unit has indicated an input power failure.</td>
<td>1138</td>
</tr>
<tr>
<td>045006</td>
<td>E</td>
<td>The power supply unit has indicated a dc failure.</td>
<td>1126</td>
</tr>
<tr>
<td>045007</td>
<td>E</td>
<td>The power supply unit has failed.</td>
<td>1124</td>
</tr>
<tr>
<td>045008</td>
<td>E</td>
<td>There is no communication with the power supply unit.</td>
<td>1148</td>
</tr>
<tr>
<td>045009</td>
<td>E</td>
<td>The model type for this enclosure is not valid.</td>
<td>1124</td>
</tr>
<tr>
<td>045010</td>
<td>E</td>
<td>The power supply unit type is unknown to this product.</td>
<td>1124</td>
</tr>
<tr>
<td>045011</td>
<td>E</td>
<td>The power supply unit serial number is not valid.</td>
<td>1124</td>
</tr>
<tr>
<td>045012</td>
<td>W</td>
<td>The canister temperature is at the warning level.</td>
<td>1098</td>
</tr>
<tr>
<td>045013</td>
<td>W</td>
<td>The canister temperature is at the critical level.</td>
<td>1095</td>
</tr>
<tr>
<td>045014</td>
<td>E</td>
<td>The SAS cable was excluded because of a missing device.</td>
<td>1260</td>
</tr>
<tr>
<td>045015</td>
<td>E</td>
<td>A SAS cable was excluded because too many change events were caused.</td>
<td>1260</td>
</tr>
<tr>
<td>045016</td>
<td>E</td>
<td>A SAS cable was excluded.</td>
<td>1255</td>
</tr>
<tr>
<td>045017</td>
<td>E</td>
<td>A SAS cable is operating at a reduced speed.</td>
<td>1260</td>
</tr>
<tr>
<td>045018</td>
<td>E</td>
<td>A SAS cable was excluded because frames were dropped.</td>
<td>1260</td>
</tr>
<tr>
<td>045019</td>
<td>E</td>
<td>A SAS cable was excluded because the enclosure discovery timed out.</td>
<td>1260</td>
</tr>
<tr>
<td>045020</td>
<td>W</td>
<td>A SAS cable is not present.</td>
<td>1265</td>
</tr>
<tr>
<td>045021</td>
<td>E</td>
<td>A canister was removed from the system.</td>
<td>1036</td>
</tr>
<tr>
<td>045022</td>
<td>E</td>
<td>A canister has been in a degraded state for too long and cannot be recovered.</td>
<td>1034</td>
</tr>
<tr>
<td>045023</td>
<td>E</td>
<td>A canister is encountering communication problems.</td>
<td>1038</td>
</tr>
<tr>
<td>045024</td>
<td>E</td>
<td>The canister VPD is not valid.</td>
<td>1032</td>
</tr>
<tr>
<td>045025</td>
<td>E</td>
<td>The canister has experienced too many resets.</td>
<td>1032</td>
</tr>
<tr>
<td>045026</td>
<td>E</td>
<td>The drive slot is causing the network to be unstable.</td>
<td>1686</td>
</tr>
<tr>
<td>045027</td>
<td>E</td>
<td>The drive slot is not running at 6 Gbps</td>
<td>1686</td>
</tr>
<tr>
<td>045028</td>
<td>E</td>
<td>The drive slot is dropping frames.</td>
<td>1686</td>
</tr>
<tr>
<td>045029</td>
<td>E</td>
<td>The drive is visible through only one SAS port.</td>
<td>1686</td>
</tr>
<tr>
<td>045031</td>
<td>E</td>
<td>The drive power control is not functional.</td>
<td>1008</td>
</tr>
<tr>
<td>045033</td>
<td>E</td>
<td>The drive slot contains a device that is not responding to queries.</td>
<td>1685</td>
</tr>
<tr>
<td>045034</td>
<td>E</td>
<td>The managed enclosure is not visible from any node canisters.</td>
<td>1042</td>
</tr>
<tr>
<td>045035</td>
<td>E</td>
<td>The electronics in the enclosure has failed.</td>
<td>1694</td>
</tr>
<tr>
<td>045036</td>
<td>E</td>
<td>The electronics in the enclosure has experienced a critical failure.</td>
<td>1008</td>
</tr>
<tr>
<td>045037</td>
<td>E</td>
<td>The SAS network has too many errors.</td>
<td>1048</td>
</tr>
<tr>
<td>045038</td>
<td>E</td>
<td>The SAS network has too many errors.</td>
<td>1048</td>
</tr>
<tr>
<td>045040</td>
<td>W</td>
<td>The firmware update for the enclosure component has failed.</td>
<td>3015</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Condition</td>
<td>Error code</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>045041</td>
<td>W</td>
<td>More than one initiator port was detected on the same strand.</td>
<td>1005</td>
</tr>
<tr>
<td>045042</td>
<td>W</td>
<td>The order of the enclosures is different on each strand.</td>
<td>1005</td>
</tr>
<tr>
<td>045044</td>
<td>W</td>
<td>Multiple canisters are connected to a single canister port.</td>
<td>1005</td>
</tr>
<tr>
<td>045045</td>
<td>W</td>
<td>Canister 1 is connected to canister 2.</td>
<td>1005</td>
</tr>
<tr>
<td>045046</td>
<td>W</td>
<td>An enclosure is connected to more than one I/O group.</td>
<td>1005</td>
</tr>
<tr>
<td>045047</td>
<td>W</td>
<td>A managed enclosure is connected to the wrong I/O group.</td>
<td>1005</td>
</tr>
<tr>
<td>045048</td>
<td>W</td>
<td>An enclosure is connected to more than one chain.</td>
<td>1005</td>
</tr>
<tr>
<td>045049</td>
<td>W</td>
<td>Too many canisters are connected to a strand.</td>
<td>1005</td>
</tr>
<tr>
<td>045050</td>
<td>W</td>
<td>The canister is connected to the wrong port.</td>
<td>1005</td>
</tr>
<tr>
<td>045051</td>
<td>E</td>
<td>A SAS cable is excluded because of single port active drives.</td>
<td>1260</td>
</tr>
<tr>
<td>045052</td>
<td>W</td>
<td>More than one canister was detected at the same hop count.</td>
<td>1005</td>
</tr>
<tr>
<td>045053</td>
<td>E</td>
<td>The node location is not able to be detected.</td>
<td>1031</td>
</tr>
<tr>
<td>045054</td>
<td>E</td>
<td>An enclosure display cannot be updated.</td>
<td>1694</td>
</tr>
<tr>
<td>045055</td>
<td>E</td>
<td>There is an enclosure battery fault.</td>
<td>1118</td>
</tr>
<tr>
<td>045056</td>
<td>E</td>
<td>An enclosure battery is missing.</td>
<td>1112</td>
</tr>
<tr>
<td>045057</td>
<td>E</td>
<td>An enclosure battery is nearing end of life.</td>
<td>1114</td>
</tr>
<tr>
<td>045058</td>
<td>E</td>
<td>An enclosure battery is at end of life.</td>
<td>1113</td>
</tr>
<tr>
<td>045062</td>
<td>W</td>
<td>An enclosure battery conditioning is required but not possible.</td>
<td>1131</td>
</tr>
<tr>
<td>045063</td>
<td>E</td>
<td>There was an enclosure battery communications error.</td>
<td>1116</td>
</tr>
<tr>
<td>045064</td>
<td>W</td>
<td>A SAS port is active, but no enclosures can be detected.</td>
<td>1005</td>
</tr>
<tr>
<td>045065</td>
<td>E</td>
<td>There is a connectivity problem between a canister and an enclosure.</td>
<td>1036</td>
</tr>
<tr>
<td>045066</td>
<td>E</td>
<td>The FRU identity of the enclosure is not valid.</td>
<td>1008</td>
</tr>
<tr>
<td>045067</td>
<td>W</td>
<td>A new enclosure FRU was detected and needs to be configured.</td>
<td>1041</td>
</tr>
<tr>
<td>045068</td>
<td>E</td>
<td>The internal device on a node canister was excluded because of too many change events.</td>
<td>1034</td>
</tr>
<tr>
<td>045069</td>
<td>E</td>
<td>The internal connector on the node canister was excluded as the cause of single ported drives.</td>
<td>1034</td>
</tr>
<tr>
<td>045070</td>
<td>W</td>
<td>The canister temperature sensor cannot be read.</td>
<td>1034</td>
</tr>
<tr>
<td>045071</td>
<td>W</td>
<td>The enclosure contains both a node canister and an expansion canister.</td>
<td>1037</td>
</tr>
<tr>
<td>045072</td>
<td>E</td>
<td>The discovery failed to complete.</td>
<td>1048</td>
</tr>
<tr>
<td>045073</td>
<td>E</td>
<td>The VPD for the enclosure cannot be read.</td>
<td>1048</td>
</tr>
<tr>
<td>045080</td>
<td>E</td>
<td>There are too many self-initiated resets on the enclosure.</td>
<td>1048</td>
</tr>
<tr>
<td>045082</td>
<td>E</td>
<td>The slots are powered off.</td>
<td>1048</td>
</tr>
</tbody>
</table>
### Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>050001</td>
<td>W</td>
<td>The relationship is stopped because of a clustered system or complete I/O group failure, and the current state of the mapping could not be recovered.</td>
<td>1700</td>
</tr>
<tr>
<td>050002</td>
<td>W</td>
<td>A Metro Mirror or Global Mirror relationship or consistency group exists within a clustered system, but its partnership has been deleted.</td>
<td>3080</td>
</tr>
<tr>
<td>050010</td>
<td>W</td>
<td>A Global Mirror relationship has stopped because of a persistent I/O error.</td>
<td>1920</td>
</tr>
<tr>
<td>050011</td>
<td>W</td>
<td>A remote copy has stopped because of a persistent I/O error.</td>
<td>1915</td>
</tr>
<tr>
<td>050020</td>
<td>W</td>
<td>Remote copy has stopped.</td>
<td>1720</td>
</tr>
<tr>
<td>050030</td>
<td>W</td>
<td>There are too many cluster (system) partnerships. The number of partnerships has been reduced.</td>
<td>1710</td>
</tr>
<tr>
<td>050031</td>
<td>W</td>
<td>There are too many cluster (system) partnerships. The system has been excluded.</td>
<td>1710</td>
</tr>
<tr>
<td>050040</td>
<td>W</td>
<td>Background copy process for the Remote Copy was blocked.</td>
<td>1960</td>
</tr>
<tr>
<td>060001</td>
<td>W</td>
<td>The thin-provisioned volume copy is offline because there is insufficient space.</td>
<td>1865</td>
</tr>
<tr>
<td>060002</td>
<td>W</td>
<td>The thin-provisioned volume copy is offline because the metadata is corrupt.</td>
<td>1862</td>
</tr>
<tr>
<td>060003</td>
<td>W</td>
<td>The thin-provisioned volume copy is offline because the repair has failed.</td>
<td>1860</td>
</tr>
<tr>
<td>060004</td>
<td>W</td>
<td>The compressed volume copy is offline because there is insufficient space.</td>
<td>1865</td>
</tr>
<tr>
<td>060005</td>
<td>W</td>
<td>The compressed volume copy is offline because the metadata is corrupt.</td>
<td>1862</td>
</tr>
<tr>
<td>060006</td>
<td>W</td>
<td>The compressed volume copy is offline because the repair has failed.</td>
<td>1860</td>
</tr>
<tr>
<td>060007</td>
<td>W</td>
<td>The compressed volume copy has bad blocks.</td>
<td>1850</td>
</tr>
<tr>
<td>062001</td>
<td>W</td>
<td>Unable to mirror medium error during volume copy synchronization</td>
<td>1950</td>
</tr>
<tr>
<td>062002</td>
<td>W</td>
<td>The mirrored volume is offline because the data cannot be synchronized.</td>
<td>1870</td>
</tr>
<tr>
<td>062003</td>
<td>W</td>
<td>The repair process for the mirrored disk has stopped because there is a difference between the copies.</td>
<td>1600</td>
</tr>
<tr>
<td>070000</td>
<td>E</td>
<td>Unrecognized node error.</td>
<td>1083</td>
</tr>
<tr>
<td>070510</td>
<td>E</td>
<td>Detected memory size does not match the expected memory size.</td>
<td>1022</td>
</tr>
<tr>
<td>070517</td>
<td>E</td>
<td>The WWNN that is stored on the service controller and the WWNN that is stored on the drive do not match.</td>
<td>1192</td>
</tr>
<tr>
<td>070521</td>
<td>E</td>
<td>Unable to detect any Fibre Channel adapter.</td>
<td>1016</td>
</tr>
<tr>
<td>070522</td>
<td>E</td>
<td>The system board processor has failed.</td>
<td>1020</td>
</tr>
<tr>
<td>070523</td>
<td>W</td>
<td>The internal disk file system of the node is damaged.</td>
<td>1187</td>
</tr>
<tr>
<td>070524</td>
<td>E</td>
<td>Unable to update BIOS settings.</td>
<td>1027</td>
</tr>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Condition</td>
<td>Error code</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>070525</td>
<td>E</td>
<td>Unable to update the service processor firmware for the system board.</td>
<td>1020</td>
</tr>
<tr>
<td>070528</td>
<td>W</td>
<td>The ambient temperature is too high while the system is starting.</td>
<td>1182</td>
</tr>
<tr>
<td>070550</td>
<td>E</td>
<td>Cannot form cluster (system) due to lack of resources.</td>
<td>1192</td>
</tr>
<tr>
<td>070556</td>
<td>E</td>
<td>Duplicate WWNN detected on the SAN.</td>
<td>1192</td>
</tr>
<tr>
<td>070558</td>
<td>E</td>
<td>A node is unable to communicate with other nodes.</td>
<td>1192</td>
</tr>
<tr>
<td>070562</td>
<td>E</td>
<td>The node hardware does not meet minimum requirements.</td>
<td>1183</td>
</tr>
<tr>
<td>070564</td>
<td>E</td>
<td>Too many software failures.</td>
<td>1188</td>
</tr>
<tr>
<td>070574</td>
<td>E</td>
<td>The node software is damaged.</td>
<td>1187</td>
</tr>
<tr>
<td>070576</td>
<td>E</td>
<td>The cluster (system) data cannot be read.</td>
<td>1030</td>
</tr>
<tr>
<td>070578</td>
<td>E</td>
<td>The cluster (system) data was not saved when power was lost.</td>
<td>1194</td>
</tr>
<tr>
<td>070580</td>
<td>E</td>
<td>Unable to read the service controller ID.</td>
<td>1044</td>
</tr>
<tr>
<td>070690</td>
<td>W</td>
<td>Node held in service state.</td>
<td>1189</td>
</tr>
<tr>
<td>071820</td>
<td>W</td>
<td>Node canister has the incorrect model for the enclosure.</td>
<td>3020</td>
</tr>
<tr>
<td>071840</td>
<td>W</td>
<td>Detected hardware is not a valid configuration.</td>
<td>1198</td>
</tr>
<tr>
<td>071841</td>
<td>W</td>
<td>Detected hardware needs activation.</td>
<td>1199</td>
</tr>
<tr>
<td>072900</td>
<td>E</td>
<td>There was a PCIe link failure between canisters.</td>
<td>1006</td>
</tr>
<tr>
<td>072901</td>
<td>E</td>
<td>The PCIe link is degraded between canisters.</td>
<td>1052</td>
</tr>
<tr>
<td>072911</td>
<td>E</td>
<td>The PCIe link for the CPU is degraded.</td>
<td>1034</td>
</tr>
<tr>
<td>073003</td>
<td>E</td>
<td>The Fibre Channel ports are not operational.</td>
<td>1060</td>
</tr>
<tr>
<td>073005</td>
<td>E</td>
<td>Cluster (system) path failure.</td>
<td>1550</td>
</tr>
<tr>
<td>073006</td>
<td>W</td>
<td>The SAN is not correctly zoned. As a result, more than 512 ports on the SAN have logged into one Storwize V7000 port.</td>
<td>1800</td>
</tr>
<tr>
<td>073007</td>
<td>W</td>
<td>There are fewer Fibre Channel ports operational than are configured.</td>
<td>1061</td>
</tr>
<tr>
<td>073305</td>
<td>W</td>
<td>One or more Fibre Channel ports are running at a speed that is lower than the last saved speed.</td>
<td>1065</td>
</tr>
<tr>
<td>073310</td>
<td>E</td>
<td>A duplicate Fibre Channel frame has been detected, which indicates that there is an issue with the Fibre Channel fabric. Other Fibre Channel errors might also be generated.</td>
<td>1203</td>
</tr>
<tr>
<td>073500</td>
<td>W</td>
<td>Incorrect enclosure.</td>
<td>1021</td>
</tr>
<tr>
<td>073501</td>
<td>E</td>
<td>Incorrect canister position.</td>
<td>1192</td>
</tr>
<tr>
<td>073502</td>
<td>E</td>
<td>No enclosure identity; cannot get status from partner.</td>
<td>1192</td>
</tr>
<tr>
<td>073503</td>
<td>E</td>
<td>Incorrect enclosure type.</td>
<td>1192</td>
</tr>
<tr>
<td>073504</td>
<td>E</td>
<td>No enclosure identity and partner does match.</td>
<td>1192</td>
</tr>
<tr>
<td>073505</td>
<td>E</td>
<td>No enclosure identity and partner does not match.</td>
<td>1192</td>
</tr>
<tr>
<td>073506</td>
<td>E</td>
<td>No enclosure identity and no state on partner.</td>
<td>1192</td>
</tr>
</tbody>
</table>
Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>073507</td>
<td>E</td>
<td>No enclosure identity and no node state.</td>
<td>1192</td>
</tr>
<tr>
<td>073508</td>
<td>W</td>
<td>Cluster (system) identity is different on the enclosure and the node.</td>
<td>1023</td>
</tr>
<tr>
<td>073509</td>
<td>E</td>
<td>Cannot read enclosure identity.</td>
<td>1036</td>
</tr>
<tr>
<td>073510</td>
<td>E</td>
<td>Detected memory size does not match the expected memory size.</td>
<td>1032</td>
</tr>
<tr>
<td>073512</td>
<td>E</td>
<td>Enclosure VPD is inconsistent</td>
<td>1008</td>
</tr>
<tr>
<td>073522</td>
<td>E</td>
<td>The system board service processor has failed.</td>
<td>1034</td>
</tr>
<tr>
<td>073523</td>
<td>W</td>
<td>The internal disk file system of the node is damaged.</td>
<td>1187</td>
</tr>
<tr>
<td>073525</td>
<td>E</td>
<td>Unable to update the service processor firmware of the system board.</td>
<td>1034</td>
</tr>
<tr>
<td>073528</td>
<td>E</td>
<td>Ambient temperature is too high during system startup.</td>
<td>1098</td>
</tr>
<tr>
<td>073535</td>
<td>E</td>
<td>The internal PCIe switch of the node canister failed.</td>
<td>1034</td>
</tr>
<tr>
<td>073550</td>
<td>E</td>
<td>Cannot form cluster (system) due to lack of resources.</td>
<td>1192</td>
</tr>
<tr>
<td>073556</td>
<td>E</td>
<td>Duplicate WWNN detected on the SAN.</td>
<td>1133</td>
</tr>
<tr>
<td>073562</td>
<td>E</td>
<td>The node hardware does not meet the minimum requirements.</td>
<td>1034</td>
</tr>
<tr>
<td>073564</td>
<td>W</td>
<td>Too many software failures.</td>
<td>1188</td>
</tr>
<tr>
<td>073565</td>
<td>E</td>
<td>The internal drive of the node is failing.</td>
<td>1032</td>
</tr>
<tr>
<td>073573</td>
<td>E</td>
<td>The node software is inconsistent.</td>
<td>1187</td>
</tr>
<tr>
<td>073574</td>
<td>E</td>
<td>The cluster (system) data cannot be read.</td>
<td>1187</td>
</tr>
<tr>
<td>073578</td>
<td>E</td>
<td>The cluster (system) data was not saved when power was lost.</td>
<td>1194</td>
</tr>
<tr>
<td>073601</td>
<td>E</td>
<td>The canister battery is missing.</td>
<td>1153</td>
</tr>
<tr>
<td>073602</td>
<td>E</td>
<td>The canister battery has failed.</td>
<td>1154</td>
</tr>
<tr>
<td>073603</td>
<td>E</td>
<td>The canister battery’s temperature is too low.</td>
<td>1156</td>
</tr>
<tr>
<td>073604</td>
<td>E</td>
<td>The canister battery’s temperature is too high</td>
<td>1157</td>
</tr>
<tr>
<td>073605</td>
<td>E</td>
<td>The canister battery communications fault.</td>
<td>1158</td>
</tr>
<tr>
<td>073606</td>
<td>E</td>
<td>The canister battery has insufficient charge.</td>
<td>1184</td>
</tr>
<tr>
<td>073609</td>
<td>W</td>
<td>Node held in service state.</td>
<td>1189</td>
</tr>
<tr>
<td>073700</td>
<td>E</td>
<td>FC adapter missing.</td>
<td>1045</td>
</tr>
<tr>
<td>073701</td>
<td>E</td>
<td>FC adapter failed.</td>
<td>1046</td>
</tr>
<tr>
<td>073702</td>
<td>E</td>
<td>FC adapter PCI error.</td>
<td>1046</td>
</tr>
<tr>
<td>073703</td>
<td>E</td>
<td>FC adapter degraded.</td>
<td>1045</td>
</tr>
<tr>
<td>073704</td>
<td>W</td>
<td>Fewer Fibre Channel ports operational.</td>
<td>1061</td>
</tr>
<tr>
<td>073705</td>
<td>W</td>
<td>Fewer Fibre Channel IO ports operational.</td>
<td>1450</td>
</tr>
<tr>
<td>073710</td>
<td>E</td>
<td>SAS adapter missing.</td>
<td>1045</td>
</tr>
<tr>
<td>073711</td>
<td>E</td>
<td>SAS adapter failed.</td>
<td>1046</td>
</tr>
<tr>
<td>073712</td>
<td>E</td>
<td>SAS adapter PCI error.</td>
<td>1046</td>
</tr>
<tr>
<td>073713</td>
<td>E</td>
<td>SAS adapter degraded.</td>
<td>1046</td>
</tr>
<tr>
<td>073720</td>
<td>E</td>
<td>Ethernet adapter missing.</td>
<td>1045</td>
</tr>
</tbody>
</table>
Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>073721</td>
<td>E</td>
<td>Ethernet adapter failed.</td>
<td>1046</td>
</tr>
<tr>
<td>073722</td>
<td>E</td>
<td>Ethernet adapter PCI error.</td>
<td>1046</td>
</tr>
<tr>
<td>073723</td>
<td>E</td>
<td>Ethernet adapter degraded.</td>
<td>1046</td>
</tr>
<tr>
<td>073724</td>
<td>W</td>
<td>Fewer Ethernet ports operational.</td>
<td>1401</td>
</tr>
<tr>
<td>073730</td>
<td>E</td>
<td>Bus adapter missing.</td>
<td>1032</td>
</tr>
<tr>
<td>073731</td>
<td>E</td>
<td>Bus adapter failed.</td>
<td>1032</td>
</tr>
<tr>
<td>073732</td>
<td>E</td>
<td>Bus adapter PCI error.</td>
<td>1032</td>
</tr>
<tr>
<td>073733</td>
<td>E</td>
<td>Bus adapter degraded.</td>
<td>1032</td>
</tr>
<tr>
<td>073734</td>
<td>W</td>
<td>Inter-canister PCIe link failure.</td>
<td>1006</td>
</tr>
<tr>
<td>073768</td>
<td>W</td>
<td>Ambient temperature warning.</td>
<td>1094</td>
</tr>
<tr>
<td>073769</td>
<td>W</td>
<td>CPU temperature warning.</td>
<td>1093</td>
</tr>
<tr>
<td>073840</td>
<td>E</td>
<td>Detected hardware is not a valid configuration.</td>
<td>1198</td>
</tr>
<tr>
<td>073841</td>
<td>E</td>
<td>Detected hardware needs activation.</td>
<td>1199</td>
</tr>
<tr>
<td>073860</td>
<td>W</td>
<td>Fabric too large.</td>
<td>1800</td>
</tr>
<tr>
<td>074001</td>
<td>W</td>
<td>Unable to determine the vital product data (VPD) for an FRU.</td>
<td>2040</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is probably because a new FRU has been installed and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the software does not recognize that FRU.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The cluster (system) continues to operate; however, you</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>must upgrade the software to fix this warning.</td>
<td></td>
</tr>
<tr>
<td>074002</td>
<td>E</td>
<td>The node warm started after a software error.</td>
<td>2030</td>
</tr>
<tr>
<td>074003</td>
<td>W</td>
<td>A connection to a configured remote system has been lost</td>
<td>1715</td>
</tr>
<tr>
<td></td>
<td></td>
<td>because of a connectivity problem.</td>
<td></td>
</tr>
<tr>
<td>074004</td>
<td>W</td>
<td>A connection to a configured remote system has been lost</td>
<td>1716</td>
</tr>
<tr>
<td></td>
<td></td>
<td>because of too many minor errors.</td>
<td></td>
</tr>
<tr>
<td>076001</td>
<td>E</td>
<td>The internal disk for a node has failed.</td>
<td>1030</td>
</tr>
<tr>
<td>076002</td>
<td>E</td>
<td>The hard disk is full and cannot capture any more</td>
<td>2030</td>
</tr>
<tr>
<td></td>
<td></td>
<td>output.</td>
<td></td>
</tr>
<tr>
<td>076401</td>
<td>E</td>
<td>One of the two power supply units in the node has</td>
<td>1096</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failed.</td>
<td></td>
</tr>
<tr>
<td>076402</td>
<td>E</td>
<td>One of the two power supply units in the node cannot</td>
<td>1096</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be detected.</td>
<td></td>
</tr>
<tr>
<td>076403</td>
<td>E</td>
<td>One of the two power supply units in the node is</td>
<td>1097</td>
</tr>
<tr>
<td></td>
<td></td>
<td>without power.</td>
<td></td>
</tr>
<tr>
<td>076502</td>
<td>E</td>
<td>Degraded PCIe lanes on a high-speed SAS adapter.</td>
<td>1121</td>
</tr>
<tr>
<td>076503</td>
<td>E</td>
<td>A PCI bus error occurred on a high-speed SAS adapter.</td>
<td>1121</td>
</tr>
<tr>
<td>076504</td>
<td>E</td>
<td>A high-speed SAS adapter requires a PCI bus reset.</td>
<td>1122</td>
</tr>
<tr>
<td>076505</td>
<td>E</td>
<td>Vital product data (VPD) is corrupt on high-speed SAS</td>
<td>1121</td>
</tr>
<tr>
<td></td>
<td></td>
<td>adapter.</td>
<td></td>
</tr>
<tr>
<td>076511</td>
<td>E</td>
<td>A high-speed SAS controller is missing.</td>
<td>1032</td>
</tr>
<tr>
<td>076512</td>
<td>E</td>
<td>Degraded PCIe lanes on a high-speed SAS adapter.</td>
<td>1032</td>
</tr>
<tr>
<td>076513</td>
<td>E</td>
<td>A PCI bus error occurred on a high-speed SAS adapter.</td>
<td>1032</td>
</tr>
<tr>
<td>076514</td>
<td>E</td>
<td>A high-speed SAS adapter requires a PCI bus reset.</td>
<td>1034</td>
</tr>
</tbody>
</table>
Table 26. Error event IDs and error codes (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Condition</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>079500</td>
<td>W</td>
<td>The limit on the number of cluster (system) secure shell (SSH) sessions has been reached.</td>
<td>2500</td>
</tr>
<tr>
<td>079501</td>
<td>W</td>
<td>Unable to access the Network Time Protocol (NTP) network time server.</td>
<td>2700</td>
</tr>
<tr>
<td>081002</td>
<td>E</td>
<td>An Ethernet port failure has occurred.</td>
<td>1401</td>
</tr>
<tr>
<td>082001</td>
<td>E</td>
<td>A server error has occurred.</td>
<td>2100</td>
</tr>
<tr>
<td>084000</td>
<td>W</td>
<td>An array MDisk has deconfigured members and has lost redundancy.</td>
<td>1689</td>
</tr>
<tr>
<td>084100</td>
<td>W</td>
<td>An array MDisk is corrupt because of lost metadata.</td>
<td>1240</td>
</tr>
<tr>
<td>084200</td>
<td>W</td>
<td>An array MDisk has taken a spare member that is not an exact match to the array goals.</td>
<td>1692</td>
</tr>
<tr>
<td>084201</td>
<td>W</td>
<td>An array has members that are located in a different I/O group.</td>
<td>1688</td>
</tr>
<tr>
<td>084300</td>
<td>W</td>
<td>An array MDisk is no longer protected by an appropriate number of suitable spares.</td>
<td>1690</td>
</tr>
<tr>
<td>084500</td>
<td>W</td>
<td>An array MDisk is offline. The metadata for the inflight writes is on a missing node.</td>
<td>1243</td>
</tr>
<tr>
<td>084600</td>
<td>W</td>
<td>An array MDisk is offline. Metadata on the missing node contains needed state information.</td>
<td>1243</td>
</tr>
</tbody>
</table>

Node error code overview

Node error codes describe failure that relate to a specific node canister.

Because node errors are specific to a node, for example, memory has failed, the errors are only reported on that node. However, some of the conditions that the node detects relate to the shared components of the enclosure. In these cases both node canisters in the enclosure report the error.

There are two types of node errors: critical node errors and noncritical node errors.

Critical errors

A critical error means that the node is not able to participate in a clustered system until the issue that is preventing it from joining a clustered system is resolved. This error occurs because part of the hardware has failed or the system detects that the code is corrupt. If it is possible to communicate with the canister with a node error, an alert that describes the error is logged in the event log. If the system cannot communicate with the node canister, a Node missing alert is reported. If a node has a critical node error, it is in service state, and the fault LED on the node is on. The exception is when the node cannot connect to enough resources to form a clustered system. It shows a critical node error but is in the starting state. The range of errors that are reserved for critical errors are 500 - 699.

Some critical errors might be accompanied by error codes 1021, 1036, 1188, and 1189.

Noncritical errors
A noncritical error code is logged when there is a hardware or code failure that is related to just one specific node. These errors do not stop the node from entering active state and joining a clustered system. If the node is part of a clustered system, there is also an alert that describes the error condition. The node error is shown to make it clear which of the node canisters the alert refers to. The range of errors that are reserved for noncritical errors are 800 - 899.

Clustered-system code overview

Recovery codes for clustered systems indicate that a critical software error has occurred that might corrupt your system. Each error-code topic includes an error code number, a description, action, and possible field-replaceable units (FRUs).

Error codes for recovering a clustered system

You must perform software problem analysis before you can perform further operations to avoid the possibility of corrupting your configuration.

Error code range

This topic shows the number range for each message classification.

Table 27 lists the number range for each message classification.

<table>
<thead>
<tr>
<th>Message classification</th>
<th>Range</th>
</tr>
</thead>
</table>
| Node errors            | Critical node errors 500-699
|                        | Some critical errors might be accompanied by error codes 1021, 1036, 1188, and 1189. |
|                        | Noncritical node errors 700-899 |
| Error codes when recovering a clustered system | 920, 990 |
501 Incorrect slot

Explanation: The node canister has saved cluster information, which indicates that the canister is now located in the expected enclosure, but in a different slot from where it was previously used. Using the node canister in this state might mean that hosts are not able to connect correctly.

User response: Follow troubleshooting procedures to relocate the node canister to the correct location.

1. Follow the procedure: Getting node canister and system information and review the saved location information of the node canister in the enclosure (the partner canister). If the node canister has been inadvertently swapped, the other node canister will have the same error. See “Procedure: Getting node canister and system information using the service assistant” on page 53.

2. If the canisters have been swapped, use the “Replacing a node canister” on page 85 procedure to swap the canisters. The system should start.

3. If the partner canister is in candidate state, use the hardware remove and replace canister procedure to swap the canisters. The system should start.

4. If the partner canister is in active state, it is running the cluster on this enclosure and has replaced the original use of this canister. You must follow the procedure to remove cluster data from this node canister. The node canister will then become active in the cluster in its current slot. See “Procedure: Removing system data from a node canister” on page 59.

5. If the partner canister is in service state, review its node error to determine the correct action. Generally, you will fix the errors reported on the partner node in priority order, and review the situation again after each change. If you have to replace the partner canister with a new one you should move this canister back to the correct location at the same time.

Possible Cause—FRUs or other:

• None

502 No enclosure identity exists and a status from the partner node could not be obtained.

Explanation: The enclosure has been replaced and communication with the other node canister (partner node) in the enclosure is not possible. The partner node could be missing, powered off, unable to boot, or an internode communication failure may exist.

User response: Follow troubleshooting procedures to configure the enclosure:

1. Follow the procedures to resolve a problem to get the partner node started. An error will still exist because the enclosure has no identity. If the error has changed, follow the service procedure for that error.

2. If the partner has started and is showing a location error (probably this one), then the PCI link is probably broken. Since the enclosure midplane was recently replaced, this is likely the problem. Obtain a replacement enclosure midplane, and replace it. See “Replacing a control enclosure chassis” on page 107.

3. If this action does not resolve the issue, contact IBM Support Center. They will work with you to ensure that the system state data is not lost while resolving the problem. Also see Chapter 6, “Resolving a problem,” on page 43.

Possible Cause—FRUs or other:

• None

504 No enclosure identity and partner node matches.

Explanation: The enclosure vital product data indicates that the enclosure midplane has been replaced. This node canister and the other node canister in the enclosure were previously operating in the same enclosure midplane.

User response: Follow troubleshooting procedures to configure the enclosure.

1. This is an expected situation during the hardware remove and replace procedure for a control enclosure midplane. Continue following the remove and replace procedure and configure the new enclosure.

Possible Cause—FRUs or other:

• None

505 No enclosure identity and partner has system data that does not match.

Explanation: The enclosure vital product data indicates that the enclosure midplane has been replaced. This node canister and the other node canister in the enclosure do not come from the same original enclosure.

User response: Follow troubleshooting procedures to relocate nodes to the correct location.

1. Follow the procedure: Getting node canister and system information and review the node canister’s saved location information and the status of the other node canister in the enclosure (the partner canister). Determine if the enclosure is part of an active system with volumes that contain required
Possible Cause—FRUs or other:

• None

### 506 No enclosure identity and no node state on partner

**Explanation:** The enclosure vital product data indicates that the enclosure midplane has been replaced. There is no cluster state information on the other node canister in the enclosure (the partner canister), so both node canisters from the original enclosure have not been moved to this one.

**User response:** Follow troubleshooting procedures to relocate nodes to the correct location:

1. Follow the procedure: Getting node canister and system information and review the saved location information of the node canister and determine why the second node canister from the original enclosure was not moved into this enclosure. See “Procedure: Getting node canister and system information using the service assistant” on page 53.

2. If you are sure that this node canister came from the enclosure that is being replaced, and the original partner canister is available, use the “Replacing a node canister” on page 53 procedure to install the second node canister in this enclosure. Restart the node canister. The two node canisters should show node error 504, and the actions for that error should be followed.

### 507 No enclosure identity and no node state

**Explanation:** The node canister has been placed in a replacement enclosure midplane. The node canister is also a replacement or has had all cluster state removed from it.

**User response:** Follow troubleshooting procedures to relocate the nodes to the correct location:

1. Check the status of the other node in the enclosure. It should show node error 506. Unless it also shows error 507, check the errors on the other node and follow the corresponding procedures to resolve the errors.

2. If the other node in the enclosure is also reporting 507, the enclosure and both node canisters have no state information. You should contact IBM technical support. They will assist you in setting the enclosure vital product data and running cluster recovery.

**Possible Cause—FRUs or other:**

• None

### 508 Cluster identifier is different between enclosure and node

**Explanation:** The node canister location information shows it is in the correct enclosure, however the enclosure has had a new cluster created on it since the node was last shut down. Therefore, the cluster state data stored on the node is not valid.

**User response:** Follow troubleshooting procedures to correctly relocate the nodes:

1. Check whether a new cluster has been created on this enclosure while this canister was not operating or whether the node canister was recently installed in the enclosure.

2. Follow the procedure: Get node canister and system information using the service assistant, and check the partner node canister to see if it is also reporting node error 508; if it is, check that the saved system information on this and the partner node match. See “Procedure: Getting node canister and system information using the service assistant” on page 53.
3. If this node canister is the one to be used in this enclosure, follow the Procedure: Removing system data from a node canister on page 59 to remove cluster data from the node canister. It will then join the cluster.

4. If this is not the node canister that you intended to use, follow the Replacing a node canister procedure to replace the node canister with the one intended for use.

Possible Cause—FRUs or other:
- Service procedure error (90%)
- Enclosure midplane (10%)

509 The enclosure identity cannot be read.

Explanation: The canister was unable to read vital product data (VPD) from the enclosure. The canister requires this data to be able to initialize correctly.

User response: Follow troubleshooting procedures to fix the hardware:
1. Check errors reported on the other node canister in this enclosure (the partner canister).
2. If it is reporting the same error follow the hardware remove and replace procedure to replace the enclosure midplane.
3. If the partner canister is not reporting this error, follow the hardware remove and replace procedure to replace this canister.

Note: If a newly installed system has this error on both node canisters, the data that needs to be written to the enclosure will not be available on the canisters, you should contact IBM support for the WWNNs to use.

Possible Cause—FRUs or other:
- Node canister (50%)
- Enclosure midplane (50%)

510 The detected memory size does not match the expected memory size.

Explanation:
The amount of memory detected in the node canister is less than the amount required for the canister to operate as an active member of a system. The error code data shows the detected memory, in MB, followed by the minimum required memory, in MB, there is then a series of values indicating the amount of memory, in GB, detected in each memory slot.

Data:
- Detected memory on MB
- Minimum required memory in MB
- Memory in slot 1 in GB
- Memory in slot 2 in GB
- ... etc.

User response: Follow troubleshooting procedures to fix the hardware:
1. Use the hardware remove and replace node canister procedure to install a new node canister.

Possible Cause—FRUs or other:
- Node canister (100%)

522 The system board service processor has failed.

Explanation: The service processor (PSOC) in the canister has failed or is not communicating.

User response:
1. Reseat the node canister.
2. If the error persists, use the remove and replace procedures to replace the node canister.

Possible Cause—FRUs or other:
- Node canister

523 The internal disk file system is damaged.

Explanation: The node startup procedures have found problems with the file system on the internal disk of the node.

User response: Follow troubleshooting procedures to reload the software.
1. Follow the procedures to rescue the software of a node from another node.
2. If the rescue node does not succeed, use the hardware remove and replace procedures for the node canister.

Possible Cause—FRUs or other:
- Node canister (100%)

525 Unable to update system board service processor firmware.

Explanation: The node startup procedures have been unable to update the firmware configuration of the node canister.

User response: Follow troubleshooting procedures to fix the hardware:
1. Follow the hardware remove and replace procedures for the node canister.

Possible Cause—FRUs or other:
- Node canister (100%)
Ambient temperature is too high during system startup.

**Explanation:** The ambient temperature in the enclosure, read during the node canister startup procedures, is too high for the node canister to continue. The startup procedure will continue when the temperature is within range.

**User response:** Reduce the temperature around the system.

1. Resolve the issue with the ambient temperature, by checking and correcting:
   a. Room temperature and air conditioning
   b. Ventilation around the rack
   c. Airflow within the rack

**Possible Cause—FRUs or other:**
- Environment issue (100%)

**Canister internal PCIe switch failed**

**Explanation:** The PCI Express switch has failed or cannot be detected. In this situation, the only connectivity to the node canister is through the Ethernet ports.

**User response:** Follow troubleshooting procedures to fix the hardware:

1. Follow the procedure for reseating a node canister.
   - See “Procedure: Reseating a node canister” on page 65

2. If reseating the canister does not resolve the situation, follow the “Replacing a node canister” on page 85 procedure to replace the canister.

**Possible Cause—FRUs or other:**
- Node canister (100%)

**Multiple, undetermined, hardware errors**

**Explanation:** Multiple hardware failures have been reported on the data paths within the node canister, and the threshold of the number of acceptable errors within a given time frame has been reached. It has not been possible to isolate the errors to a single component.

After this node error has been raised, all ports on the node will be deactivated. The reason for this is that the node canister is considered unstable, and has the potential to corrupt data.

**User response:**
1. Follow the procedure for collecting information for support, and contact your support organization.
2. A software [code] upgrade may resolve the issue.
3. Replace the node canister.

**A cluster cannot be formed because of a lack of cluster resources.**

**Explanation:** The node canister cannot become active in a cluster because it is unable to connect to enough cluster resources. The cluster resources are the node canisters in the system and the active quorum disk or drive. The node needs to be able to connect to a majority of the resources before that group will form an online cluster. This prevents the cluster splitting into two or more active parts, with both parts independently performing I/O.

The error data lists the missing resources. This will include a list of node canisters and optionally a drive that is operating as the quorum drive or a LUN on an external storage system that is operating as the quorum disk.

If a drive in one of the system enclosures is the missing quorum disk, it is listed as enclosures:slot[part identification] where enclosures:slot is the location of the drive when the node shut down, enclosure is the seven digit product serial number of the enclosure, slot is a number between 1 and 24. The part identification is the 22 character string starting “11S” found on a label on a drive. The part identification cannot be seen until the drive is removed from the enclosure.

If a LUN on an external storage system is the missing quorum disk, it is listed as WWWW/WWWW/WWWW/WWWW/WWWW/LL, where WWWW/WWWW/WWWW/WWWW/WWWW is a worldwide port name (WWPN) on the storage system that contains the missing quorum disk and LL is the Logical Unit Number (LUN).

**User response:** Follow troubleshooting procedures to correct connectivity issues between the cluster nodes and the quorum devices.

1. Check for any node errors that indicate issues with bus or Fibre Channel connectivity. Resolve any issues.
2. Check the status of other node canisters in the system, resolve any faults on them.
3. Check all enclosures in the system are powered on and that the SAS cabling between the enclosures has not been disturbed. If any wiring changes have been made check all cables are securely connected and that the cabling rules have been followed.
4. If a quorum drive in a system enclosure is shown as missing, find the drive and check that it is working. The drive may have been moved from the location shown, in that case find the drive and ensure it is installed and working. If the drive is not located in the control enclosure, try moving it to the control enclosure, because a problem in SAS connectivity may be the issue.

**Note:** If you are able to reestablish the systems operation you will be able to use the extra
556  A duplicate WWNN has been detected.

Explanation:
The node canister has detected another device that has the same World Wide Node Name (WWNN) on the Fibre Channel network. A WWNN is 16 hexadecimal digits long. For a Storwize V7000, the first 11 digits are always 50050768020. The last 5 digits of the WWNN are given in the additional data of the error. The Fibre Channel ports of the node canister are disabled to prevent disruption of the Fibre Channel network. One or both node canisters with the same WWNN can show the error. Because of the way WWNNs are allocated, a device with a duplicate WWNN is normally another Storwize V7000 node canister.

User response:
1. Find the Storwize V7000 node canister with the sameWWNN as the node canister reporting the error. The WWNN for a Storwize V7000 node canister can be found from the node Vital Product Data (VPD) or from the node canister details shown by the service assistant. The node with the duplicate WWNN need not be part of the same cluster as the node reporting the error; it could be remote from the node reporting the error on a part of the fabric connected through an inter-switch link. The two node canisters within a control enclosure must have different WWNNs. The WWNN of the node canister is stored within the enclosure chassis, so the duplication is most likely caused by the replacement of a control enclosure chassis.
2. If a Storwize V7000 node canister with a duplicate WWNN is found, determine whether it, or the node reporting the error, has the incorrect WWNN. Generally, it is the node canister that has had its enclosure chassis recently replaced or had its WWNN changed incorrectly. Also, consider how the SAN is zoned when making your decision.
3. Determine the correct WWNN for the node with the incorrect WWNN. If the enclosure chassis has been replaced as part of a service action, the WWNN for the node canister should have been written down. If the correct WWNN cannot be determined contact your support center for assistance.
4. Use the service assistant to modify the incorrect WWNN. If it is the node showing the error that should be modified, this can safely be done immediately. If it is an active node that should be modified, use caution because the node will restart when the WWNN is changed. If this node is the only operational node in an enclosure, access to the volumes that it is managing will be lost. You should ensure that the host systems are in the correct state before you change the WWNN.
5. If the node showing the error had the correct WWNN, it can be restarted, using the service assistant, after the node with the duplicate WWNN is updated.
6. If you are unable to find a Storwize V7000 node canister with the same WWNN as the node canister showing the error, use the SAN monitoring tools to determine whether there is another device on the SAN with the same WWNN. This device should not be using a WWNN assigned to a Storwize V7000, so you should follow the service procedures for the device to change its WWNN. Once the duplicate has been removed, restart the node canister.

562  The nodes hardware configuration does not meet the minimum requirements

Explanation: The node hardware is not at the minimum specification for the node to become active in a cluster. This may be because of hardware failure, but is also possible after a service action has used an incorrect replacement part.

User response:
Follow troubleshooting procedures to fix the hardware:
1. It is not possible to service parts within the node canister. Reseat the existing node canister to see whether the problem fixes. If it does not, use the hardware node canister remove and replace procedures to change the node canister.

564  Too many machine code crashes have occurred.

Explanation: The node has been determined to be unstable because of multiple resets. The cause of the resets can be that the system encountered an unexpected state or has executed instructions that were...
not valid. The node has entered the service state so that diagnostic data can be recovered.

The node error does not persist across restarts of the node machine code.

**User response:** Follow troubleshooting procedures to reload the machine code:
1. Get a support package (snap), including dumps, from the node, using the management GUI or the service assistant.
2. If more than one node is reporting this error, contact IBM technical support for assistance. The support package from each node will be required.
3. Check the support site to see whether the issue is known and whether a machine code upgrade exists to resolve the issue. Update the cluster machine code if a resolution is available. Use the manual upgrade process on the node that reported the error first.
4. If the problem remains unresolved, contact IBM technical support and send them the support package.

Possible Cause—FRUs or other:
- None

---

**565 The internal drive of the node is failing.**

**Explanation:** The internal drive within the node is reporting too many errors. It is no longer safe to rely on the integrity of the drive. Replacement is recommended.

**User response:** Follow troubleshooting procedures to fix the hardware:
1. The drive of the node canister cannot be replaced individually. Follow the hardware remove and replace instructions to change the node canister.

Possible Cause—FRUs or other:
- None

---

**574 The node machine code is damaged.**

**Explanation:** A checksum failure has indicated that the node machine code is damaged and needs to be reinstalled.

**User response:**
1. If the other nodes are operational, run node rescue; otherwise, install new machine code using the service assistant. Node rescue failures, as well as the repeated return of this node error after reinstallation, are symptomatic of a hardware fault with the node.

Possible Cause—FRUs or other:
- None

---

**576 The cluster state and configuration data cannot be read.**

**Explanation:** The node has been unable to read the saved cluster state and configuration data from its internal drive because of a read or medium error.

**User response:** Follow troubleshooting procedures to fix the hardware:
1. The drive of the node canister cannot be replaced individually. Follow the hardware remove and replace instructions to change the node canister.

Possible Cause—FRUs or other:
- None

---

**578 The state data was not saved following a power loss.**

**Explanation:** On startup, the node was unable to read its state data. When this happens, it expects to be automatically added back into a cluster. However, if it has not joined a cluster in 60 sec, it raises this node error. This is a critical node error, and user action is required before the node can become a candidate to join a cluster.

**User response:** Follow troubleshooting procedures to fix connectivity issues between the cluster nodes and the quorum devices.
1. Manual intervention is required once the node reports this error.
2. Attempt to reestablish the cluster using other nodes. This may involve fixing hardware issues on other nodes or fixing connectivity issues between nodes.
3. If you are able to reestablish the cluster, remove the cluster data from the node showing 578 so it goes to candidate state, it will then be automatically added back to the cluster.
   a. To remove the cluster data from the node, either go to the service assistant, select the radio button for the node with a 578, click **Manage System**, then choose **Remove System Data.**
If the node does not automatically add back to the cluster, note the name and I/O group of the node, then delete the node from the cluster configuration (if this has not already happened) and then add the node back to the cluster using the same name and I/O group.

4. If all nodes have either node error 578 or 550, follow the cluster recovery procedures.

5. Attempt to determine what caused the nodes to shut down.

Possible Cause—FRUs or other:
- None

---

**650 The canister battery is not supported**

**Explanation:** The canister battery shows product data that indicates it cannot be used with the code version of the canister.

**User response:** This is resolved by either obtaining a battery which is supported by the system's code level, or the canister's code level is updated to a level which supports the battery.

1. Remove the canister and its lid and check the FRU part number of the new battery matches that of the replaced battery. Obtain the correct FRU part if it does not.
2. If the canister has just been replaced, check the code level of the partner node canister and use the service assistant to upgrade this canister's code level to the same level.

Possible cause—FRUs or other cause
- canister battery

---

**651 The canister battery is missing**

**Explanation:** The canister battery cannot be detected.

**User response:**
1. Use the remove and replace procedures to remove the node canister and its lid.
2. Use the remove and replace procedures to install a battery.
3. If there is a battery present ensure it is fully inserted. Replace the canister.
4. If this error persists, use the remove and replace procedures to replace the battery.

Possible cause—FRUs or other cause
- canister battery

---

**652 The canister battery has failed**

**Explanation:** The canister battery has failed. The battery may be showing an error state, it may have reached the end of life, or it may have failed to charge.

**Data**
Number indicators with failure reasons
- 1—battery reports a failure
- 2—end of life
- 3—failure to charge

**User response:**
1. Use the remove and replace procedures to replace the battery.

Possible cause—FRUs or other cause
- canister battery

---

**653 The canister battery's temperature is too low**

**Explanation:** The canister battery’s temperature is below its minimum operating temperature.

**User response:**
- Wait for the battery to warm up, the error will clear when its minimum working temperature is reached.
- If the error persists for more than an hour when the ambient temperature is normal, use the remove and replace procedures to replace the battery.

Possible cause—FRUs or other cause
- canister battery

---

**654 The canister battery's temperature is too high**

**Explanation:** The canister battery’s temperature is above its safe operating temperature.

**User response:**
- If necessary, reduce the ambient temperature.
- Wait for the battery to cool down, the error will clear when normal working temperature is reached. Keep checking the reported error as the system may determine the battery has failed.
- If the node error persists for more than two hours after the ambient temperature returns to the normal operating range, use the remove and replace procedures to replace the battery.

Possible cause—FRUs or other cause
- canister battery
655  The canister battery communications fault

Explanation: The canister cannot communicate with the battery.

User response:
• Use the remove and replace procedures to replace the battery.
• If the node error persists, use the remove and replace procedures to replace the node canister.

Possible cause—FRUs or other cause
• canister battery
• node canister

656  The canister battery has insufficient charge

Explanation: The canister battery has insufficient charge to save the canister’s state and cache data to the internal drive if power were to fail.

User response:
• Wait for the battery to charge, the battery does not need to be fully charged for the error to automatically clear.

Possible cause—FRUs or other cause
• none

671  The available battery charge is not enough to allow the node canister to start. Two batteries are charging.

Explanation: The battery charge within the enclosure is not sufficient for the node to safely become active in a cluster. The node will not start until sufficient charge exists to store the state and configuration data held in the node canister memory if power were to fail. Two batteries are within the enclosure, one in each of the power supplies. Neither of the batteries indicate an error—both are charging.

The node will start automatically when sufficient charge is available. The batteries do not have to be fully charged before the nodes can become active.

Both nodes within the enclosure share the battery charge, so both node canisters report this error.

The service assistant shows the estimated start time, and the battery status, in the node canister hardware details.

Possible Cause-FRUs or other:
• None

672  The available battery charge is not enough to allow the node canister to start. One battery is charging.

Explanation: The battery charge within the enclosure is not sufficient for the node to safely become active in a cluster. The node will not start until sufficient charge exists to store the state and configuration data held in the node canister memory if power were to fail. Two batteries are within the enclosure, one in each of the power supplies. Only one of the batteries is charging, so the time to reach sufficient charge will be extended.

The node will start automatically when sufficient charge is available. The batteries do not have to be fully charged before the nodes can become active.

Both nodes within the enclosure share the battery charge, so both node canisters report this error.

The service assistant shows the estimated start time, and the battery status, in the node canister hardware details.

Possible Cause-FRUs or other:
• Battery (33%)
• Control power supply (33%)
• Power cord (33%)

673  The available battery charge is not enough to allow the node canister to start. No batteries are charging.

Explanation: A node cannot be in active state if it does not have sufficient battery power to store configuration and cache data from memory to internal disk after a power failure. The system has determined that both batteries have failed or are missing. The problem with the batteries must be resolved to allow the system to start.

User response: Follow troubleshooting procedures to fix hardware:
1. Resolve problems in both batteries by following the procedure to determine status using the LEDs.
2. If the LEDs do not show a fault on the power supplies or batteries, power off both power supplies in the enclosure and remove the power cords. Wait 20 seconds, then replace the power cords and restore power to both power supplies. If both node canisters continue to report this error replace the enclosure chassis.
Possible Cause—FRUs or other:
- Battery (33%)
- Power supply (33%)
- Power cord (33%)
- Enclosure chassis (1%)

**690** The node is held in the service state.

**Explanation:** The node is in service state and has been instructed to remain in service state. While in service state, the node will not run as part of a cluster. A node must not be in service state for longer than necessary while the cluster is online because a loss of redundancy will result. A node can be set to remain in service state either because of a service assistant user action or because the node was deleted from the cluster.

**User response:** When it is no longer necessary to hold the node in the service state, exit the service state to allow the node to run:

1. Use the service assistant action to release the service state.

Possible Cause—FRUs or other:
- none

**700** The Fibre Channel adapter that was previously present has not been detected.

**Explanation:** A Fibre Channel adapter that was previously present has not been detected. For Storwize V7000, the adapter is located on the node canister system board.

This node error does not, in itself, stop the node canister becoming active in the system; however, the Fibre Channel network might be being used to communicate between the node canisters in a clustered system. It is possible that this node error indicates why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
- A number indicating the adapter location. Location 0 indicates the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause—FRUs or other cause:
- Node canister

**702** A Fibre Channel adapter has a PCI error.

**Explanation:** A Fibre Channel adapter has a PCI error. The adapter is located on the node canister system board.

This node error does not, in itself, stop the node canister becoming active in the system. However, the Fibre Channel network might be being used to communicate between the node canisters in a clustered system. Therefore, it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
- A number indicating the adapter location. Location 0 indicates the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

There are a number of possibilities.

a. If you have deliberately removed the adapter (possibly replacing it with a different adapter type), you will need to follow the management GUI recommended actions to mark the hardware change as intentional.

b. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Use the procedures to restart (physically remove and reseat) a node canister.
3. As the adapter is located on the system board, replace the node canister by using the remove and replace procedures.

Possible Cause-FRUs or other cause:
• Node canister

**A Fibre Channel adapter is degraded.**

**Explanation:** A Fibre Channel adapter is degraded. The adapter is located on the node canister system board.

This node error does not, in itself, stop the node canister becoming active in the system. However, the Fibre Channel network might be being used to communicate between the node canisters in a clustered system. Therefore, it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
• A number indicating the adapter location. Location 0 indicates the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. If the port has been intentionally disconnected, use the management GUI recommended action for the service error code and acknowledge the intended change.
3. Check that the Fibre Channel cable is connected at both ends and is not damaged. If necessary, replace the cable.
4. Check the switch port or other device that the cable is connected to is powered and enabled in a compatible mode. Rectify any issue. The device service interface might indicate the issue.
5. Use the remove and replace procedures to replace the SFP transceiver in the Storwize V7000 and the SFP transceiver in the connected switch or device.
6. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
• Fibre Channel cable
• SFP transceiver
• Node canister

**Fewer Fibre Channel I/O ports operational.**

**Explanation:** One or more Fibre Channel I/O ports that have previously been active are now inactive. This situation has continued for one minute.

A Fibre Channel I/O port might be established on either a Fibre Channel platform port or an Ethernet platform port using FCoE. This error is expected if the associated Fibre Channel or Ethernet port is not operational.

**Data:**
Three numeric values are listed:
• The ID of the first unexpected inactive port. This ID is a decimal number.
• The ports that are expected to be active, which is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is expected to be active.
• The ports that are actually active, which is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is active.
The ports that are expected to be active, which is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is expected to be active.

The ports that actually have connections. This is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port has a connection to all online nodes.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Follow the procedure: Mapping I/O ports to platform ports to determine which platform port does not have connectivity.
3. There are a number of possibilities.
   • If the port's connectivity has been intentionally reconfigured, use the management GUI recommended action for the service error code and acknowledge the intended change. You must have at least two I/O ports with connections to all other node canisters, except the node canisters in the same enclosure.
   • Resolve other node errors relating to this platform port or I/O port.
   • Check that the SAN zoning is correct.

Possible Cause: FRUs or other cause:
• None

Fibre Channel clustered system path failure.

Explanation: One or more Fibre Channel (FC) input/output (I/O) ports that have previously been able to see all required online node canisters can no longer see them. This situation has continued for 5 minutes. This error is not reported unless a node is active in a clustered system.

Data:
Three numeric values are listed:
• The ID of the first FC 1/O port that does not have connectivity. This is a decimal number.
• The ports that are expected to have connections. This is a hexadecimal number, and each bit position represents a port - with the least significant bit representing port 1. The bit is 1 if the port is expected to have a connection to all online node canisters.
A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

**712** A SAS adapter has a PCI error.

**Explanation:** A SAS adapter has a PCI error. The adapter is located on the node canister system board.

**Data:**
- A number indicating the adapter location. Location 0 indicates the adapter that is integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Use the procedures to restart (physically remove and reseat) a node canister.
3. Locate the adapter on the system board and replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

**713** A SAS adapter is degraded.

**Explanation:** A SAS adapter is degraded. The adapter is located on the node canister system board.

**Data:**
- A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Use the procedures to restart (physically remove and reseat) a node canister.
3. Locate the adapter on the system board and replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

**720** Ethernet adapter that was previously present has not been detected.

**Explanation:** An Ethernet adapter that was previously present has not been detected. The adapters form a part of the canister assembly.

**Data:**
- A number indicating the adapter location. The location indicates an adapter slot. See the node canister description for the definition of the adapter slot locations. If the location is 0, the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the Ethernet adapters are integrated into the node canisters, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

**721** An Ethernet adapter has failed.

**Explanation:** An Ethernet adapter has failed. The adapters form part of the canister assembly.

**Data:**
- A number indicating the adapter location. The location indicates an adapter slot. See the node canister description for the definition of the adapter slot locations. If the location is 0, the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the Ethernet adapters are integrated into the node canisters, use the remove and replace procedures to replace the node canister.

Possible Cause—FRUs or other cause:
- Node canister

---

**722** An Ethernet adapter has a PCI error.

**Explanation:** An Ethernet adapter has a PCI error. The adapters form part of the canister assembly.

**Data:**
- A number indicating the adapter location. The location indicates an adapter slot. See the node canister description for the definition of the adapter slot locations. If the location is 0, the adapter integrated into the system board is being reported.
canister description for the definition of the adapter slot locations. If the location is 0, the adapter integrated into the system board is being reported.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the Ethernet adapters are integrated into the node canisters, use the remove and replace procedures to replace the node canister.

Possible Cause—FRUs or other cause:
- Node canister

723  An Ethernet adapter is degraded.

Explanation: An Ethernet adapter is degraded. The adapters form part of the canister assembly.

Data:
- A number indicating the adapter location. The location indicates an adapter slot. See the node canister description for the definition of the adapter slot locations. If the location is 0, the adapter integrated into the system board is being reported.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the Ethernet adapters are integrated into the node canisters, use the remove and replace procedures to replace the node canister.

Possible Cause—FRUs or other cause:
- Node canister

724  Fewer Ethernet ports active.

Explanation: An Ethernet port that was previously operational is no longer operational. The physical link is down.

Data:
- Three numeric values are listed:
  - The ID of the first unexpected inactive port. This is a decimal number.
  - The ports that are expected to be active. This is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is expected to be active.
  - The ports that are actually active. This is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is active.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Possibilities:
   a. If the port has been intentionally disconnected, use the management GUI recommended action for the service error code and acknowledge the intended change.
   b. Make sure the Ethernet cable is connected to both ends and is undamaged. If necessary, replace the cable.
   c. Make sure the switch port or other device the cable is connected to is powered and enabled in a compatible mode. Rectify any issue. The device service interface might indicate the issue.
   d. If this is a 10 Gb/s port, use the remove and replace procedures to replace the SFP transceiver in the Storwize V7000 and the SFP transceiver in the connected switch or device.
   e. Replace the node canister using the remove and replace procedures.

Possible Cause—FRUs or other cause:
- Ethernet cable
- Ethernet SFP transceiver
- Node canister

730  The bus adapter has not been detected.

Explanation: The bus adapter that connects the canister to the enclosure midplane has not been detected.

This node error does not, in itself, stop the node canister becoming active in the system. However, the bus might be being used to communicate between the node canisters in a clustered system. Therefore, it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

Data:
- A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause—FRUs or other cause:
- Node canister
The bus adapter has failed.

**Explanation:** The bus adapter that connects the canister to the enclosure midplane has failed.

This node error does not, in itself, stop the node canister becoming active in the system. However, the bus might be being used to communicate between the node canisters in a clustered system. Therefore, it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
- A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

The bus adapter has a PCI error.

**Explanation:** The bus adapter that connects the canister to the enclosure midplane has a PCI error.

This node error does not, in itself, stop the node canister becoming active in the system. However, the bus might be being used to communicate between the node canisters in a clustered system; therefore it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
- A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

**User response:**
1. If possible, this noncritical node error should be serviced using the management GUI and running the recommended actions for the service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

The bus adapter degraded.

**Explanation:** The bus adapter that connects the canister to the enclosure midplane is degraded.

This node error does not, in itself, stop the node canister becoming active in the system. However, the bus might be being used to communicate between the node canisters in a clustered system. Therefore, it is possible that this node error indicates the reason why the critical node error 550 A cluster cannot be formed because of a lack of cluster resources is reported on the node canister.

**Data:**
- A number indicating the adapter location. Location 0 indicates that the adapter integrated into the system board is being reported.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. As the adapter is located on the system board, replace the node canister using the remove and replace procedures.

Possible Cause-FRUs or other cause:
- Node canister

---

Fewer bus ports.

**Explanation:** One or more PCI bus ports that have previously been active are now inactive. This condition has existed for over one minute. That is, the internode link has been down at the protocol level.

This could be a link issue but is more likely caused by the partner node unexpectedly failing to respond.

**Data:**
Three numeric values are listed:
- The ID of the first unexpected inactive port. This is a decimal number.
- The ports that are expected to be active. This is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is expected to be active.
- The ports that are actually active. This is a hexadecimal number. Each bit position represents a port, with the least significant bit representing port 1. The bit is 1 if the port is active.

**User response:**
1. If possible, this noncritical node error should be serviced using the management GUI and running the recommended actions for the service error code.
2. Follow the procedure for getting node canister and clustered-system information and determine the state of the partner node canister in the enclosure.

Fix any errors reported on the partner node canister.
3. Use the remove and replace procedures to replace the enclosure.

Possible Cause-FRUs or other cause:
- Node canister
- Enclosure midplane

820 Canister type is incompatible with enclosure model

Explanation: The node canister has detected that it has a hardware type that is not compatible with the control enclosure MTM, such as node canister type 300 in an enclosure with MTM 2076-112.

This is an expected condition when a control enclosure is being upgraded to a different type of node canister.

User response:
1. Check that all the upgrade instructions have been followed completely.
2. Use the management GUI to run the recommended actions for the associated service error code.

Possible Cause-FRUs or other cause:
- None

860 Fibre Channel network fabric is too big.

Explanation: The number of Fibre Channel (FC) logins made to the node canister exceeds the allowed limit. The node canister continues to operate, but only communicates with the logins made before the limit was reached. The order in which other devices log into the node canister cannot be determined, so the node canister’s FC connectivity might vary after each restart. The connection might be with host systems, other storage systems, or with other node canisters.

This error might be the reason the node canister is unable to participate in a system.

The number of allowed logins per node is 1024.

Data:
- None

User response: This error indicates a problem with the Fibre Channel fabric configuration. It is resolved by reconfiguring the FC switch:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Res zone the FC network so only the ports the node canister needs to connect to are visible to it.

Possible Cause-FRUs or other cause:
- None

878 Attempting recovery after loss of state data.

Explanation: During startup, the node canister cannot read its state data. It reports this error while waiting to be added back into a clustered system. If the node canister is not added back into a clustered system within a set time, node error 578 is reported.

User response:
1. Allow time for recovery. No further action is required.
2. Keep monitoring in case the error changes to error code 578.

920 Unable to perform cluster recovery because of a lack of cluster resources.

Explanation: The node is looking for a quorum of resources which also require cluster recovery.

User response: Contact IBM technical support.

950 Special upgrade mode.

Explanation: Special upgrade mode.

User response: None.

990 Cluster recovery has failed.

Explanation: Cluster recovery has failed.

User response: Contact IBM technical support.

1021 Incorrect enclosure

Explanation: The cluster is reporting that a node is not operational because of critical node error 500. See the details of node error 500 for more information.

User response: See node error 500.

1036 The enclosure identity cannot be read.

Explanation: The cluster is reporting that a node is not operational because of critical node error 509. See the details of node error 509 for more information.

User response: See node error 509.

1188 Too many software crashes have occurred.

Explanation: The cluster is reporting that a node is not operational because of critical node error 564. See the details of node error 564 for more information.

User response: See node error 564.
The node is held in the service state.

**Explanation:** The cluster is reporting that a node is not operational because of critical node error 690. See the details of node error 690 for more information.

**User response:** See node error 690.

A solid-state drive is missing from the configuration.

**Explanation:** The offline solid-state drive (SSD) identified by this error must be repaired.

**User response:** In the management GUI, click Troubleshooting > Recommended Actions to run the recommended action for this error. Otherwise, use MAP 6000 to replace the drive.
Appendix. Accessibility features for *IBM Storwize V7000*

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

**Accessibility features**

These are the major accessibility features associated with the *Storwize V7000 Information Center*:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. PDF documents have been tested using Adobe Reader version 7.0. HTML documents have been tested using JAWS version 13.0.
- This product uses standard Windows navigation keys.

**Keyboard navigation**

You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the *Storwize V7000 Information Center* from the keyboard by using the shortcut keys for your browser or screen-reader software. See your browser or screen-reader software Help for a list of shortcut keys that it supports.

**IBM and accessibility**

See the [IBM Human Ability and Accessibility Center](http://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Almaden Research
650 Harry Road
Blag 80, D3-304, Department 277
San Jose, CA 95120-6099
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application
programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

IBM trademarks and special non-IBM trademarks in this information are identified and attributed.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Xeon, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

**Electronic emission notices**

The following electronic emission statements apply to this product. The statements for other products that are intended for use with this product are included in their accompanying documentation.

**Federal Communications Commission (FCC) statement**

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications.
Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

**Industry Canada compliance statement**

This Class A digital apparatus complies with ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

**Avis de conformité à la réglementation d’Industrie Canada**

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

**Australia and New Zealand Class A Statement**

**Attention:** This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

**European Union Electromagnetic Compatibility Directive**

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

**Attention:** This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:
Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A
EU-Richtlinie zur Elektromagnetischen Verträglichkeit


Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Department M372
Generelle Informationen: Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Council Class A statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

People’s Republic of China Class A Electronic Emission Statement

中华人民共和国“A类”警告声明

International Electrotechnical Commission (IEC) statement

This product has been designed and built to comply with (IEC) Standard 950.

United Kingdom telecommunications requirements

This apparatus is manufactured to the International Safety Standard EN60950 and as such is approved in the U.K. under approval number NS/G/1234/J/100003 for indirect connection to public telecommunications systems in the United Kingdom.

Korean Communications Commission (KCC) Class A Statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.
Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры.

Taiwan Class A compliance statement

警告使用者: 
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

European Contact Information

This topic contains the product service contact information for Europe.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
Email: mailto: tjahn @ de.ibm.com

Taiwan Contact Information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

電話：0800-016-888
Index

Numerics
10G Ethernet 68
2.5" drive assembly replacing 104
3.5" drive assembly replacing 102

A
about this document sending comments xv
accessibility  
disability xi, 155
features 155
keyboard xi, 155
navigation 155
overview xi
repeat rate
up and down buttons 155
shortcut keys 155
accessing
    canisters
        Ethernet cable 64
        cluster (system) CLI 35
        management GUI 32
    publications 155
    service assistant 34, 66
    service CLI 36
actions
    reset service IP address 38
    reset superuser password 38
    alerts
    best practices 21, 22
    apply software command 40

B
backing up
    best practices 21
    system configuration files 79
    backup configuration files deleting using the CLI 84
    restoring 81
bad blocks 29
battery
    maintenance 25, 26
    removing 99
    best practices 21, 22
    alerts 21, 22
    backing up data 21
    drive characteristics 21
    inventory reporting 21
    IP address 19
    notifications 20
    passwords 19
    power management 20
    RAID 21
    record
        location information 22
    best practices (continued)
        subscribe
            notifications 22
        troubleshooting 19
        warranty agreement
            maintenance agreement 22
        blank carrier
            replacing 102, 104
        browsers
            supported 48
    components (continued)
        end cap
            indicators 4
            hardware 1
    contact information
        European 163
        Taiwan 163
    control enclosure
        detection error 50
        power supply unit 6
        control enclosure chassis replacing 107
        create cluster command 40
        critical
            node errors 137
            Customer replaced 116
    C
cable retention bracket
        releasing 102
    Canadian electronic emission notice 160
    canister
        expansion 87
        identification 52
        node 85
        replacing 85, 87
    changing
        service IP address 61
    CLI
        cluster (system) commands 35
        service commands 35
        cluster (system) CLI
            accessing 35
            when to use 35
        cluster (system) commands CLI 35
    clustered storage system
        failure to create 46
    clustered system
        initializing
            with service assistant 63
            with USB key 62
        restore 77
    clustered systems
        error codes 138
        recovery codes 138
        restore 72
        T3 recovery 72
    codes
        node error
            critical 137
            noncritical 137
    commands
        apply software 40
        create cluster 40
        query status 41
        reset service assistant password 39
        satask.txt 38
        snap 39
        svcconfig backup 79
        svcconfig restore 81
    comments, sending xv
    components
        enclosure 2
        illustration 5
    documentation
        improvement xv
    drive characteristics
        best practices 21
        drives
            2.5-inch drives 2
            3.5-inch drives 2
            LED indicator 2
    electronic emission notices
        Avis de conformité à la réglementation d’Industrie Canada 160
        Deutschsprachiger EU Hinweis 161
        documentation
            accessibility xi, 155
        European Union (EU) 160
        Federal Communications Commission (FCC) 159
        French Canadian 160
        Germany 161
        Industry Canada 160
        International Electrotechnical Commission (IEC) 162
        Japanese Voluntary Control Council for Interference (VCCI) 162
        Korean 162
        New Zealand 160
        People’s Republic of China 162
Taiwan 163
United Kingdom 162
EMC statement, People's Republic of China 162
enclosure
components 5
identification 52
enclosure end caps
replacing 106
end cap
indicators 4
environmental notices ix
error
cell enclosure 50
expansion enclosure 49
node canister 48
not detected 49, 50
SAS cabling 49
USB flash drive 50
error codes 126
understanding 122
error event IDs 126
error events 119
errors
logs
describing the fields 120
error events 119
managing 120
understanding 119
viewing 119
node 137
Ethernet
accessing
canister 64
ports 11
status 59
European contact information 163
European Union (EU), EMC Directive conformance statement 160
event IDs 122
event notification 121
events
reporting 119
expansion canister
LEDs 16
expansion enclosure
detection error 49
power supply unit 7
replacing 112

failure
storage system creation 46
FCC (Federal Communications Commission) electronic emission notice 159
features
accessibility 155
Federal Communications Commission (FCC) electronic emission notice 159
Fibre Channel
link failures 68
port numbers 10
SFP transceiver 68
Fibre Channel ports
rear-panel indicators 9
field replaceable units (FRUs) 116
fields
event log 120
finding
Ethernet
status 59
fix
errors 74
fixing
node errors 61
French Canadian electronic emission notice 160
Germany electronic emission compliance statement 161
GUI connectivity issues
troubleshooting procedure 44, 47
hardware components 1
identifying
canister 52
enclosure 52
status 52
IEC (International Electrotechnical Commission) electronic emission notice 162
indicators
detected 4
information center xii
informational events 122
initialization tool
interface 36
using 37
initializing
clustered system
with USB key 62
clustered systems
with service assistant 63
International Electrotechnical Commission (IEC) electronic emission notice 162
inventory information 121
inventory reporting
best practices 21
IP address
best practices 19
Japanese electronic emission notice 162
keyboard
accessibility xi, 155
Korean electronic emission statement 162
LEDs
exansion canister 16
Fibre Channel ports 9
node canister 14
rear-panel indicators 9
system status 54
legal notices
Notices 157
trademarks 159
link failures
Fibre Channel 68
location information record
best practices 22
log files
viewing 119
maintenance
battery 25, 26
management GUI
accessing 32
cannot log on 45
review browsers 48
troubleshooting procedure start here 43
management GUI interface
when to use 32
management IP address
troubleshooting procedure 44
managing
error log 120
medium errors 29
message classification 138
mirrored volumes
not identical 50
navigation
accessibility 155
New Zealand electronic emission statement 160
node canister
LEDs 14
location error 48
repeating 65
unknown service address 46
USB ports 10
viewing
system status 53
node errors
fixing 61
node rescue
performing 67
noncritical
node errors 137
notifications
best practices 20
sending 121
subscribe
best practices 22
number range 138

P
panel
   rear
      Fibre Channel ports 9
parts
   removing
      overview 85
      preparing 85
   replacing
      overview 85
      preparing 85
passwords
   best practices 19
People's Republic of China, electronic emission statement 162
performing
   node rescue 67
ports
   Ethernet 11
      port names, worldwide 10
      port numbers, Fibre Channel 10
   SAS 13, 16
POST (power-on self-test) 121
power management
   best practices 20
power supply
   replacing 91, 95
power supply unit
   control enclosure 6
   expansion enclosure 7
      with battery 6
power-on self-test 121
powering off
   system 65
problem
   mirrored volumes
      not identical 50
publications
   accessing 155
query status command 41

Q
query status command 41

R
RAID
   best practices 21
reader feedback, sending xv
rear-panel indicators
   Fibre Channel ports 9
recovery
   offline virtual disks (volumes)
      using CLI 76
recovery
   system
      when to run 72
   systems
      starting 75
related information xii
releasing
   cable retention bracket 102
removing
   550 errors 74
   578 errors 74
   parts
      overview 85
      preparing 85
   SFP transceiver 89
   system 60
   system data 60
replaceable units 116
replacing
   2.5" drive assembly 104
   3.5" drive assembly 102
   battery 99
   blank carrier 102, 104
   control enclosure chassis 107
   enclosure end caps 106
   expansion canister 87
   expansion enclosure 112
   node canister 85
   parts
      overview 85
      preparing 85
   power supply
      control enclosure 91
      expansion enclosure 95
   SAS cable 106
   SFP transceiver 89
   support rails 115
reporting
   events 119
rescue
   performing
      for a node 67
reseating
   node canister 65
reset service assistant password 39
reset service IP address 38
reset superuser password 38
resetting
   superuser password 51
restore
   system 71, 77
service CLI
   accessing 36
   when to use 36
service commands
   apply software 40
   CLI 35
   create cluster 40
   reset service assistant password 39
   reset service IP address 38
   reset superuser password 38
   snap 39
service IP address
   changing 61
SFP transceiver
   removing 89
   replacing 89
shortcut keys
   accessibility 155
   keyboard 155
snap command 39
sound pressure
   safety notices ix
starting
   system recovery 75
status
   Ethernet 59
       identifying 52
       node canister 53
       system 53
storage area network (SAN)
   problem determination 68
storage systems
   restore 71
   servicing 71
Storwize V7000 library
   related publications xii
summary of changes xi, xii
superuser
   password
      resetting 51
supported browsers 48
system
   backing up configuration file using
      the CLI 79
   deleting 60
   restoring backup configuration files 81
system data
   removing 60
system status
   LEDs 54

T
T3 recovery
   removing
      550 errors 74
      578 errors 74
   when to run 72
Taiwan
   contact information 163
   electronic emission notice 163
trademarks 159
troubleshooting
   best practices 19
   event notification email 121
   node errors 61
troubleshooting (continued)
SAN failures 68
troubleshooting procedure
GUI connectivity issues
main GUI 44
service assistant 47
management IP address 44
start here
management GUI 43

U
understanding
clustered-system recovery codes 138
troubleshooting (continued)
error codes 122
event log 119
United Kingdom electronic emission notice 162
USB flash drive
detection error 50
USB key
using 36
when to use 36
USB ports 10
using
GUI interfaces 31
initialization tool 37
initialization tool interface 36
management GUI 31
service assistant 33
USB key 36

V
VDisks (volumes)
recovering from offline
using CLI 76
viewing
event log 119
node canister status 53
system status 53
volumes (VDisks)
recovering from offline
using CLI 76

W
warranty agreement
best practices 22
when to use
cluster (system) CLI 35
management GUI interface 32
service assistant 33
service CLI 36
USB key 36
worldwide port names (WWPNs)
description 10