Before using this information and the product it supports, read the general information in "Notices" on page 205, the information in the "Safety and environmental notices" on page iii, as well as the information in the IBM Environmental Notices and User Guide, which is provided on a DVD.
Safety and environmental notices

Review the safety notices, environmental notices, and electronic emission notices for IBM® Storwize® V7000 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.

Here are examples of a caution and a danger notice:

**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)

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 preceding examples, the numbers (C001) and (D002) are the identification numbers.
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](http://www.ibm.com/storage/support/storwize/v7000) and click the documentation link.

Safety notices and labels

Review the safety notices and safety information labels before using this product.

To view a PDF file, you need Adobe Acrobat Reader. You can download it at no charge from the Adobe website:


IBM Systems Safety Notices

This publication contains the safety notices for the IBM Systems products in English and other languages. Anyone who plans, installs, operates, or services the system must be familiar with and understand the safety notices. Read the related safety notices before you begin work.

**Note:** The *IBM Systems Safety Notices* document is organized into two sections. The danger and caution notices without labels are organized alphabetically by
language in the “Danger and caution notices by language” section. The danger and caution notices that are accompanied with a label are organized by label reference number in the “Labels” section.

The following notices and statements are used in IBM documents. They are listed in order of decreasing severity of potential hazards.

**Danger notice definition**
A special note that emphasize a situation that is potentially lethal or extremely hazardous to people.

**Caution notice definition**
A special note that emphasize a situation that is potentially hazardous to people because of some existing condition, or to a potentially dangerous situation that might develop because of some unsafe practice.

**Note:** In addition to these notices, labels might be attached to the product to warn of potential hazards.

### Finding translated notices

Each safety notice contains an identification number. You can use this identification number to check the safety notice in each language.

To find the translated text for a caution or danger notice:

1. In the product documentation, look for the identification number at the end of each caution notice or each danger notice. In the following examples, the numbers (D002) and (C001) are the identification numbers.

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

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

2. Open the [IBM Systems Safety Notices](#).
3. Under the language, find the matching identification number. Review the topics about the safety notices to ensure that you are in compliance.

**Note:** This product was designed, tested, and manufactured to comply with IEC 60950-1, and where required, to relevant national standards that are based on IEC 60950-1.

### Caution notices for the Storwize V7000

Ensure that you understand the caution notices for Storwize V7000.

Use the reference numbers in parentheses at the end of each notice, such as (C003) for example, to find the matching translated notice in *IBM Storwize V7000 Safety Notices*. 
CAUTION:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not: Throw or immerse into water, heat to more than 100°C (212°F), repair or disassemble. (C003)

CAUTION:
Electrical current from power, telephone, and communication cables can be hazardous. To avoid personal injury or equipment damage, disconnect the attached power cords, telecommunication systems, networks, and modems before you open the machine covers, unless instructed otherwise in the installation and configuration procedures. (26)

CAUTION:
Use safe practices when lifting.

(27)

CAUTION:
- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- (For sliding drawers) Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.
- (For fixed drawers) This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.

(R001 part 2 of 2)
CAUTION:
Removing components from the upper positions in the rack cabinet improves rack stability during a relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building.

- Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must observe the following precautions.
  - Remove all devices in the 32U position and above.
  - Ensure that the heaviest devices are installed in the bottom of the rack cabinet.
  - Ensure that there are no empty U-levels between devices installed in the rack cabinet below the 32U level.
- If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.
- If the rack cabinet you are relocating was supplied with removable outriggers, they must be reinstalled before the cabinet is relocated.
- Inspect the route that you plan to take to eliminate potential hazards.
- Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.
- Verify that all door openings are at least 760 x 230 mm (30 x 80 in.).
- Ensure that all devices, shelves, drawers, doors, and cables are secure.
- Ensure that the four leveling pads are raised to their highest position.
- Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.
- Do not use a ramp inclined at more than 10 degrees.
- When the rack cabinet is in the new location, complete the following steps:
  - Lower the four leveling pads.
  - Install stabilizer brackets on the rack cabinet.
  - If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.
- If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off the pallet and bolt the rack cabinet to the pallet.

(R002)

CAUTION:
- Rack is not intended to serve as an enclosure and does not provide any degrees of protection required of enclosures.
- It is intended that equipment installed within this rack will have its own enclosure. (R005).

CAUTION:
Tighten the stabilizer brackets until they are flush against the rack. (R006)

CAUTION:
Use safe practices when lifting. (R007)
CAUTION:
Do not place any object on top of a rack-mounted device unless that
rack-mounted device is intended for use as a shelf. (R008)

CAUTION:
If the rack is designed to be coupled to another rack only the same model rack
should be coupled together with another same model rack. (R009)

Danger notices for Storwize V7000

Ensure that you are familiar with the danger notices for Storwize V7000.

Use the reference numbers in parentheses at the end of each notice, such as (C003)
for example, to find the matching translated notice in IBM Storwize V7000 Safety
Notices.
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:

- If IBM supplied a power cord(s), 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)

DANGER

Heavy equipment—personal injury or equipment damage might result if
mishandled. (D006)

DANGER
Observe the following precautions when working on or around your IT rack system:

- Heavy equipment—personal injury or equipment damage might result if mishandled.
- Always lower the leveling pads on the rack cabinet.
- Always install stabilizer brackets on the rack cabinet.
- To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.
- Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices.

- Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

(R001 part 1 of 2)

DANGER

Racks with a total weight of > 227 kg (500 lb.), Use Only Professional Movers! (R003)

DANGER

Do not transport the rack via fork truck unless it is properly packaged, secured on top of the supplied pallet. (R004)
DANGER

Main Protective Earth (Ground):

This symbol is marked on the frame of the rack.

The PROTECTIVE EARTHING CONDUCTORS should be terminated at that point. A recognized or certified closed loop connector (ring terminal) should be used and secured to the frame with a lock washer using a bolt or stud. The connector should be properly sized to be suitable for the bold or stud, the locking washer, the rating for the conducting wire used, and the considered rating of the breaker. The intent is to ensure the frame is electrically bonded to the PROTECTIVE EARTHING CONDUCTORS. The hole that the bolt or stud goes into where the terminal conductor and the lock washer contact should be free of any non-conductive material to allow for metal to metal contact. All PROTECTIVE EARTHING CONDUCTORS should terminate at this main protective earthing terminal or at points marked with ↓. (R010)

Special caution and safety notices

This information describes special safety notices that apply to the Storwize V7000. These notices are in addition to the standard safety notices supplied and address specific issues relevant to the equipment provided.

General safety

When you service the Storwize V7000, follow general safety guidelines.

Use the following general rules to ensure safety to yourself and others:

- Observe good housekeeping in the area where the devices are kept during and after maintenance.
- Follow the guidelines when lifting any heavy object:
  1. Ensure that you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 18 kg (40 lb) or objects that you think are too heavy for you.
- Do not perform any action that causes a hazard or that makes the equipment unsafe.
- Before you start the device, ensure that other personnel are not in a hazardous position.
- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the unit.
- Keep your tool case away from walk areas so that other people will not trip over it.
• Do not wear loose clothing that can be trapped in the moving parts of a device. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
• Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconducting clip, approximately 8 cm (3 in.) from the end.
• Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing.

  **Remember:** Metal objects are good electrical conductors.
• Wear safety glasses when you are: hammering, drilling, soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.
• After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
• Reinstall all covers correctly after you have finished servicing the unit.

### Handling static-sensitive devices

Ensure that you understand how to handle devices that are sensitive to static electricity.

**Attention:** Static electricity can damage electronic devices and your system. To avoid damage, keep static-sensitive devices in their static-protective bags until you are ready to install them.

To reduce the possibility of electrostatic discharge, observe the following precautions:
• Limit your movement. Movement can cause static electricity to build up around you.
• Handle the device carefully, holding it by its edges or frame.
• Do not touch solder joints, pins, or exposed printed circuitry.
• Do not leave the device where others can handle and possibly damage the device.
• While the device is still in its antistatic bag, touch it to an unpainted metal part of the system unit for at least two seconds. (This action removes static electricity from the package and from your body.)
• Remove the device from its package and install it directly into your Storwize V7000, without putting it down. If it is necessary to put the device down, place it onto its static-protective bag. (If your device is an adapter, place it component-side up.) Do not place the device onto the cover of the Storwize V7000 or onto a metal table.
• Take additional care when you handle devices during cold weather because heating reduces indoor humidity and increases static electricity.

### 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.

### Environmental notices

This information contains all the required environmental notices for IBM Systems products in English and other languages.

To view a PDF file, you need Adobe Reader. You can download it at no charge from the Adobe web site (get.adobe.com/reader/).
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.

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:

publib.boulder.ibm.com/infocenter/storwize/ic/index.jsp

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/e-business/linkweb/publications/servlet/pbi.wss

The following table lists websites where you can find help, services, and more information:

<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>
</tbody>
</table>
Table 1. IBM websites for help, services, and information (continued)

<table>
<thead>
<tr>
<th>Website</th>
<th>Address</th>
</tr>
</thead>
</table>

Each of the PDF publications in the Table 2 is also available in the information center by clicking the number in the “Order number” column:

Table 2. 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 detailed 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>GC27-4234</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 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>
</tbody>
</table>
Table 2. Storwize V7000 library (continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Order number</th>
</tr>
</thead>
<tbody>
<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 Z125-5468)</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>IBM Storage Management Pack for Microsoft System Center Operations Manager (SCOM)</td>
<td>The IBM Storage Host Software Solutions Information Center describes how to install, configure, and use the IBM Storage Management Pack for Microsoft System Center Operations Manager.</td>
</tr>
<tr>
<td>IBM Storage Management Console for VMware vCenter</td>
<td>The IBM Storage Host Software Solutions Information Center 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>
</tr>
<tr>
<td>IBM Storage Device Driver for VMware VAAI</td>
<td>IBM Storage Host Software Solutions Information Center describes how to install, configure, and use the IBM Storage Device Driver for VMware VAAI.</td>
</tr>
<tr>
<td>IBM Storwize V7000 Adapter for VMware vCenter Site Recovery Manager</td>
<td>The VMware website describes how to install, configure, and use the IBM Storwize V7000 Adapter for VMware vCenter Site Recovery Manager.</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 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

Related websites

The following websites provide information about Storwize V7000 or related products or technologies:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storwize V7000 support</td>
<td><a href="http://www.ibm.com/storage/support/storwize/v7000">www.ibm.com/storage/support/storwize/v7000</a></td>
</tr>
</tbody>
</table>

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 form on the website for the Storwize V7000 Information Center at [publib.boulder.ibm.com/infocenter/storwize/ic/index.jsp?topic=](http://publib.boulder.ibm.com/infocenter/storwize/ic/index.jsp?topic=/com.ibm.storwize.v7000.doc/feedback.htm) You can use the form to enter and submit comments. You can browse to the topic in question and use the feedback link at the very bottom of the page to automatically identify the topic for which you have a comment.
- Send your comments by email to starpubs@us.ibm.com Include the following information in your email:
  - Publication title
  - Publication form number
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that should be changed

How to get information, help, and technical assistance

If you need help, service, technical assistance, or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Information

IBM maintains pages on the web where you can get information about IBM products and fee services, product implementation and usage assistance, break and fix service support, and the latest technical information. For more information, refer to [Table 4 on page xvii](#).
Table 4. IBM websites for help, services, and information

<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>
</tbody>
</table>

Note: Available services, telephone numbers, and web links are subject to change without notice.

Help and service

Before calling for support, be sure to have your IBM Customer Number available. If you are in the US or Canada, you can call 1 (800) IBM SERV for help and service. From other parts of the world, see http://www.ibm.com/planetwide for the number that you can call.

When calling from the US or Canada, choose the storage option. The agent decides where to route your call, to either storage software or storage hardware, depending on the nature of your problem.

If you call from somewhere other than the US or Canada, you must choose the software or hardware option when calling for assistance. Choose the software option if you are uncertain if the problem involves the Storwize V7000 software or hardware. Choose the hardware option only if you are certain the problem solely involves the Storwize V7000 hardware. When calling IBM for service regarding the product, follow these guidelines for the software and hardware options:

Software option
Identify the Storwize V7000 product as your product and supply your customer number as proof of purchase. The customer number is a 7-digit number (0000000 to 9999999) assigned by IBM when the product is purchased. Your customer number should be located on the customer information worksheet or on the invoice from your storage purchase. If asked for an operating system, use Storage.

Hardware option
Provide the serial number and appropriate 4-digit machine type. For Storwize V7000, the machine type is 2076.

In the US and Canada, hardware service and support can be extended to 24x7 on the same day. The base warranty is 9x5 on the next business day.

Getting help online

You can find information about products, solutions, partners, and support on the IBM website.

To find up-to-date information about products, services, and partners, visit the IBM website at [www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000)

Before you call

Make sure that you have taken steps to try to solve the problem yourself before you call.
Some suggestions for resolving the problem before calling IBM Support include:

- Check all cables to make sure that they are connected.
- Check all power switches to make sure that the system and optional devices are turned on.
- Use the troubleshooting information in your system documentation. The troubleshooting section of the information center contains procedures to help you diagnose problems.
- Go to the IBM Support website at [www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000) to check for technical information, hints, tips, and new device drivers or to submit a request for information.

**Using the documentation**

Information about your IBM storage system is available in the documentation that comes with the product.

That documentation includes printed documents, online documents, readme files, and help files in addition to the information center. See the troubleshooting information for diagnostic instructions. The troubleshooting procedure might require you to download updated device drivers or software. IBM maintains pages on the web where you can get the latest technical information and download device drivers and updates. To access these pages, go to [www.ibm.com/storage/support/storwize/v7000](http://www.ibm.com/storage/support/storwize/v7000) and follow the instructions. Also, some documents are available through the IBM Publications Center.

**Sign up for the Support Line Offering**

If you have questions about how to use and configure the machine, sign up for the IBM Support Line offering to get a professional answer.

The maintenance supplied with the system provides support when there is a problem with a hardware component or a fault in the system machine code. At times, you might need expert advice about using a function provided by the system or about how to configure the system. Purchasing the IBM Support Line offering gives you access to this professional advice while deploying your system, and in the future.

Contact your local IBM sales representative or the IBM Support Center for availability and purchase information.

**What's new**

New and updated information was included in this version of the book as a result of usability testing and other feedback. Read all of the steps no matter how familiar you are with the installation.
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 installed in each slot.

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

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 5 shows the status descriptions for the two LEDs.

**Table 5. Drive LEDs**

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

**Enclosure end cap indicators**

This topic describes the indicators on the enclosure end cap.

Figure 5 on page 4 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 on page 4 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 6. 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>1 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>![Power LED symbol]</td>
</tr>
<tr>
<td>Fault</td>
<td>2 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>![Fault LED symbol]</td>
</tr>
<tr>
<td>Identify</td>
<td>3 The identify LED is the lower LED. When the blue LED is lit, it identifies the enclosure.</td>
<td>Blue</td>
<td>![Identify LED symbol]</td>
</tr>
<tr>
<td>N/A</td>
<td>4 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 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 shows the rear of an expansion enclosure.
Power supply unit and battery for the 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.

Each power supply unit has a power switch. 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](image) shows the location of the LEDs in the rear of the power supply unit.

![Figure 10](image) shows the location of the LEDs in the rear of the power supply unit.

<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>
</tbody>
</table>

Table 7 identifies the LEDs in the rear of the control enclosure.
Table 7. Power supply unit LEDs in the rear of the control enclosure (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<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 on the power supply units of the expansion enclosure.  

![Figure 11](image)

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

Table 8 on page 8 identifies the LEDs in the rear of the expansion enclosure.
Table 8. 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 on page 9. 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.

Table 9. 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</td>
<td>First LED between ports 1 and 3</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 1</td>
<td>Second LED between ports 1 and 3</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 3</td>
<td>Third LED between ports 1 and 3</td>
<td>Link</td>
</tr>
<tr>
<td>Port 1</td>
<td>Fourth LED between ports 1 and 3</td>
<td>Link</td>
</tr>
<tr>
<td>Port 4</td>
<td>First LED between ports 2 and 4</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 2</td>
<td>Second LED between ports 2 and 4</td>
<td>Speed</td>
</tr>
<tr>
<td>Port 4</td>
<td>Third LED between ports 2 and 4</td>
<td>Link</td>
</tr>
<tr>
<td>Port 2</td>
<td>Fourth LED between ports 2 and 4</td>
<td>Link</td>
</tr>
</tbody>
</table>

Table 10 provides the status descriptions for the LEDs on the Fibre Channel ports.

Table 10. 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 run 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. 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.

Figure 14. USB ports on the node canisters

The USB ports have no indicators.
Ethernet ports and indicators

Ethernet 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. 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 11 provides a description of the two 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 16 on page 12 shows the location of the 10 Gbps Ethernet ports.
Table 12 provides a description of the LEDs.

### Table 12. 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 on page 13. 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.
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 13. 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.
**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>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
</table>
| System status | Indicates the status of the node.  
  - 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.  
  - The off status indicates there is no power to the canister or the canister is in standby mode. These conditions can cause the off state:  
    - The main processor is off and only the service processor is active.  
    - A power-on self-test (POST) is running on the canister.  
    - The operating system is loading.  
  - 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. | Green | ![Symbol] |
| 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 | ![Symbol] |
| 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 | ![Symbol] |
Table 14. Node canister LEDs (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Color</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>If the system status LED is on and the fault LED is off, the node canister is an active member of a system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>If the system status LED is on and the fault LED is on, there is a problem establishing a system.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 on page 16. 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.
Port 1, 6 Gbps SAS port and LEDs
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 15. SAS port LEDs on the expansion 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>

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 16. Expansion canister LEDs

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

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 the 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 in Table 17 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 management GUI or the `chserviceip` CLI command.

- The service IP address of the node canisters on the control enclosure 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 17. 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 management GUI and CLI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The management user ID (the default is <code>admin</code>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The management user ID password (the default is <code>admin</code>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The additional management user IDs and passwords that you create on your system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The control enclosure superuser IP address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 17. 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: node canister 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control enclosure service IP address: node canister 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The control enclosure superuser password (the default is <code>password</code>)</td>
<td></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.
- **Call Home.** 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 the 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.

Complete 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
www.ibm.com/storage/support/

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

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 brown outs,
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.
Chapter 4. Understanding the medium errors and bad blocks

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

Table 18 lists the bad block error codes.

<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 18. 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.
- Complete service procedures from the service assistant.
- Use the command-line interface (CLI) to manage your system. The front panel on the node provides an alternative service interface.

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 action (default)**

Shows only the alerts that require attention and have an associated fix procedure. 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 on any alert with an error code.
- 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 on any alert with an error code.
• 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.

- **Recommended Actions.** For each problem that is selected, you can:
  - Run a fix procedure.
  - View the properties.
- **Event log.** 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.

**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

To view events, you must access the management GUI.

About this task

You must use a supported web browser. For a list of supported browsers, refer to the “Web browser requirements to access the management GUI” topic.

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 will 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: Complete 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 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 complete 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 completing 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.

The service assistant completes a number of tasks that 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 completed 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. For a list of supported browsers, refer to the “Web browser requirements to access the management GUI” topic.

Procedure

To start the application, complete the following steps.

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 passw0rd. 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

Complete 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” 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” 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**

To initialize and use a CLI session, complete the steps in the “Command-line interface” topic in the “Reference” section of this information center.

**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 that is used to create the satask.txt file on a USB flash drive.

Before you begin

Verify that you are using a supported operating system. The initialization tool is valid for the following operating systems.
- Microsoft Windows 7 (64-bit) or XP (32-bit)
- Apple MacOS X 10.7
- Red Hat Enterprise Server 5 or Ubuntu desktop 11.04

About this task

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

Set the management IP addresses.

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.

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
```

**Procedure**

To use the initialization tool, complete the following steps.

1. If you downloaded the initialization tool, copy the file onto the USB flash drive that you are going to use.
2. To start the initialization tool, insert the USB flash drive that contains the program into a USB slot on a suitable personal computer.
3. Run the `InitTool.exe` program from the USB drive.
   - **Windows**: Open the USB flash drive and double-click `InitTool.bat`.
   - **Apple Macintosh**: Locate the root directory of the USB flash drive (usually located in the `/Volumes/` directory). Type `sh InitTool.sh`.
   - **Linux**: Locate the root directory of the USB flash drive. (It is usually located in the `/media/` directory. If an automatic mount system is used, the root directory can be located by typing the mount command.) Type `sh InitTool.sh`.

   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.

4. After the `satask.txt` file is created, follow the instructions in “Using a USB flash drive” on page 37 to run the commands on the node.
5. When the commands have run, return the USB flash drive to your personal computer and start the tool again to see the results.

**satask.txt commands**

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

```
 $$ satask - chserviceip --serviceip=ipv4 --gw=ipv4 --mask=ipv4 --resetpassword $$
```

```
 $$ satask - chserviceip --serviceip_6=ipv6 --gw_6=ipv6 --prefix_6=int --resetpassword $$
```

```
 $$ satask - chserviceip --default --resetpassword $$
```

Parameters

- `serviceip ipv4`
  (Optional) The IPv4 address for the service assistant.

- `gw ipv4`
  (Optional) The IPv4 gateway for the service assistant.

- `mask ipv4`
  (Optional) The IPv4 subnet for the service assistant.

- `serviceip_6 ipv6`
  (Optional) The IPv6 address for the service assistant.

- `gw_6 ipv6`
  (Optional) The IPv6 gateway for the service assistant.

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

- `prefix_6 int`
  (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 `passw0rd`. 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 the `snap` command to collect diagnostic information from the node canister and to write the output to a USB flash drive.

Syntax

```
> satask -- snap ---------------
```

Parameters

- `-dump`
  (Optional) Indicates the most recent dump file in the output.

- `-noimm`
  (Optional) Indicates the `/dumps/imm.ffdc` file should not be included in the output.

- `panel_name`
  (Optional) Indicates the node on which to execute the `snap` command.

Description

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

This command calls the `satask snap` command.

If collected, the IMM FFDC file is present in the `snap` archive in `/dumps/imm.ffdc.<node.dumpname>.<date>.<time>.tgz`. The system waits for up to five minutes for the IMM to generate its FFDC. The status of the IMM FFDC is located in the `snap` archive in `/dumps/imm.ffdc.log`. These two files are not left on the node.
An invocation example

satask snap -dump 111584

The resulting output:
No feedback

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

Syntax

```
    satask installsoftware -file filename [-ignore] [-pacedccu]
```

Parameters

- **-file filename**
  (Required) The *filename* designates the name of the upgrade package.

- **-ignore** | **-pacedccu**
  (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 system 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 ipv4**
  (Optional) The IPv4 address for Ethernet port 1 on the system.

- **-gw ipv4**
  (Optional) The IPv4 gateway for Ethernet port 1 on the system.

- **-mask ipv4**
  (Optional) The IPv4 subnet for Ethernet port 1 on the system.
- `clusterip_6 ipv6`
  (Optional) The IPv6 address for Ethernet port 1 on the system.

- `gw_6 ipv6`
  (Optional) The IPv6 gateway for Ethernet port 1 on the system.

- `prefix_6 int`
  (Optional) The IPv6 prefix for Ethernet port 1 on the system.

- `name cluster_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 initialize or create a 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.
Ensuring 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 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 all node canisters is candidate, then there is not a clustered system to connect to. If all nodes are in a service state, go to “Procedure: Fixing node errors” on page 60.

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**

If you can see the management GUI login screen but cannot log on, you have several options for correcting the problem.

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

- If you are not logging on as superuser, contact your system administrator to 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.
- If you do not know the password for superuser, go to “Procedure: Resetting superuser password” on page 51.
Problem: Cannot initialize or create a system

This topic helps if your attempt to create a 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 "Procedure: Getting node canister and system information using the service assistant" on page 53 or "Procedure: Getting node canister and system information using a USB flash drive" on page 53.

- 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 "Procedure: Getting node canister and system information using the service assistant" on page 53 or "Procedure: Getting node canister and system information using a USB flash drive" on page 53. 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

You can use several methods to determine the service address of a node canister.

A default service address is initially assigned to each node canister, as shown in Table 19 on page 47. Try using these addresses if the node has not been reconfigured, and the addresses are valid on your network.

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.

Table 19. Default service IP addresses

<table>
<thead>
<tr>
<th>Canister and port</th>
<th>IPv4 address</th>
<th>IPv4 subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canister 1 (left) port 1 (left)</td>
<td>192.168.70.121</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Canister 2 (right) port 1 (left)</td>
<td>192.168.70.122</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**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 1 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 63.

Problem: Management GUI or service assistant does not display correctly

If the Management GUI or the service assistant does not display correctly, verify that you are using a supported web browser.

For a list of supported browsers, see Web browser requirements to access the management GUI.

Problem: A node canister has a location node error

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

A location error means 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.
A number of different conditions are reported as location errors. 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” on page 49.

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 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 `passw0rd` 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
Procedure
1. Insert the USB flash drive in one of the USB ports of the node canister from which you want to collect data.
2. The node canister fault LED flashes while information is collected and written to the USB flash drive.
3. Wait until the LED stops flashing before removing the USB flash drive. Because the LED is a fault indicator, it might remain permanently on or off.
4. View the results in file `satask_result.html` in a web browser. The file contains the details and results of the command that was run and the status and the configuration information from the node canister.

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.

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 52.

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 20. Power-supply unit LEDs

<table>
<thead>
<tr>
<th>Power supply OK</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>On</td>
<td>Communication failure between the power supply unit and the enclosure chassis. 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>Off</td>
<td>No ac power to the enclosure. 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. Seat the power supply unit correctly in the enclosure.</td>
<td></td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>Off</td>
<td>On</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 21. LEDs on the power supply units of the control enclosure*
Table 20. Power-supply unit LEDs (continued)

<table>
<thead>
<tr>
<th>Power supply OK</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>Off</td>
<td>Off</td>
<td>Off</td>
<td>Power supply is on and operational.</td>
<td>No actions</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>Off</td>
<td>Fan failure</td>
<td>Replace the power supply unit.</td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>Communication failure and power supply problem</td>
<td>Replace the power supply unit. If replacing the power supply unit does not fix the problem, replace the enclosure chassis.</td>
</tr>
<tr>
<td>Flashing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>No canister is operational.</td>
<td>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.</td>
</tr>
<tr>
<td>Off</td>
<td>Flashing</td>
<td>Flashing</td>
<td>Flashing</td>
<td>Firmware is downloading.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 21. 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 64. If the state persists, follow the hardware replacement procedures for the parts in the following order: node canister, enclosure chassis.</td>
</tr>
<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 &quot;Procedure: Reseating a node canister&quot; on page 64.</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 &quot;Procedure: Reseating a node canister&quot; on page 64. If the state persists, follow the hardware replacement procedure for the node canister.</td>
</tr>
</tbody>
</table>
3. If the power LED is on, consider the states of the clustered-system status and fault LEDs.

Table 22. 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>
</table>
| Off               | Off       | Code is not active. | • Follow procedures for reviewing power LEDs.  
|                   |           |        | • If the power LEDs show green, reseat the node canister. See “Procedure: Reseating a node canister” on page 64. If the LED status does not change, see “Replacing a node canister” on page 85. |
| Off               | On        | Code is not active. The BIOS or the service processor has detected a hardware fault. | Follow the hardware replacement procedures for the node canister. |
| On                | Off       | Code is active. Node state is active. | No action. The node canister is part of a clustered system and can be managed by the management GUI. |
| On                | On        | 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. |
Table 22. 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>Flasing</td>
<td>Off</td>
<td>Code is active. Node state is candidate.</td>
<td>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>
</tr>
<tr>
<td>Flasing</td>
<td>On</td>
<td>Code is active. Node state is service.</td>
<td>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>
</tr>
<tr>
<td>Any</td>
<td>Flashing</td>
<td>The node canister is being identified so that you can locate it.</td>
<td>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>
</tr>
</tbody>
</table>

Results

To review the status of the control enclosure batteries, see Table 23.

Table 23. Control enclosure battery LEDs

<table>
<thead>
<tr>
<th>Battery Good</th>
<th>Battery Fault</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 in process.</td>
<td>None</td>
</tr>
<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

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:

- If the node software is active on the node, 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 whether 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.

Procedure

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

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: Do not remove the system data from a node unless instructed to do so by a service procedure. Do not use this procedure to remove the system data from the only online node canister in a system. If the system data is removed or lost from all node canisters in the system, the system is effectively deleted. Attempting a system recovery procedure to restore a deleted system is not guaranteed to recover all of your volumes.

Procedure

1. Log into the service assistant of the node canister.
2. Use the service assistant node action to hold the node in service state.
3. Click Manage System; then click Remove system data to remove the system data from the node.

Results

The node canister restarts in service state.
What to do next

When you want the node canister to be active again, use the service assistant to leave service state. The node canister moves to candidate state, and can be added to the system. If the partner node canister is already active, the candidate node is added automatically.

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. Repeat steps 1 through 3 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 node errors that are detected by node canisters in your system, use this procedure.

About this task

Node errors are reported in the service assistant when a node detects erroneous conditions in a node canister.

Procedure

1. Carry out "Procedure: Getting node canister and system information using the service assistant" on page 53 to understand the state of each node.
2. If possible, log into the management GUI and use the monitoring page to run the recommended fix procedure.
   a. Follow the fix procedure instructions to completion.
   b. Repeat this step for each subsequent recommended fix procedure.
3. If it is not possible to access the management GUI, or no recommended actions are listed, refer to Reference > Messages and codes > Event IDs Error event IDs and error codes from the Information Center and follow the identified user response for each reported node error.

**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, 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 37.

**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 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. (For a complete list of commands you can use in a satask.txt file, see “satask.txt commands” on page 38.)

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:
   ```
   satask mkcluster -clusterip aaa.aaa.aaa.aaa
   ```
   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:
   ```
   ```
   where you must replace **aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa** with the
   management IPv6 address, **gggg:gggg:gggg:gggg:gggg:gggg:gggg:gggg**
   with the network gateway IPv6 address, and **pp** with the prefix value.
   For other command options, see “Create system command” on page 41.
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.
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.

Procedure

To initialize a clustered system using the service assistant, complete the following steps.

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 passw0rd. If you cannot 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.

6. Point a supported browser to the management IP address that you specified to start the management GUI. The management GUI logon panel is displayed.

7. Log on as superuser. Use passw0rd for the password.

8. Follow the on-screen instructions.

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.

Procedure

Complete the following steps to access a canister using a directly attached Ethernet cable.

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. Get the service IP address of the node canister attached at step 1. If the service IP address is unknown, refer to “Problem: Node canister service IP address unknown” on page 46.

4. Use the operating system tools on the computer to set the IP address and subnet mask of the Ethernet port that is used in step 2. Set them to the same subnet of the node canister service IP address.

5. Point the web browser to the service IP address for the node canister.

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

7. Set the service address of the canister to one that can be accessed on the network as soon as possible.

8. Wait for the action to complete.

9. Disconnect your personal computer.

10. Reconnect the node canister to the Ethernet network.

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 52.
   - 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

You must power off your Storwize V7000 system in order to service it, or to permit other maintenance actions in your data center.

About this task

To power off your Storwize V7000 system, complete 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 svinfo 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.

iSCSI performance analysis and tuning

This procedure provides a solution for iSCSI host performance problems while connected to Storwize V7000 system, and its connectivity to the network switch.

About this task

Some of the attributes and host parameters that might affect iSCSI performance:

• Transmission Control Protocol (TCP) Delayed ACK
• Ethernet jumbo frame
• Network bottleneck or over subscription
• iSCSI session login balance

Procedure

1. Disable the TCP delayed acknowledgment feature.

To disable this feature, please refer to OS/platform documentation.

• VMWare: [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002598(TCP)]
• Windows: [http://support.microsoft.com/kb/823764]

The primary signature of this issue: read performance is significantly lower than write performance. Transmission Control Protocol (TCP) delayed acknowledgment is a technique used by some implementations of the TCP in an effort to improve network performance. However, in this scenario where the number of outstanding I/O is 1, the technique can significantly reduce I/O performance.
In essence, several ACK responses may be combined together into a single response, reducing protocol overhead. As described in RFC 1122, a host may delay sending an ACK response by up to 500 ms. Additionally, with a stream of full-sized incoming segments, ACK responses must be sent for every second segment.

**Important**: The host must be rebooted for these settings to take effect. A few platforms (for example, standard Linux distributions) do not provide a way to disable this feature. However, the issue has been resolved with the version 7.1 release, and no host configuration changes are required to manage ` TcpDelayedAck` behavior.

2. Enable jumbo frame for iSCSI.

   Jumbo frames are Ethernet frames with a size exceeding 1500 bytes. The maximum transmission unit (MTU) parameter is used to measure the size of jumbo frames.

   The Storwize V7000 supports 9000 bytes MTU. Refer to the CLI command `CFGPORTIP` to enable jumbo frame. This command is disruptive as the link flips and the I/O operation through that port will pause.

   The network must support jumbo frames end-to-end for this to be effective; verify this by sending a ping packet to be delivered without fragmentation. For example:

   - Windows:
     ```
     #ping -t <iscsi target ip> source <iscsi initiator ip> -f -l <new mtu size - 28>
     ```
   - Linux:
     ```
     #ping <iscsi target ip> source <iscsi initiator ip> -s <new mtu size - 28> -M do
     ```
   - ESXi:
     ```
     #ping <iscsi target ip> source <iscsi initiator ip> -s <new mtu size - 28> -d
     ```

3. Verify the switch’s port statistic where initiator/target ports are connected to make sure packet drops are not high.

   Review network architecture to avoid any bottlenecks and oversubscription. The network need to be balanced to avoid any packet drop; packet drop significantly reduces storage performance. Involve networking support to fix any such issues.

4. Optimize and utilize all iSCSI ports.

   To optimize Storwize V7000 resource utilization all iSCSI ports must be utilized.

   - If two ports of a node are used for iSCSI, lay out the network such that hosts are logged in to the required port.
   - Each port is assigned to one CPU, and by balancing the login, one can maximize CPU utilization and achieve better performance.
   - Avoid situations where 50 hosts are logged in to port 1 and only 5 host are logged in to port 2.
   - Use proper subnetting to achieve a balance between the number of sessions and redundancy.

---

**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.
Chapter 7. Recovery procedures

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
   - Recovering from offline VDisks (volumes) by using the CLI
   - Checking your system, for example, to ensure that all mapped volumes can access the host.
When to run the recover system procedure

Attempt a recover procedure 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 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 to know the number of control enclosures in the system. 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.

1. Check that no node in the cluster is active and that the management IP is not accessible from any other node. If this is the case, there is no need to recover the cluster.
2. Resolve all hardware errors in nodes so that only nodes 578 or 550 are present. If this is not the case, go to “Fix hardware errors.”
3. Ensure all backend-storage that is administered by cluster is present before you run the recover system procedure.
4. If any nodes have been replaced, ensure that the WWNN of the replacement node matches that of the replaced node, and that no prior system data remains on this node. (See “Procedure: Removing system data from a node canister” on page 59.)

Fix hardware errors

Before running a system recovery procedure, it is important to identify and fix the root cause of the hardware issues.

Identifying and fixing the root cause can help recover a system, if these are the faults that are causing the system to fail. The following are common issues which can be easily resolved:

• The node has been powered off or the power cords were unplugged.
• 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 11S serial number>]` (7 characters, colon, 1 or 2 numbers, open square bracket, 22 characters, close square bracket), for example, `01234A9:21[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 from the service assistant by clicking Restart Node.

- 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 verification, 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 verification, if the 550 error is still present, restart the node from the service assistant by clicking Restart Node.

- 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, verify:
  - There are at least two Fibre Channel ports that are operational and connected on every node.
  - The SAN zoning allows every port to connect to every port on every other node
  - All redundant SANs (if used) are operational.

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

**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. Call the IBM Support Center 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.

**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.

**Running 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.

**Before you begin**

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.
Note: Ensure that the web browser is not blocking pop-up windows. If it does, progress windows cannot open.

Before beginning this procedure, read the recover system procedure introductory information; see "Recover system procedure" on page 71.

About this task

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

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 can take significant time to complete, depending on the specific configuration.

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.
   b. 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

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” for details.

- **T3 failed**

Call IBM Support. Do not attempt any further action.

Verify the environment is operational by completing 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 VDisks (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 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” on page 77 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 completed before you use the system.

The recovery procedure recreates 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 these 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 (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.
- Intrasytem 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.
- Any Global Mirror secondary volumes on the recovered system might have inconsistent data if there was replication I/O from the primary volume cached on the secondary system at the point of the disaster. A full synchronization is required when recreating and restarting these remote copy relationships.

Before using the volumes, complete the following tasks:
- Start the host systems.
- Manual actions might be necessary on the hosts to trigger them to rescan for devices. You can complete 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 data to determine which
node canisters previously belonged in each I/O group.

Restoring the system configuration should be performed via one of the nodes
previously in I/O 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. Do this after any significant changes in configuration have been
made to the system.

**Note:** The system automatically creates a backup of the configuration data each
day at 1 AM. 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
might 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
might be possible to automatically recover the application data. This can be
attempted with the Recover System Procedure, also known as a Tier 3 (T3)
procedure. To restore the system configuration without attempting to recover the application data, use 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.

Complete 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 back up your configuration:

   `svcconfig backup`

   The following output is an example of the messages that might 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>svc.config.backup.xml_&lt;serial#&gt;</td>
<td>Contains your configuration data.</td>
</tr>
<tr>
<td>svc.config.backup.sh_&lt;serial#&gt;</td>
<td>Contains the names of the commands that were issued to create the backup of the system.</td>
</tr>
<tr>
<td>svc.config.backup.log_&lt;serial#&gt;</td>
<td>Contains details about the backup, including any reported errors or warnings.</td>
</tr>
</tbody>
</table>

3. 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.

4. 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 -unsafe 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 (passw0rd).

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, date 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, select No, do not 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. If the system you are restoring was previously configured in the replication layer, you must change the layer manually now. Refer to the System layers topic that is 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 from which you want to restore.
   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.

a. From the management GUI, click **Settings > Support**.

b. Click **Show full log listing**.

c. For each node (canister) in the system, complete the following steps:

   1) Select the node to operate on from the selection box at the top of the table.

   2) Find all the files with names matching the pattern `svc.config.*.xml*`.

   3) Double-click the files to download them 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. Copy onto the system the XML backup file from which you want to restore.

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

11. 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.

12. 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
```

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

14. Check the log file for errors.

   - If you find errors, correct the condition that caused the errors and reissue the command. You must correct all errors before you can proceed to step 15.

   - If an error indicates that the system layer will not be restored, then return to **7 on page 83**, configure the layer setting correctly, and then continue the restore process from step 10.

   - If you need assistance, contact the IBM Support Center.

15. 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`.

16. 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
```
17. Open the log file from the server where the copy is now stored.
18. 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>
   ```

19. 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:

```
svccfg 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:

   ```
   svcconfig clear -all
   ```
Chapter 8. Replacing parts

You can remove and replace customer-replaceable units (CRUs) in control enclosures or expansion enclosures.

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

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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 processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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: 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 52.
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). The handle with the finger grip on the left removes the lower canister (2).

![Figure 24. Rear of node canisters that shows the handles.](image)

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. Make sure that the canister is firmly and correctly seated, otherwise this can lead to problems.
   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 processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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).

![Figure 26. Rear of expansion canisters that shows the handles.](image)

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. Make sure that the canister is firmly and correctly seated, otherwise this can lead to problems.
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 components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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:
  - If IBM supplied a power cord(s), 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 processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of 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 components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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 unit using the switch at the back.
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.
b. **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:

- If IBM supplied a power cord(s), 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 processing I/O operations, go to the
management GUI and follow the fix procedures. Initiating the replacement actions
without the assistance of the fix procedures can result in loss of data or loss of
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 components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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 unit using the switch at the back of the unit.
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:
  - If IBM supplied a power cord(s), 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.

(C007)
Attention: If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating 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 90.

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.

Figure 33. Removing the battery from the control enclosure power-supply unit
1. 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. Initiating the replacement actions without the assistance of the fix procedures results in loss of data or loss of 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.

Figure 34. Unlocking the 3.5" drive

3. Open the handle to the full extension.

Figure 35. Removing the 3.5" drive

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 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. Initiating the replacement actions without the assistance of the fix procedures results in loss of data or loss of 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.

Figure 36. Unlocking the 2.5" drive
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

You can remove and replace enclosure end caps.

About this task

Attention: The left end cap is printed with information that helps identify the enclosure.
- Machine type and model
- Enclosure serial number
- 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.

Procedure

To remove and replace either the left or right end cap, complete the following steps.
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.
4. Fit the slot on the top of the new end cap over the tab on the top of the chassis flange.
5. Rotate the end cap down until it snaps into place. Ensure that the inside surface of the end cap is flush with the chassis.

## 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:

- If IBM supplied a power cord(s), 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:
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:

- If IBM supplied a power cord(s), 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 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, 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 24 on page 117 provides a brief description of each replaceable unit.
Table 24. Replaceable units

<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 drive, in carrier assembly</td>
<td>85Y5864</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 15 K, 146 GB drive, in carrier assembly</td>
<td>85Y6088</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 15 K, 300 GB drive, in carrier assembly</td>
<td>85Y6185</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 900 GB drive, in carrier assembly</td>
<td>00L4680</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 300 GB drive, in carrier assembly</td>
<td>85Y6256</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 600 GB drive, in carrier assembly</td>
<td>85Y6268</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 10 K, 900 GB drive, in carrier assembly</td>
<td>85Y6274</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” 7.2 K, Nearline SAS, 1 TB drive, in carrier assembly</td>
<td>85Y6186</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” SSD, 200 GB drive, in carrier assembly</td>
<td>85Y6188</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>2.5” SSD, 400 GB drive, in carrier assembly</td>
<td>85Y6189</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>
</tbody>
</table>
Table 24. Replaceable units (continued)

<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>3.5&quot; 7.2 K Nearline SAS - 3 TB in carrier assembly</td>
<td>85Y6187</td>
<td>112, 212, 312</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Blank 2.5&quot; carrier</td>
<td>85Y5893</td>
<td>124, 224, 324</td>
<td>Customer replaced</td>
</tr>
<tr>
<td>Blank 3.5&quot; 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>85Y5852</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 on an IP network by using the syslog protocol.
• If enabled, event notifications can be forwarded by email by using Simple Mail Transfer Protocol (SMTP).
• Call Home can be enabled so that critical faults generate a problem management record (PMR) that is then sent directly to the appropriate IBM Support Center by using email.

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 (lsentlog). 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 25 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

Storwize V7000 can use Simple Network Management Protocol (SNMP) traps, syslog messages, emails and Call Homes to notify you and IBM(r) Remote Technical Support 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 26 describes the levels of event notifications.

<table>
<thead>
<tr>
<th>Notification level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error</strong></td>
<td>Error notification is sent to indicate a problem that must be corrected as soon as possible. This notification indicates a serious problem with the system. 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. Error notifications can be configured to be sent as a Call Home to the IBM Remote Technical Support.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>A warning notification is sent to indicate a problem or unexpected condition with the system. 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 Error.</td>
</tr>
<tr>
<td><strong>Information</strong></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, a failing component, 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, informational event notifications can be sent 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 event notifications can be sent 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, based on notification type, 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 27** provides a list of informational events, the notification type, and the reason for the event.

**Table 27. 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>
<tr>
<td>Event ID</td>
<td>Notification type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<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>
</tbody>
</table>
Table 27. Informational events (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Notification type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 27. 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 28 lists the event IDs and corresponding error codes, the notification type, and the condition of the event.

Table 28. 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>
</tbody>
</table>
Table 28. 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>009052</td>
<td>W</td>
<td>The following causes are possible:</td>
<td>1196</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The node is missing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The node is no longer a functional member of the system.</td>
<td></td>
</tr>
<tr>
<td>009053</td>
<td>E</td>
<td>A node has been missing for 30 minutes.</td>
<td>1195</td>
</tr>
<tr>
<td>009100</td>
<td>W</td>
<td>The software install process has failed.</td>
<td>2010</td>
</tr>
<tr>
<td>009101</td>
<td>W</td>
<td>The software upgrade package delivery has failed.</td>
<td>2010</td>
</tr>
<tr>
<td>009150</td>
<td>W</td>
<td>Unable to connect to the SMTP (email) server</td>
<td>2600</td>
</tr>
<tr>
<td>009151</td>
<td>W</td>
<td>Unable to send mail through the SMTP (email) server</td>
<td>2601</td>
</tr>
<tr>
<td>009170</td>
<td>W</td>
<td>The Metro Mirror or Global Mirror feature capacity is not set.</td>
<td>3030</td>
</tr>
<tr>
<td>009171</td>
<td>W</td>
<td>The FlashCopy feature capacity is not set.</td>
<td>3031</td>
</tr>
<tr>
<td>009172</td>
<td>W</td>
<td>The Virtualization feature has exceeded the amount that is licensed.</td>
<td>3032</td>
</tr>
<tr>
<td>009173</td>
<td>W</td>
<td>The FlashCopy feature capacity has exceeded the amount that is licensed.</td>
<td>3032</td>
</tr>
<tr>
<td>009174</td>
<td>W</td>
<td>The Metro Mirror or Global Mirror feature has exceeded the amount that is licensed.</td>
<td>3032</td>
</tr>
<tr>
<td>009175</td>
<td>W</td>
<td>The usage for the thin-provisioned volume is not licensed.</td>
<td>3033</td>
</tr>
<tr>
<td>009176</td>
<td>W</td>
<td>The value set for the virtualization feature capacity is not valid.</td>
<td>3029</td>
</tr>
<tr>
<td>009177</td>
<td>E</td>
<td>A physical disk FlashCopy feature license is required.</td>
<td>3035</td>
</tr>
<tr>
<td>009178</td>
<td>E</td>
<td>A physical disk Metro Mirror and Global Mirror feature license is required.</td>
<td>3036</td>
</tr>
<tr>
<td>009179</td>
<td>E</td>
<td>A virtualization feature license is required.</td>
<td>3025</td>
</tr>
<tr>
<td>009180</td>
<td>E</td>
<td>Automatic recovery of offline node failed.</td>
<td>1194</td>
</tr>
<tr>
<td>009181</td>
<td>W</td>
<td>Unable to send email to any of the configured email servers.</td>
<td>3081</td>
</tr>
<tr>
<td>009182</td>
<td>W</td>
<td>The external virtualization feature license limit was exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009183</td>
<td>W</td>
<td>Unable to connect to LDAP server.</td>
<td>2251</td>
</tr>
<tr>
<td>009184</td>
<td>W</td>
<td>The LDAP configuration is not valid.</td>
<td>2250</td>
</tr>
<tr>
<td>009185</td>
<td>E</td>
<td>The limit for the compression feature license was exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009186</td>
<td>E</td>
<td>The limit for the compression feature license was exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009187</td>
<td>E</td>
<td>Unable to connect to LDAP server that has been automatically configured.</td>
<td>2256</td>
</tr>
<tr>
<td>009188</td>
<td>E</td>
<td>Invalid LDAP configuration for automatically configured server.</td>
<td>2255</td>
</tr>
<tr>
<td>009189</td>
<td>W</td>
<td>A licensable feature’s trial-timer has reached 0. The feature has now been deactivated.</td>
<td>3082</td>
</tr>
<tr>
<td>009190</td>
<td>W</td>
<td>A trial of a licensable feature will expire in 5 days.</td>
<td>3083</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>009191</td>
<td>W</td>
<td>A trial of a licensable feature will expire in 10 days.</td>
<td>3084</td>
</tr>
<tr>
<td>009192</td>
<td>W</td>
<td>A trial of a licensable feature will expire in 15 days.</td>
<td>3085</td>
</tr>
<tr>
<td>009193</td>
<td>W</td>
<td>A trial of a licensable feature will expire in 45 days.</td>
<td>3086</td>
</tr>
<tr>
<td>009194</td>
<td>W</td>
<td>Easy Tier feature license limit exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009195</td>
<td>W</td>
<td>FlashCopy feature license limit exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009196</td>
<td>W</td>
<td>External virtualization feature license limit exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>009197</td>
<td>W</td>
<td>Remote copy feature license limit exceeded.</td>
<td>3032</td>
</tr>
<tr>
<td>010002</td>
<td>E</td>
<td>The node ran out of base event sources. As a result, the node has stopped and exited the system.</td>
<td>2030</td>
</tr>
<tr>
<td>010003</td>
<td>W</td>
<td>The number of device logins has reduced.</td>
<td>1630</td>
</tr>
<tr>
<td>010006</td>
<td>E</td>
<td>A software error has occurred.</td>
<td>2030</td>
</tr>
<tr>
<td>010008</td>
<td>E</td>
<td>The block size is invalid, the capacity or LUN identity has changed during the managed disk initialization.</td>
<td>1660</td>
</tr>
<tr>
<td>010010</td>
<td>E</td>
<td>The managed disk is excluded because of excessive errors.</td>
<td>1310</td>
</tr>
<tr>
<td>010011</td>
<td>E</td>
<td>The remote port is excluded for a managed disk and node.</td>
<td>1220</td>
</tr>
<tr>
<td>010012</td>
<td>E</td>
<td>The local port is excluded.</td>
<td>1210</td>
</tr>
<tr>
<td>010013</td>
<td>E</td>
<td>The login is excluded.</td>
<td>1230</td>
</tr>
<tr>
<td>010014</td>
<td>E</td>
<td>The local port is excluded.</td>
<td>1211</td>
</tr>
<tr>
<td>010017</td>
<td>E</td>
<td>A timeout has occurred as a result of excessive processing time.</td>
<td>1340</td>
</tr>
<tr>
<td>010018</td>
<td>E</td>
<td>An error recovery procedure has occurred.</td>
<td>1370</td>
</tr>
<tr>
<td>010019</td>
<td>E</td>
<td>A managed disk I/O error has occurred.</td>
<td>1310</td>
</tr>
<tr>
<td>010020</td>
<td>E</td>
<td>The managed disk error count threshold has exceeded.</td>
<td>1310</td>
</tr>
<tr>
<td>010021</td>
<td>W</td>
<td>There are too many devices presented to the clustered system.</td>
<td>1200</td>
</tr>
<tr>
<td>010022</td>
<td>W</td>
<td>There are too many managed disks presented to the cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010023</td>
<td>W</td>
<td>There are too many LUNs presented to a node.</td>
<td>1200</td>
</tr>
<tr>
<td>010024</td>
<td>W</td>
<td>There are too many drives presented to a cluster (system).</td>
<td>1200</td>
</tr>
<tr>
<td>010025</td>
<td>W</td>
<td>A disk I/O medium error has occurred.</td>
<td>1320</td>
</tr>
<tr>
<td>010026</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</td>
<td>W</td>
<td>The quorum disk is not available.</td>
<td>1335</td>
</tr>
<tr>
<td>010028</td>
<td>W</td>
<td>A controller configuration is not supported.</td>
<td>1625</td>
</tr>
<tr>
<td>010029</td>
<td>E</td>
<td>A login transport fault has occurred.</td>
<td>1360</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>010030</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</td>
<td>E</td>
<td>One or more MDisks on a controller are degraded.</td>
<td>1623</td>
</tr>
<tr>
<td>010032</td>
<td>W</td>
<td>The controller configuration limits failover.</td>
<td>1625</td>
</tr>
<tr>
<td>010033</td>
<td>E</td>
<td>The controller configuration uses the RDAC mode; this is not supported.</td>
<td>1624</td>
</tr>
<tr>
<td>010034</td>
<td>E</td>
<td>Persistent unsupported controller configuration.</td>
<td>1695</td>
</tr>
<tr>
<td>010040</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</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</td>
<td>E</td>
<td>The controller system device is only connected to the clustered system nodes through a single target port.</td>
<td>1627</td>
</tr>
<tr>
<td>010043</td>
<td>E</td>
<td>The controller system device is only connected to the clustered 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 clustered 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>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>Event</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>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 clustered 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>
<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>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>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>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 unity has indicated an output 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>
</tbody>
</table>
Table 28. 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>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>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>
</tbody>
</table>
Table 28. 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>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>
<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 clustered 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 clustered 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>050050</td>
<td>W</td>
<td>The Global Mirror secondary volume is offline. The relationship has pinned hardened write data for this volume.</td>
<td>1925</td>
</tr>
<tr>
<td>050060</td>
<td>W</td>
<td>The Global Mirror secondary volume is offline due to missing I/O group partner node. The relationship has pinned hardened write data for this volume but the node containing the required data is currently offline.</td>
<td>1730</td>
</tr>
<tr>
<td>050070</td>
<td>W</td>
<td>Global Mirror performance is likely to be impacted. A large amount of pinned data for the offline volumes has reduced the resource available to the global mirror secondary disks.</td>
<td>1925</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>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>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>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 clustered 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 clustered system data cannot be read.</td>
<td>1030</td>
</tr>
<tr>
<td>070578</td>
<td>E</td>
<td>The clustered 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>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>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>Clustered 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>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>
<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>Clustered 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 clustered 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>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 clustered system data cannot be read.</td>
<td>1187</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>073578</td>
<td>E</td>
<td>The clustered system data was not saved when power was lost.</td>
<td>1194</td>
</tr>
<tr>
<td>073651</td>
<td>E</td>
<td>The canister battery is missing.</td>
<td>1153</td>
</tr>
<tr>
<td>073652</td>
<td>E</td>
<td>The canister battery has failed.</td>
<td>1154</td>
</tr>
<tr>
<td>073653</td>
<td>E</td>
<td>The canister battery’s temperature is too low.</td>
<td>1156</td>
</tr>
<tr>
<td>073654</td>
<td>E</td>
<td>The canister battery’s temperature is too high</td>
<td>1157</td>
</tr>
<tr>
<td>073655</td>
<td>E</td>
<td>The canister battery communications fault.</td>
<td>1158</td>
</tr>
<tr>
<td>073656</td>
<td>E</td>
<td>The canister battery has insufficient charge.</td>
<td>1184</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>
<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. This is probably because a new FRU has been installed and the software does not recognize that FRU. The clustered system continues to operate; however, you must upgrade the software to fix this warning.</td>
<td>2040</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 because of a connectivity problem.</td>
<td>1715</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>074004</td>
<td>W</td>
<td>A connection to a configured remote system has been lost because of too many minor errors.</td>
<td>1716</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 output.</td>
<td>2030</td>
</tr>
<tr>
<td>076401</td>
<td>E</td>
<td>One of the two power supply units in the node has failed.</td>
<td>1096</td>
</tr>
<tr>
<td>076402</td>
<td>E</td>
<td>One of the two power supply units in the node cannot be detected.</td>
<td>1096</td>
</tr>
<tr>
<td>076403</td>
<td>E</td>
<td>One of the two power supply units in the node is without power.</td>
<td>1097</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 adapter.</td>
<td>1121</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>
<tr>
<td>079500</td>
<td>W</td>
<td>The limit on the number of clustered 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 29 on page 141 lists the number range for each message classification.
### Table 29. Message classification number range

<table>
<thead>
<tr>
<th>Message classification</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node errors</td>
<td>Critical node errors: 500-699 Some critical errors might be accompanied by error codes 1021, 1036, 1188, and 1189.</td>
</tr>
<tr>
<td></td>
<td>Noncritical node errors: 700-899</td>
</tr>
<tr>
<td>Error codes when recovering a clustered system</td>
<td>920, 990</td>
</tr>
</tbody>
</table>

**100 Boot is running**

**Explanation:** The SAN Volume Controller node has started. It is running diagnostics and loading the runtime code.

**User response:** Go to the hardware boot MAP to resolve the problem.

Possible Cause-FRUs or other:
- 2145-CG8 or 2145-CF8
  - Service controller (47%)
  - Service controller cable (47%)
  - System board assembly (6%)

- 2145-8G4 or 2145-8A4
  - Service controller (95%)
  - System board (5%)

**120 Disk drive hardware error**

**Explanation:** The internal disk drive of the node has reported an error. The node is unable to start.

**User response:** Ensure that the boot disk drive and all related cabling is properly connected, then exchange the FRU for a new FRU. (See “Possible Cause-FRUs or other.”)

Possible Cause-FRUs or other:
- 2145-CF8 or 2145-CG8
  - Disk drive (50%)
  - Disk controller (30%)
  - Disk backplane (10%)
  - Disk signal cable (8%)
  - Disk power cable (1%)
  - System board (1%)

- 2145-8G4 or 2145-8A4
  - Disk drive assembly (95%)
  - Disk cable assembly (4%)
  - System board (1%)

**130 Checking the internal disk file system**

**Explanation:** The file system on the internal disk drive of the node is being checked for inconsistencies.

**User response:** If the progress bar has been stopped for at least five minutes, power off the node and then power on the node. If the boot process stops again at this point, run the node rescue procedure.

Possible Cause-FRUs or other:
- None.

**132 Updating BIOS settings of the node**

**Explanation:** The system has found that changes are required to the BIOS settings of the node. These changes are being made. The node will restart once the changes are complete.

**User response:** If the progress bar has stopped for more than 10 minutes, or if the display has shown codes 100 and 132 three times or more, go to MAP 5900: Hardware boot to resolve the problem.

**135 Verifying the software**

**Explanation:** The software packages of the node are being checked for integrity.

**User response:** Allow the verification process to complete.

**137 Updating system board service processor firmware**

**Explanation:** The service processor firmware of the node is being updated to a new level. This process can take 90 minutes. Do not restart the node while this is in progress.

**User response:** Allow the updating process to complete.

**150 Loading cluster code**

**Explanation:** The SAN Volume Controller code is being loaded.
If the progress bar has been stopped for at least 90 seconds, power off the node and then power on the node. If the boot process stops again at this point, run the node rescue procedure.

Possible Cause-FRUs or other:
- None.

**155 Loading cluster data**

**Explanation:** The saved cluster state and cache data is being loaded.

**User response:** If the progress bar has been stopped for at least 5 minutes, power off the node and then power on the node. If the boot process stops again at this point, run the node rescue procedure.

Possible Cause-FRUs or other:
- None.

**150 Updating the service controller**

**Explanation:** The firmware on the service controller is being updated. This can take 30 minutes.

**User response:** When a node rescue is occurring, if the progress bar has been stopped for at least 30 minutes, exchange the FRU for a new FRU. When a node rescue is not occurring, if the progress bar has been stopped for at least 15 minutes, exchange the FRU for a new FRU.

Possible Cause-FRUs or other:
- 2145-CG8 or 2145-CF8
- Service controller (95%)
- Service controller cable (5%)

All previous 2145 models
- Service controller (100%)

**160 Checking uninterruptible power supply**

**Explanation:** The node is checking whether the uninterruptible power supply is operating correctly.

**User response:** Allow the checking process to complete.

**232 Checking uninterruptible power supply connections**

**Explanation:** The node is checking whether the power and signal cable connections to the uninterruptible power supply are correct.

**User response:** Allow the checking process to complete.

**300 The 2145 is running node rescue.**

**Explanation:** The 2145 is running node rescue.

**User response:** If the progress bar has been stopped for at least two minutes, exchange the FRU for a new FRU.

Possible Cause-FRUs or other:
- 2145-CG8 or 2145-CF8
- Service controller (95%)
- Service controller cable (5%)

All previous 2145 models
- Service controller (100%)

**310 The 2145 is running a format operation.**

**Explanation:** The 2145 is running a format operation.

**User response:** If the progress bar has been stopped for two minutes, exchange the FRU for a new FRU.

Possible Cause-FRUs or other:
- 2145-CG8 or 2145-CF8
- Disk drive (50%)
- Disk controller (30%)
- Disk backplane (10%)
- Disk signal cable (8%)
- Disk power cable (1%)
- System board (1%)
320  A 2145 format operation has failed.
Explanation:  A 2145 format operation has failed.
User response:  Exchange the FRU for a new FRU.
Possible Cause-FRUs or other:
2145-CG8 or 2145-CF8
• Disk drive (50%)
• Disk controller (30%)
• Disk backplane (10%)
• Disk signal cable (8%)
• Disk power cable (1%)
• System board (1%)

2145-8G4 or 2145-8A4
• Disk drive assembly (90%)
• Disk cable assembly (10%)

330  The 2145 is partitioning its disk drive.
Explanation:  The 2145 is partitioning its disk drive.
User response:  If the progress bar has been stopped for two minutes, exchange the FRU for a new FRU.
Possible Cause-FRUs or other:
2145-CG8 or 2145-CF8
• Disk drive (50%)
• Disk controller (30%)
• Disk backplane (10%)
• Disk signal cable (8%)
• Disk power cable (1%)
• System board (1%)

2145-8G4 or 2145-8A4
• Disk drive assembly (90%)
• Disk cable assembly (10%)

Other:
• Configuration problem
• Software error

340  The 2145 is searching for donor node.
Explanation:  The 2145 is searching for a donor node from which to copy the software.
User response:  If the progress bar has stopped for more than two minutes, exchange the FRU for a new FRU.
Possible Cause-FRUs or other:
• Fibre Channel adapter (100%)

345  The 2145 is searching for a donor node.
Explanation:  The node is searching at 1 Gb/s for a donor node.
User response:  If the progress bar has stopped for more than two minutes, exchange the FRU for a new FRU.
Possible Cause-FRUs or other:
• Fibre Channel adapter (100%)

350  The 2145 cannot find a donor node.
Explanation:  The 2145 cannot find a donor node.
User response:  If the progress bar has stopped for more than two minutes, perform the following steps:
1. Ensure that all of the Fibre Channel cables are connected correctly and securely to the cluster.
2. Ensure that at least one other node is operational, is connected to the same Fibre Channel network, and is a donor node candidate. A node is a donor node candidate if the version of software that is installed on that node supports the model type of the node that is being rescued.
3. Ensure that the Fibre Channel zoning allows a connection between the node that is being rescued and the donor node candidate.
4. Perform the problem determination procedures for the network.

Possible Cause-FRUs or other:
• None

Other:
• Fibre Channel network problem

360  The 2145 is loading software from the donor.
Explanation:  The 2145 is loading software from the donor.
User response:  If the progress bar has been stopped for at least two minutes, restart the node rescue procedure.
Possible Cause-FRUs or other:
• None

365  Cannot load SW from donor
Explanation:  None.
User response:  None.
370 Installing software

Explanation: The 2145 is installing software.

User response:
1. If this code is displayed and the progress bar has been stopped for at least ten minutes, the software install process has failed with an unexpected software error.
2. Power off the 2145 and wait for 60 seconds.
3. Power on the 2145. The software upgrade operation continues.
4. Report this problem immediately to your Software Support Center.

Possible Cause-FRUs or other:
• None

500 Incorrect enclosure

Explanation: The node canister has saved cluster information, which indicates that the canister is now located in a different enclosure from where it was previously used. Using the node canister in this state might corrupt the data held on the enclosure drives.

User response: Follow troubleshooting procedures to move the 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 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 data. See Procedure: Getting node canister and system information using the service assistant on page 53.
2. If you have unintentionally moved the canister into this enclosure, move the canister back to its original location, and put the original canister back in this enclosure. Follow the Replacing a node canister procedure on page 85.
3. If you have intentionally moved the node canister into this enclosure you should check it is safe to continue or whether you will lose data on the enclosure you removed it from. Do not continue if the system the node canister was removed from is offline, rather return the node canister to that system.
4. If you have determined it is alright to continue, follow the procedure to remove cluster data from node canister. See Procedure: Removing system data from a node canister on page 59.
5. If the partner node in this enclosure is not online, or is not present, you will have to perform a system recovery. Do not create a new system, you will lose all the volume data.

Possible Cause-FRUs or other cause:
• None

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 and the status of the other 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 procedure on page 85 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 cause:
• 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:
- Enclosure midplane (100%)

---

503 Incorrect enclosure type

Explanation: The node canister has been moved to an expansion enclosure. A node canister will not operate in this environment.

User response: Follow troubleshooting procedures to relocate the nodes to the correct location.

1. Follow the procedure: Getting node canister and system information using a USB flash drive and review the saved location information of the node canister to determine which control enclosure the node canister should be in. See “Procedure: Getting node canister and system information using a USB flash drive” on page 53.

2. Follow the procedure Replacing a node canister to move the node canister to the correct location, and follow the procedure Replacing an expansion canister to move the expansion canister, that is probably in that location, to here. If there is a node canister that is in active state where this node canister should be, do not replace that node canister with this one.

---

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 data. See “Procedure: Getting node canister and system information using the service assistant” on page 53.

2. Decide what to do with the node canister that did not come from the enclosure that is being replaced.
   a. If the other node canister from the enclosure being replaced is available, use the hardware remove and replace canister procedures to remove the incorrect canister and replace it with the second node canister from the enclosure being replaced. Restart both canisters. The two node canister should show node error 504 and the actions for that error should be followed.
   b. If the other node canister from the enclosure being replaced is not available, check the enclosure of the node canister that did not come from the replaced enclosure. Do not use this canister in this enclosure if you require the volume data on the system from which the node canister was removed, and that system is not running with two online nodes. You should return the canister to its original enclosure and use a different canister in this enclosure.
   c. When you have checked that it is not required elsewhere, follow the procedure to remove cluster data from the node canister that did not come from the enclosure that is being replaced. See “Procedure: Removing system data from a node canister” on page 59. Restart both nodes. Expect node error 506 to now be reported, and follow the service procedures for that error.

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 85 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.

3. If you are sure this node canister came from the enclosure that is being replaced, and that the original partner canister has failed, continue following the remove and replace procedure for an enclosure midplane and configure the new enclosure.

Possible Cause—FRUs or other:

* None

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 “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” on page 85 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 canister, 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:
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). A series of values indicates the amount of memory (in GB) detected in each memory slot.

<table>
<thead>
<tr>
<th>Data:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected memory on MB</td>
<td></td>
</tr>
<tr>
<td>Minimum required memory in MB</td>
<td></td>
</tr>
<tr>
<td>Memory in slot 1 in GB</td>
<td></td>
</tr>
<tr>
<td>Memory in slot 2 in GB</td>
<td></td>
</tr>
<tr>
<td>... etc.</td>
<td></td>
</tr>
</tbody>
</table>

**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 (50%)

---

512  Enclosure VPD is inconsistent

**Explanation:** The enclosure midplane VPD is not consistent. The machine part number is not compatible with the machine type and model. This indicates that the enclosure VPD is corrupted.

**User response:**
1. Check the support site for a code update.
2. Use the remove and replace procedures to replace the enclosure midplane.

Possible Cause—FRUs or other:
* Enclosure midplane (100%)

---

517  The WWNNs of the service controller and the disk do not match.

**Explanation:** The node is unable to determine the WWNN that it should use. This is because of the service controller or the nodes internal drive being replaced.

**User response:** Follow troubleshooting procedures to configure the WWNN of the node.
1. Continue to follow the hardware remove and replace procedure for the service controller or disk these explain the service actions.
2. If you have not followed the hardware remove and replace procedures, you should determine the correct WWNN. If you do not have this information recorded, examine your Fibre Channel switch configuration to see whether it is listed there. Follow the procedures to change the WWNN of a node.

Possible Cause—FRUs or other:
* None

---

521  Unable to detect a Fibre Channel adapter

**Explanation:** The 2145 cannot detect any Fibre Channel adapter cards.

**User response:** Ensure that a Fibre Channel adapter card has been installed. Ensure that the Fibre Channel card is seated correctly in the riser card. Ensure that the riser card is seated correctly on the system board. If the problem persists, exchange FRUs for new FRUs in the order shown.

Possible Cause—FRUs or other:
* 2145-CG8 or 2145-CF8
  * 4-port Fibre Channel host bus adapter assembly (95%)
  * System board assembly (5%)
* 2145-8G4 or 2145-8A4
  * 4-port Fibre Channel host bus adapter (80%)
  * Riser card (19%)
  * System board (1%)
  * 4-port Fibre Channel host bus adapter (99%)
  * Frame assembly (1%)

---

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.

---

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%)

524 Unable to update BIOS settings.

Explanation: Unable to update BIOS settings.
User response: Power off node, wait 30 seconds, and then power on again. If the error code is still reported, replace the system board.

Possible Cause—FRUs or other:
• System board (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%)

528 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%)

530 A problem with one of the node's power supplies has been detected.

Explanation: The 530 error code is followed by two numbers. The first number is either 1 or 2 to indicate which power supply has the problem.
The second number is either 1, 2 or 3 to indicate the reason. 1 indicates that the power supply is not detected. 2 indicates that the power supply has failed. 3 indicates that there is no input power to the power supply.

If the node is a member of a cluster, the cluster will report error code 1096 or 1097, depending on the error reason.
The error will automatically clear when the problem is fixed.

User response:
1. Ensure that the power supply is seated correctly and that the power cable is attached correctly to both the node and to the 2145 UPS-1U.
2. If the error has not been automatically marked fixed after two minutes, note the status of the three LEDs on the back of the power supply. For the 2145-CG8 or 2145-CF8, the AC LED is the top green LED, the DC LED is the middle green LED and the error LED is the bottom amber LED.
3. If the power supply error LED is off and the AC and DC power LEDs are both on, this is the normal condition. If the error has not been automatically fixed after two minutes, replace the system board.
4. Follow the action specified for the LED states noted in the table below.
5. If the error has not been automatically fixed after two minutes, contact support.

Error, AC, DC: Action

ON, ON or OFF, ON or OFF: The power supply has a fault. Replace the power supply.

OFF, OFF, OFF: There is no power detected. Ensure that the power cable is connected at the node and 2145 UPS-1U. If the AC LED does not light, check whether the 2145 UPS-1U is showing any errors. Follow MAP 5150 2145 UPS-1U if the UPS-1U is showing an error; otherwise, replace the power cable. If the AC LED still does not light, replace the power supply.

OFF, OFF, ON: The power supply has a fault. Replace the power supply.

OFF, ON, OFF: Ensure that the power supply is installed correctly. If the DC LED does not light, replace the power supply.

Possible Cause—FRUs or other:
Reason 1: A power supply is not detected.
- Power supply (19%)
- System board (1%)
- Other: Power supply is not installed correctly (80%)

Reason 2: The power supply has failed.
- Power supply (90%)
- Power cable assembly (5%)
- System board (5%)

Reason 3: There is no input power to the power supply.
- Power cable assembly (25%)
- UPS-1U assembly (4%)
- System board (1%)
- Other: Power supply is not installed correctly (70%)

535  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 64.
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%)

541  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.

550  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 enclosure:slot[part identification] where enclosure: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 WWWWWWWWWWWWWWWWW/LL, where WWWWWWWWWWWWWWWWW 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
diagnostics the system provides to diagnose problems on SAS cables and expansion enclosures.

5. If a quorum disk on an external storage system is shown as missing, find the storage control and confirm that the LUN is available, check the Fibre Channel connections between the storage controller and the 2076 are working and that any changes made to the SAN configuration and zoning have not effected the connectivity. Check the status of the Fibre Channel ports on the node and resolve any issues.

6. If a quorum disk on an external storage system is shown as missing, find the storage control and confirm that the LUN is available, check the Fibre Channel connections between the storage controller and the system are working and that any changes made to the SAN configuration and zoning have not effected the connectivity. Check the status of the Fibre Channel ports on the canister and resolve any issues.

7. If all canisters have either node error 578 or 550, attempt to reestablish a cluster by following the service procedures for the nodes showing node error 578. If this is not successful, follow the cluster recovery procedures.

---

### 551

**A cluster cannot be formed because of a lack of cluster resources.**

---

### 555

**Power Domain error**

**Explanation:** Both 2145s in an I/O group are being powered by the same uninterruptible power supply. The ID of the other 2145 is displayed with the node error code on the front panel.

**User response:** Ensure that the configuration is correct and that each 2145 is in an I/O group is connected from a separate uninterruptible power supply.

---

### 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 same WWNN 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 has 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.

---

### 558

**The node is unable to communicate with other nodes.**

**Explanation:** The 2145 cannot see the Fibre Channel fabric or the Fibre Channel card port speed might be set to a different speed than the Fibre Channel fabric.

**User response:** Ensure that:

1. The Fibre Channel network fabric switch is powered-on.
2. At least one Fibre Channel cable connects the 2145 to the Fibre Channel network fabric.
3. The Fibre Channel card port speed is equal to the Fibre Channel fabric.
4. At least one Fibre Channel adapter is installed in the 2145.
5. Go to the Fibre Channel MAP.

Possible Cause—FRUs or other:

- None

**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 machine code on the node.

**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

**573** The node machine code is inconsistent.

**Explanation:** Parts of the node machine code package are receiving unexpected results; there may be an inconsistent set of subpackages installed, or one subpackage may be damaged.

**User response:** Follow troubleshooting procedures to reload the machine code:
1. Follow the procedure to run a node rescue.
2. If the error occurs again, contact IBM technical support.

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:
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

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 correct 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.
   b. Or use the CLI to `satask leavecluster`.

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

The service controller ID could not be read.

**Explanation:** The 2145 cannot read the unique ID from the service controller, so the Fibre Channel adapters cannot be started.

**User response:** In the sequence shown, exchange the following FRUs for new FRUs.

Possible Cause-FRUs or other:

2145-CG8 or 2145-CF8
- Service controller (70%)
- Service controller cable (30%)

2145-8G4 or 2145-8A4

Service controller (100%)

Other:

- None

A serial link error in the 2145 UPS-1U has occurred.

**Explanation:** There is a fault in the communications cable, the serial interface in the uninterruptible power supply 2145 UPS-1U, or 2145.

**User response:** Check that the communications cable is correctly plugged in to the 2145 and the 2145 UPS-1U. If the cable is plugged in correctly, replace the FRUs in the order shown.

Possible Cause-FRUs or other:

2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
- 2145 power cable assembly (40%)
- 2145 UPS-1U assembly (30%)
- 2145 system board (30%)

A battery error in the 2145 UPS-1U has occurred.

**Explanation:** A problem has occurred with the uninterruptible power supply 2145 UPS-1U battery.

**User response:** Exchange the FRU for a new FRU. After replacing the battery assembly, if the 2145 UPS-1U service indicator is on, press and hold the 2145 UPS-1U Test button for three seconds to start the self-test and verify the repair. During the self-test, the rightmost four LEDs on the 2145 UPS-1U front-panel assembly flash in sequence.

Possible Cause-FRUs or other:

- UPS-1U battery assembly (50%)
- UPS-1U assembly (50%)

An electronics error in the 2145 UPS-1U has occurred.

**Explanation:** A problem has occurred with the 2145 UPS-1U electronics.

**User response:** Exchange the FRU for a new FRU.

Possible Cause-FRUs or other:

- 2145 UPS-1U assembly
**584** The 2145 UPS-1U is overloaded.

**Explanation:** A problem with output overload has been reported by the uninterruptible power supply 2145 UPS-1U. The Overload Indicator on the 2145 UPS-1U front panel is illuminated red.

**User response:**
1. Ensure that only one 2145 is receiving power from the 2145 UPS-1U. Also ensure that no other devices are connected to the 2145 UPS-1U.
2. Disconnect the 2145 from the 2145 UPS-1U. If the Overload Indicator is still illuminated, on the disconnected 2145 replace the 2145 UPS-1U.
3. If the Overload Indicator is now off, and the node is a 2145-8G4 or 2145-8A4, on the disconnected 2145, with all outputs disconnected, in the sequence shown, exchange the FRUs for new FRUs.
4. If the Overload Indicator is now off, and the node is a 2145-8G8 or 2145-8C8, on the disconnected 2145, with all outputs disconnected, determine whether it is one of the two power supplies or the power cable assembly that must be replaced. Plug just one power cable into the left hand power supply and start the node and see whether the error is reported. Then shut down the node and connect the other power cable into the left hand power supply and start the node and see whether the error is repeated. Then repeat the two tests for the right hand power supply. If the error is repeated for both cables on one power supply but not the other, replace the power supply that showed the error; otherwise, replace the power cable assembly.

Possible Cause-FRUs or other:
- Power cable assembly (45%)
- Power supply assembly (45%)
- UPS-1U assembly (10%)

**586** The power supply to the 2145 UPS-1U does not meet requirements.

**Explanation:** None.

**User response:** Follow troubleshooting procedures to fix the hardware.

**587** An incorrect type of uninterruptible power supply has been detected.

**Explanation:** An incorrect type of 2145 UPS-1U was installed.

**User response:** Exchange the 2145 UPS-1U for one of the correct type.

Possible Cause-FRUs or other:
- 2145 UPS-1U (100%)

**588** The 2145 UPS-1U is not cabled correctly.

**Explanation:** The signal cable or the 2145 power cables are probably not connected correctly. The power cable and signal cable might be connected to different 2145 UPS-1U assemblies.

**User response:**
1. Connect the cables correctly.
2. Restart the node.

Possible Cause-FRUs or other:
- None.

Other:
- Cabling error (100%)

**589** The 2145 UPS-1U ambient temperature limit has been exceeded.

**Explanation:** The ambient temperature threshold for the 2145 UPS-1U has been exceeded.

**User response:** Reduce the temperature around the system:
1. Turn off the 2145 UPS-1U and unplug it from the power source.
2. Clear the vents and remove any heat sources.
3. Ensure that the air flow around the 2145 UPS-1U is not restricted.
4. Wait at least five minutes, and then restart the 2145 UPS-1U. If the problem remains, exchange 2145 UPS-1U assembly.

**590** Repetitive node restarts have occurred because of errors from the 2145 UPS-1U.

**Explanation:** Multiple node restarts have occurred because of 2145 UPS-1U errors.

**User response:** Follow troubleshooting procedures to fix the hardware:
1. Verify that the room temperature is within specified limits and that the input power is stable.
2. Verify that the 2145 UPS-1U signal cable is fastened securely at both ends.

**Note:** The condition will be reset by powering off the node from the node front panel.

**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.

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
668 The remote setting is not available for users for the current system.

Explanation: On the current systems, users cannot be set to remote.

User response: Any user defined on the system must be a local user. To create a remote user the user must not be defined on the local system.

670 The UPS battery charge is not enough to allow the node to start.

Explanation: The uninterruptible power supply connected to the node does not have sufficient battery charge for the node to safely become active in a cluster. The node will not start until a sufficient charge exists to store the state and configuration data held in the node memory if power were to fail. The front panel of the node will show "charging".

User response: Wait for sufficient battery charge for enclosure to start:
1. Wait for the node to automatically fix the error when there is sufficient charge.
2. Ensure that no error conditions are indicated on the uninterruptible power supply.

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 in the node canister hardware details.

User response: Wait for the node to automatically fix the error when sufficient charge becomes available.

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%)
The cycling mode of a Metro Mirror object cannot be changed.

**Explanation:** The cycling mode may only be set for Global Mirror objects. Metro Mirror objects cannot have a cycling mode defined.

**User response:** The object's type must be set to 'global' before or when setting the cycling mode.

System code upgrade cannot start because a component firmware update is in progress.

**Explanation:** An attempt was made to initiate an system code upgrade (CCU) while the system was updating the firmware of various hardware components. A CCU can not be done while a firmware download is in progress and so the request to start a CCU failed.

**User response:** The firmware download needs to complete before you can perform a CCU. Due to the dynamic nature of firmware downloads there is no way of following the progress of one. Wait approximately 10 minutes and retry the command.

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

A Fibre Channel adapter has failed.

**Explanation:** A Fibre Channel adapter has failed. 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:**

- Location—A number indicating the adapter location. Location 0 indicates 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.

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.

Possible Cause—FRUs or other cause:

- Node canister 100%
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. 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 using the remove and replace procedures.

**Possible Cause-FRUs or other cause:**
- Node canister

---

704 Fewer Fibre Channel ports operational.

**Explanation:** A Fibre Channel port that was previously operational is no longer operational. The physical link is down.

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:**

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.

**User response:**
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. **Possibilities:**
   - If the port has been intentionally disconnected, use the management GUI recommended action for the service error code and acknowledge the intended change.
   - Check that the Fibre Channel cable is connected at both ends and is not damaged. If necessary, replace the cable.
   - 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.
   - 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.
   - 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
705 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.

User response:

1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Follow the procedure for mapping I/O ports to platform ports to determine which platform port is providing this I/O port.
3. Check for any 704 (Fibre channel platform port not operational) or 724 (Ethernet platform port not operational) node errors reported for the platform port.
4. Possibilities:
   - If the port has been intentionally disconnected, use the management GUI recommended action for the service error code and acknowledge the intended change.
   - Resolve the 704 or 724 error.
   - If this is an FCoE connection, use the information the view gives about the Fibre Channel forwarder (FCF) to troubleshoot the connection between the port and the FCF.

Possible Cause-FRU's or other cause:

- None

706 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.

A Fibre Channel I/O port might be established on either a FC platform port or an Ethernet platform port using Fiber Channel over Ethernet (FCoE).

Data:

Three numeric values are listed:

- The ID of the first FC I/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.
- 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, 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: 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: FRU’s or other cause:

- None

710 The SAS adapter that was previously present has not been detected.

Explanation: A SAS adapter that was previously present has not been detected. The adapter is located on the node canister system board.
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

711 A SAS adapter has failed.

Explanation: A SAS adapter has failed. 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. 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. 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

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.

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 at 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

### 731
**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

### 732
**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, 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

### 733
**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

### 734
**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:

Chapter 9. Event reporting  161
• 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

740  The command failed because of a wiring error described in the event log.

Explanation: It is dangerous to exclude a sas port while the topology is invalid, so we forbid the user from attempting it to avoid any potential loss of data access.

User response: Correct the topology, then retry the command.

768  Ambient temperature warning.

Explanation: Data:
• A text string identifying the thermal sensor reporting the warning level and the current temperature in degrees (Celsius).

User response: Possible Cause-FRUs or other cause:
• None

769  CPU temperature warning.

Explanation: Data:
• A text string identifying the thermal sensor reporting the warning level and the current temperature in degrees (Celsius).

User response: Possible Cause—FRUs or other cause:
• CPU

770  shutdown temperature reached

Explanation: The node temperature has reached the point at which it is must shut down to protect electronics and data. This is most likely an ambient temperature problem, but it could be a hardware issue.

Data:
• A text string identifying the thermal sensor reporting the warning level and the current temperature in degrees (Celsius).

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Check the temperature of the room and correct any air conditioning or ventilation problems.
3. Check the airflow around the system and make sure no vents are blocked.

Possible Cause-FRUs or other cause:
• CPU

803  Fibre Channel adapter not working

Explanation: A problem has been detected on the node’s Fibre Channel (FC) adapter. This node error is reported only on SAN Volume Controller 2145-CG8 or older nodes.

User response: Follow troubleshooting procedures to fix the hardware.
1. If possible, use the management GUI to run the recommended actions for the associated service error code.

Possible Cause-FRUs or other cause:
• None

818  Unable to recover the service controller flash disk.

Explanation: A nonrecoverable error occurred when accessing the service controller persistent memory.

User response:
1. Restart the node and see if it recovers.
2. Replace the field replaceable units (FRUs) in the order listed.

Possible Cause-FRUs or other cause:
• Service controller
• Service controller cable
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

840 Unsupported hardware change detected.

Explanation:

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. If the hardware configuration is unexpectedly reduced, make sure the component has not been unseated. Hardware replacement might be necessary.

If the hardware detected does not match the expected configuration, replace the hardware component that is reported incorrectly.

Possible Cause-FRUs or other cause:
• One of the optional hardware components might require replacement

841 Supported hardware change detected.

Explanation:

User response:
1. Use the management GUI to run the recommended actions for the associated service error code. Use the directed maintenance to accept or reject the new configuration.

850 The canister battery is reaching the end of its useful life.

Explanation: The canister battery is reaching the end of its useful life. It should be replaced within a week of the node error first being reported.

User response:
1. If possible, use the management GUI to run the recommended actions for the associated service error code.
2. Replace the node canister battery by using the remove and replace procedures.

Possible Cause-FRUs or other cause:
• Canister battery

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. Rezone 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

870 Too many cluster creations made on node

Explanation: Too many Storwize V7000 clustered systems have been created on this node. The count of the number of clustered systems created on the node is stored within the node service controller.

Data:
• None

User response:
1. Try to create the clustered system on a different node.
2. Replace the service controller using the remove and replace procedures.

Possible cause-FRUs or other cause:
• Service controller
871  Failed to increment cluster ID

**Explanation:** The clustered system create option failed because the clustered system, which is stored in the service controller, could not be updated.

**Data:**
- None

**User response:**
1. Try to create the clustered system on a different node.
2. Replace the service controller using the remove and replace procedures.

**Possible cause-FRUs or other cause:**
- Service controller

---

888  Too many Fibre Channel logins between nodes.

**Explanation:** The system has determined that the user has zoned the fabric such that this node has received more than 16 unmasked logins originating from another node or node canister - this can be any non-service mode node or canister in the local cluster or in a remote cluster with a partnership. An unmasked login is from a port whose corresponding bit in the FC port mask is '1'. If the error is raised against a node in the local cluster, then it is the local FC port mask that is applied. If the error is raised against a node in a remote cluster, then it is the partner FC port masks from both clusters that apply.

More than 16 logins is not a supported configuration as it increases internode communication and can affect bandwidth and performance. For example, if node A has 8 ports and node B has 8 ports where the nodes are in different clusters, if node A has a partner FC port mask of 00000011 and node B has a partner FC port mask of 11000000 there are 4 unmasked logins possible (1,7, 1,8, 2,7, 2,8). Fabric zoning may be used to reduce this amount further, i.e. if node B port 8 is removed from the zone there are only 2 (1,7 and 2,7). The combination of masks and zoning must leave 16 or fewer possible logins.

**Note:** This count includes both FC and Fibre Channel over Ethernet (FCoE) logins. The log-in count will not include masked ports.

When this event is logged, the cluster id and node id of the first node whose logins exceed this limit on the local node will be reported, as well as the WWNN of said node. If logins change, the error is automatically fixed and another error is logged if appropriate (this may or may not choose the same node to report in the sense data if the same node is still over the maximum allowed).

**Data**

- Text string showing
  - WWNN of the other node
  - Cluster ID of other node
  - Arbitrary node ID of one other node that is logged into this node. (node ID as it appears in lsnode)

**User response:** The error is resolved by either re-configuring the system to change which type of connection is allowed on a port, or by changing the SAN fabric configuration so ports are not in the same zone. A combination of both options may be used.

The system reconfiguration is to change the Fibre...
Channel ports mask to reduce which ports can be used for internode communication.

The local Fibre Channel port mask should be modified if the cluster id reported matches the cluster id of the node logging the error.

The partner Fibre Channel port mask should be modified if the cluster id reported does not match the cluster id of the node logging the error. The partner Fibre Channel port mask may need to be changed for one or both clusters.

SAN fabric configuration is set using the switch configuration utilities.

Use the *lsfabric* command to view the current number of logins between nodes.

Possible Cause-FRU or other cause:
- None

**Service error code**

1801

<table>
<thead>
<tr>
<th>889</th>
<th>Failed to create remote IP connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Despite a request to create a remote IP replication port connection, the action has failed or timed out.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>Fix the remote IP link so that traffic can flow correctly. Once the connection is made, the error will auto-correct.</td>
</tr>
</tbody>
</table>

920 | Unable to perform cluster recovery because of a lack of cluster resources. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>The node is looking for a quorum of resources which also require cluster recovery.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>Contact IBM technical support.</td>
</tr>
</tbody>
</table>

921 | Unable to perform cluster recovery because of a lack of cluster resources. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>The node does not have sufficient connectivity to other nodes or quorum device to form a cluster. If a disaster has occurred and the nodes at the other site cannot be recovered, then it is possible to allow the nodes at the surviving site to form a system using local storage.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>Repair the fabric or quorum device to establish connectivity. As a last resort when the nodes at the other site cannot be recovered, then it is possible to allow the nodes at the surviving site to form a system using local site storage as described below:</td>
</tr>
<tr>
<td></td>
<td>To avoid data corruption ensure that all host servers that were previously accessing the system have had all volumes un-mounted or have been rebooted. Ensure that the nodes at the other site are not operational and are unable to form a system in the future.</td>
</tr>
<tr>
<td></td>
<td>After invoking this command a full re-synchronization of all mirrored volumes will be performed when the other site is recovered. This is likely to take many hours or days to complete.</td>
</tr>
<tr>
<td></td>
<td>Contact IBM support personnel if you are unsure.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Before continuing confirm that you have taken the following actions - failure to perform these actions can lead to data corruption that will be undetected by the system but will affect host applications.</td>
</tr>
<tr>
<td></td>
<td>1. All host servers that were previously accessing the system have had all volumes un-mounted or have been rebooted.</td>
</tr>
<tr>
<td></td>
<td>2. Ensure that the nodes at the other site are not operating as a system and actions have been taken to prevent them from forming a system in the future.</td>
</tr>
</tbody>
</table>

After these actions have been taken the *satask overridequorum* can be used to allow the nodes at the surviving site to form a system using local storage.

950 | Special upgrade mode. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Special upgrade mode.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>None.</td>
</tr>
</tbody>
</table>

990 | Cluster recovery has failed. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Cluster recovery has failed.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>Contact IBM technical support.</td>
</tr>
</tbody>
</table>

1001 | Automatic cluster recovery has run. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>All cluster configuration commands are blocked.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>Call your software support center.</td>
</tr>
</tbody>
</table>

**Caution:** You can unblock the configuration commands through the cluster GUI, but you must first consult with your software support to avoid corrupting your cluster configuration.

Possible Cause-FRU or other:
- None

1002 | Event log full. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Event log full.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>To fix the errors in the event log, go to the start MAP.</td>
</tr>
</tbody>
</table>

Possible Cause-FRU or other:
- Unfixed errors in the log.
1011 Fibre Channel adapter (4 port) in slot 1 is missing.

Explanation: Fibre Channel adapter (4 port) in slot 1 is missing.

User response:
1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-CG8 or 2145-CF8
• 4-port Fibre Channel host bus adapter (98%)
• System board (2%)

2145-8G4 or 2145-8A4
• 4-port Fibre Channel host bus adapter (90%)
• PCI Express riser card (8%)
• System board (2%)

1013 Fibre Channel adapter (4-port) in slot 1 PCI fault.

Explanation: Fibre Channel adapter (4-port) in slot 1 PCI fault.

User response:
1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-CG8 or 2145-CF8
• 4-port Fibre Channel host bus adapter (98%)
• System board (2%)

2145-8G4 or 2145-8A4
• 4-port Fibre Channel host bus adapter (80%)
• PCI Express riser card (10%)
• System board (10%)

N/A

1014 Fibre Channel adapter in slot 1 is missing.

Explanation: Fibre Channel adapter in slot 1 is missing.

User response:
1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4
• N/A

1015 Fibre Channel adapter in slot 2 is missing.

Explanation: Fibre Channel adapter in slot 2 is missing.

User response:
1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4
• N/A

1016 Fibre Channel adapter (4 port) in slot 2 is missing.

Explanation: Fibre Channel adapter (4 port) in slot 2 is missing.

User response:
1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRU or other:

2145-8G4
• N/A

<table>
<thead>
<tr>
<th>1017</th>
<th>Fibre Channel adapter in slot 1 PCI bus error.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>Fibre Channel adapter in slot 1 PCI bus error.</td>
</tr>
<tr>
<td>User response:</td>
<td>1. In the sequence shown, exchange the FRUs for new FRUs.</td>
</tr>
<tr>
<td></td>
<td>2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.</td>
</tr>
<tr>
<td></td>
<td>3. Go to repair verification MAP.</td>
</tr>
<tr>
<td>Possible Cause-FRU or other:</td>
<td></td>
</tr>
<tr>
<td>2145-8G4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1018</th>
<th>Fibre Channel adapter in slot 2 PCI fault.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>Fibre Channel adapter in slot 2 PCI fault.</td>
</tr>
<tr>
<td>User response:</td>
<td>1. In the sequence shown, exchange the FRUs for new FRUs.</td>
</tr>
<tr>
<td></td>
<td>2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.</td>
</tr>
<tr>
<td></td>
<td>3. Go to repair verification MAP.</td>
</tr>
<tr>
<td>Possible Cause-FRU or other:</td>
<td></td>
</tr>
<tr>
<td>2145-8G4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1019</th>
<th>Fibre Channel adapter (4-port) in slot 2 PCI fault.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>Fibre Channel adapter (4-port) in slot 2 PCI fault.</td>
</tr>
<tr>
<td>User response:</td>
<td>1. In the sequence shown, exchange the FRUs for new FRUs.</td>
</tr>
</tbody>
</table>

2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.

3. Go to repair verification MAP.

Possible Cause-FRU or other:

2145-8G4
• N/A

<table>
<thead>
<tr>
<th>1020</th>
<th>The system board service processor has failed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>The cluster is reporting that a node is not operational because of critical node error 522. See the details of node error 522 for more information.</td>
</tr>
<tr>
<td>User response:</td>
<td>See node error 522.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1021</th>
<th>Incorrect enclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>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.</td>
</tr>
<tr>
<td>User response:</td>
<td>See node error 500.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1022</th>
<th>The detected memory size does not match the expected memory size.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>The cluster is reporting that a node is not operational because of critical node error 510. See the details of node error 510 for more information.</td>
</tr>
<tr>
<td>User response:</td>
<td>See node error 510.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1025</th>
<th>The 2145 system assembly is failing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explanation:</td>
<td>The 2145 system assembly is failing.</td>
</tr>
<tr>
<td>User response:</td>
<td>1. Go to the light path diagnostic MAP and perform the light path diagnostic procedures.</td>
</tr>
<tr>
<td></td>
<td>2. If the light path diagnostic procedure isolates the FRU, mark this error as “fixed” and go to the repair verification MAP. If you have just replaced a FRU but it has not corrected the problem, ensure that the FRU is installed correctly and go to the next step.</td>
</tr>
<tr>
<td></td>
<td>3. Replace the system board or frame assembly as indicated in the Possible Cause list below.</td>
</tr>
<tr>
<td></td>
<td>4. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to the start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.</td>
</tr>
<tr>
<td></td>
<td>5. Go to the repair verification MAP.</td>
</tr>
</tbody>
</table>
Possible Cause-FRUs or other:
2145-8G4, 2145-CF8, or 2145-CG8
- The FRUs that are indicated by the Light path diagnostics (98%)
- System board (2%)

1027 Unable to update BIOS settings.
**Explanation:** The cluster is reporting that a node is not operational because of critical node error 524. See the details of node error 524 for more information.
**User response:** See node error 524.

1030 The internal disk of a node has failed.
**Explanation:** An error has occurred while attempting to read or write data to the internal disk of one of the nodes in the cluster. The disk has failed.
**User response:** Determine which node's internal disk has failed using the node information in the error. Replace the FRUs in the order shown. Mark the error as fixed.
Possible Cause-FRUs or other:
2145-CG8 or 2145-CF8
- disk drive (50%)
- Disk controller (30%)
- Disk backplane (10%)
- Disk signal cable (8%)
- Disk power cable (1%)
- System board (1%)
2145-8A4
- disk drive (90%)
- disk cable assembly (10%)
2145-8G4
- disk drive assembly (90%)
- disk drive cables (10%)

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.

1040 A flash module error has occurred after a successful start of a 2145.
**Explanation:** Note: The node containing the flash module has not been rejected by the cluster.
**User response:**
1. Replace the FRUs below in the order listed
2. Check node status. If all nodes show a status of Online, mark the error that you have just repaired “fixed”. If any nodes do not show a status of Online, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.
Possible Cause-FRUs or other:
2145-CG8 or 2145-CF8
- Service controller (50%)
- Service controller cable (50%)
2145-8G4 or 2145-8A4
Service controller (100%)

1044 A service controller read failure occurred.
**Explanation:** A service controller read failure occurred.
**User response:**
1. Replace the FRUs below in the order listed.
2. Check node status. If all nodes show a status of Online, mark the error that you have just repaired “fixed”. If any nodes do not show a status of Online, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.
Possible Cause-FRUs or other:
2145-CG8 or 2145-CF8
- Service controller (50%)
- Service controller cable (50%)
2145-8G4 or 2145-8A4
Service controller (100%)

1052 Incorrect type of uninterruptible power supply detected
**Explanation:** The cluster is reporting that a node is not operational because of critical node error 587. See the details of node error 587 for more information.
**User response:** See node error 587.

1054 Fibre Channel adapter in slot 1 adapter present but failed.
**Explanation:** Fibre Channel adapter in slot 1 adapter present but failed.
**User response:**
1. Replace the Fibre Channel adapter.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

1055  Fibre Channel adapter (4 port) in slot 1 adapter present but failed.

Explanation: Fibre Channel adapter (4 port) in slot 1 adapter present but failed.

User response:
1. Exchange the FRU for new FRU.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4
• N/A

1056  Fibre Channel adapter in slot 2 adapter present but failed.

Explanation: Fibre Channel adapter in slot 2 adapter present but failed.

User response:
1. Replace the Fibre Channel adapter.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4
• N/A

1057  Fibre Channel adapter (4 port) in slot 2 adapter present but failed.

Explanation: Fibre Channel adapter (4 port) in slot 2 adapter present but failed.

User response:
1. Exchange the FRU for new FRU.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4
• N/A

1060  One or more Fibre Channel ports on the 2145 are not operational.

Explanation: One or more Fibre Channel ports on the 2145 are not operational.

User response:
1. Go to MAP 5600: Fibre Channel to isolate and repair the problem.
2. Go to the repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4, 2145-CF8, or 2145-CG8
• Fibre Channel cable (80%)
• Small Form-factor Pluggable (SFP) connector (5%)
• 4-port Fibre Channel host bus adapter (5%)

Other:
• Fibre Channel network fabric (10%)

1065  One or more Fibre Channel ports are running at lower than the previously saved speed.

Explanation: The Fibre Channel ports will normally operate at the highest speed permitted by the Fibre Channel switch, but this speed might be reduced if the signal quality on the Fibre Channel connection is poor. The Fibre Channel switch could have been set to operate at a lower speed by the user, or the quality of the Fibre Channel signal has deteriorated.

User response:
• Go to MAP 5600: Fibre Channel to resolve the problem.

Possible Cause-FRUs or other:
1083 • 1092

2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
- Fibre Channel cable (50%)
- Small Form-factor Pluggable (SFP) connector (20%)
- 4-port Fibre Channel host bus adapter (5%)

Other:
- Fibre Channel switch, SFP connector, or GBIC (25%)

---

1083  Unrecognized node error

Explanation: The cluster is reporting that a node is not operational because of critical node error 562. See the details of node error 562 for more information.

User response: See node error 562.

---

1089  One or more fans are failing.

Explanation: One or more fans are failing.

User response:
1. Determine the failing fan(s) from the fan indicator on the system board or from the text of the error data in the log. The reported fan for the 2145-8A4, 2145-CF8, or 2145-CG8 matches the fan assembly position. For the 2145-8G4, if you have determined the failing fan number from the error data in the log, use the following list to determine the position of the fan assembly to replace. Each fan assembly contains two fans.
2. Exchange the FRU for a new FRU.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- Fan assembly (100%)
- 1 or 2:1
- 3 or 4:2
- 5 or 6:3
- 7 or 8:4
- 9 or 10:5
- 11 or 12:6

---

1091  One or more fans (40x40x56) are failing.

Explanation: One or more fans (40x40x56) are failing.

User response:
1. Determine the failing fan(s) from the fan indicator on the system board or from the text of the error data in the log.
2. If all fans on the fan backplane are failing or if no fan fault lights are illuminated, verify that the cable between the fan backplane and the system board is connected.
3. Exchange the FRU for a new FRU.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145-8G4
  - N/A

---

1092  The temperature soft or hard shutdown threshold of the 2145 has been exceeded. The 2145 has automatically powered off.

Explanation: The temperature soft or hard shutdown threshold of the 2145 has been exceeded. The 2145 has automatically powered off.

User response:
1. Ensure that the operating environment meets specifications.
2. Ensure that the airflow is not obstructed.
3. Ensure that the fans are operational.
4. Go to the light path diagnostic MAP and perform the light path diagnostic procedures.
5. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to the start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
6. Go to the repair verification MAP.

Possible Cause-FRUs or other:
- 2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
  - The FRU that is indicated by the Light path diagnostics (25%)
  - System board (5%)

---
Other:

System environment or airflow blockage (70%)

1093 The internal temperature sensor of the 2145 has reported that the temperature warning threshold has been exceeded.

Explanation: The internal temperature sensor of the 2145 has reported that the temperature warning threshold has been exceeded.

User response:
1. Ensure that the internal airflow of the node has not been obstructed.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to the start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
• Fan assembly (25%)
• System board (5%)

Other:

Airflow blockage (70%)

1094 The ambient temperature threshold has been exceeded.

Explanation: The ambient temperature threshold has been exceeded.

User response:
1. Check that the room temperature is within the limits allowed.
2. Check for obstructions in the air flow.
3. Mark the errors as fixed.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:

None

Other:

System environment (100%)
A Power Supply Unit reports no A/C power.

Explanation: One of the two power supply units in the node is reporting that no main power is detected.

User response:
1. Ensure that the power supply is attached correctly to both the node and to the 2145 UPS-1U.
2. If the error has not been automatically marked fixed after two minutes, note the status of the three LEDs on the back of the power supply. For the 2145-CG8 or 2145-CF8, the AC LED is the top green LED, the DC LED is the middle green LED and the error LED is the bottom amber LED.
3. If the power supply error LED is off and the AC and DC power LEDs are both on, this is the normal condition. If the error has not been automatically fixed after two minutes, replace the system board.
4. Follow the action specified for the LED states noted in the table below.
5. If the error has not been automatically fixed after two minutes, contact support.
6. Go to repair verification MAP.

Possible Cause-FRUs or other:

- Power cable assembly (5%)
- System board (5%)

Error,AC,DC:Action

ON,ON or OFF,ON or OFF: The power supply has a fault. Replace the power supply.

OFF,OFF,OFF: There is no power detected. Ensure that the power cable is connected at the node and 2145 UPS-1U. If the AC LED does not light, check whether the 2145 UPS-1U is showing any errors. Follow MAP 5150 2145 UPS-1U if the UPS-1U is showing an error; otherwise, replace the power cable. If the AC LED still does not light, replace the power supply.

OFF,OFF,ON: The power supply has a fault. Replace the power supply.

OFF,ON,OFF: Ensure that the power supply is installed correctly. If the DC LED does not light, replace the power supply.

Possible Cause-FRUs or other:
- Power cable assembly (85%)
- UPS-1U assembly (10%)
- System board (5%)

One of the voltages that is monitored on the system board is over the set threshold.

Explanation: One of the voltages that is monitored on the system board is over the set threshold.

User response:
1. See the light path diagnostic MAP.
2. If the light path diagnostic MAP does not resolve the issue, exchange the frame assembly.
3. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:

- Light path diagnostic MAP FRUs (98%)
- System board (2%)

One of the voltages that is monitored on the system board is under the set threshold.

Explanation: One of the voltages that is monitored on the system board is under the set threshold.

User response:
1. Check the cable connections.
2. See the light path diagnostic MAP.
3. If the light path diagnostic MAP does not resolve the issue, exchange the frame assembly.
4. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.

5. Go to repair verification MAP.

### 1106

**One of the voltages that is monitored on the system board is under the set threshold.**

**Explanation:** One of the voltages that is monitored on the system board is under the set threshold.

**User response:**

1. Check the cable connections.
2. See the light path diagnostic MAP.
3. If the light path diagnostic MAP does not resolve the issue, exchange the system board assembly.
4. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.

5. Go to repair verification MAP.

**Possible Cause-FRUs or other:**

- 2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
- Light path diagnostic MAP FRUs (98%)
- System board (2%)

### 1107

**The power management board detected a voltage that is outside of the set thresholds.**

**Explanation:** The power management board detected a voltage that is outside of the set thresholds.

**User response:**

1. In the sequence shown, exchange the FRUs for new FRUs.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired as “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
3. Go to repair verification MAP.

**Possible Cause-FRUs or other:**

- 2145-CG8 or 2145-CF8
- Power supply unit (50%)
- System board (50%)

### 1120

**A high speed SAS adapter is missing.**

**Explanation:** This node has detected that a high speed SAS adapter that was previously installed is no longer present.

**User response:** If the high speed SAS adapter was deliberately removed, mark the error “fixed.” Otherwise, the high speed SAS adapter has failed and must be replaced. In the sequence shown, exchange the FRUs for new FRUs.

Go to the repair verification MAP.

**Possible Cause-FRUs or other:**

- High speed SAS adapter (90%)
- System board (10%)

### 1121

**A high speed SAS adapter has failed.**

**Explanation:** A fault has been detected on a high speed SAS adapter.

**User response:** In the sequence shown, exchange the FRUs for new FRUs.

Go to the repair verification MAP.

**Possible Cause-FRUs or other:**

- High speed SAS adapter (90%)
- System board (10%)

### 1122

**A high speed SAS adapter error has occurred.**

**Explanation:** The high speed SAS adapter has detected a PCI bus error and requires service before it can be restarted. The high speed SAS adapter failure has caused all of the solid-state drives that were being accessed through this adapter to go Offline.

**User response:** If this is the first time that this error has occurred on this node, complete the following steps:

1. Power off the node.
2. Reseat the high speed SAS adapter card.
3. Power on the node.
4. Submit the `lsmdisk` task and ensure that all of the solid-state drive managed disks that are located in this node have a status of Online.

If the sequence of actions above has not resolved the problem or the error occurs again on the same node, complete the following steps:
1. In the sequence shown, exchange the FRUs for new FRUs.

2. Submit the `lsmdisk` task and ensure that all of the solid-state drive managed disks that are located in this node have a status of Online.

3. Go to the repair verification MAP.

Possible Cause-FRUs or other:
1. High speed SAS adapter (90%)
2. System board (10%)

---

**1133** A duplicate WWNN has been detected.

**Explanation:** The cluster is reporting that a node is not operational because of critical node error 556. See the details of node error 556 for more information.

**User response:** See node error 556.

---

**1135** The 2145 UPS has reported an ambient over temperature.

**Explanation:** The 2145 UPS has reported an ambient over temperature. The uninterruptible power supply switches to Bypass mode to allow the 2145 UPS to cool.

**User response:**
1. Power off the nodes attached to the 2145 UPS.
2. Turn off the 2145 UPS, and then unplug the 2145 UPS from the main power source.
3. Ensure that the air vents of the 2145 UPS are not obstructed.
4. Ensure that the air flow around the 2145 UPS is not restricted.
5. Wait for at least five minutes, and then restart the 2145 UPS. If the problem remains, check the ambient temperature. Correct the problem. Otherwise, exchange the FRU for a new FRU.
6. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
7. Go to repair verification MAP.

Possible Cause-FRUs or other:
2145 UPS-1U assembly (50%)

Other:

The system ambient temperature is outside the specification (50%)

---

**1136** The 2145 UPS-1U has reported an ambient over temperature.

**Explanation:** The 2145 UPS-1U has reported an ambient over temperature.

**User response:**
1. Power off the node attached to the 2145 UPS-1U.
2. Turn off the 2145 UPS-1U, and then unplug the 2145 UPS-1U from the main power source.
3. Ensure that the air vents of the 2145 UPS-1U are not obstructed.
4. Ensure that the air flow around the 2145 UPS-1U is not restricted.
5. Wait for at least five minutes, and then restart the 2145 UPS-1U. If the problem remains, check the ambient temperature. Correct the problem. Otherwise, exchange the FRU for a new FRU.
6. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
7. Go to repair verification MAP.

---

**1140** The 2145 UPS has reported that it has a problem with the input AC power.

**Explanation:** The 2145 UPS has reported that it has a problem with the input AC power.

**User response:**
1. Check the input AC power, whether it is missing or out of specification. Correct if necessary. Otherwise, exchange the FRU for a new FRU.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145 UPS input power cable (10%)
- Electronics assembly (10%)

Other:
1141 The 2145 UPS-1U has reported that it has a problem with the input AC power.

**Explanation:** The 2145 UPS-1U has reported that it has a problem with the input AC power.

**User response:**
1. Check the input AC power, whether it is missing or out of specification. Correct if necessary. Otherwise, exchange the FRU for a new FRU.
2. Check node status. If all nodes show a status of "online", mark the error that you have just repaired as "fixed". If any nodes do not show a status of "online", go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145 UPS-1U input power cable (10%)
- 2145 UPS-1U assembly (10%)

Other:
- The input AC power is missing (40%)
- The input AC power is not in specification (40%)

1145 The signal connection between a 2145 and its 2145 UPS is failing.

**Explanation:** The signal connection between a 2145 and its 2145 UPS is failing.

**User response:**
1. If other 2145s that are using this uninterruptible power supply are reporting this error, exchange the 2145 UPS electronics unit for a new one.
2. If only this 2145 is reporting the problem, check the signal cable, exchange the FRUs for new FRUs in the sequence shown.
3. Check node status. If all nodes show a status of "online", mark the error that you have just repaired as "fixed". If any nodes do not show a status of "online", go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145-CF8 or 2145-CG8
    - Power cable assembly (40%)
    - 2145 UPS-1U assembly (30%)
    - System board (30%)
- 2145-8G4
    - Power cable assembly (40%)
    - 2145 UPS-1U assembly (30%)
    - System board (30%)

1150 Data that the 2145 has received from the 2145 UPS suggests the 2145 UPS power cable, the signal cable, or both, are not connected correctly.

**Explanation:** Data that the 2145 has received from the 2145 UPS suggests the 2145 UPS power cable, the signal cable, or both, are not connected correctly.

**User response:**
1. Connect the cables correctly. See your product’s installation guide.
2. Check node status. If all nodes show a status of "online", mark the error that you have just repaired as "fixed". If any nodes do not show a status of "online", go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:
- Configuration error
1151  Data that the 2145 has received from the 2145 UPS-1U suggests the 2145 UPS-1U power cable, the signal cable, or both, are not connected correctly.

**Explanation:** Data that the 2145 has received from the 2145 UPS-1U suggests the 2145 UPS-1U power cable, the signal cable, or both, are not connected correctly.

**User response:**
1. Connect the cables correctly. See your product’s installation guide.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Configuration error

1152  Incorrect type of uninterruptible power supply detected.

**Explanation:** The cluster is reporting that a node is not operational because of critical node error 587. See the details of node error 587 for more information.

**User response:** See node error 587.

1155  A power domain error has occurred.

**Explanation:** Both 2145s of a pair are powered by the same uninterruptible power supply.

**User response:**
1. List the 2145s of the cluster and check that 2145s in the same I/O group are connected to a different uninterruptible power supply.
2. Connect one of the 2145s as identified in step 1 to a different uninterruptible power supply.
3. Mark the error that you have just repaired, “fixed”.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Configuration error

1156  The output load on the 2145 UPS exceeds the specification.

**Explanation:** The 2145 UPS is reporting that too much power is being drawn from it. The power overload warning LED, which is above the load level indicators, on the 2145 UPS will be on.

**User response:**
1. Determine the 2145 UPS that is reporting the error from the error event data. Perform the following steps on just this uninterruptible power supply.
2. Check that the 2145 UPS is still reporting the error. If the power overload warning LED is no longer on, go to step 6.
3. Ensure that only 2145s are receiving power from the uninterruptible power supply. Ensure that there are no switches or disk controllers that are connected to the 2145 UPS.
4. Remove each connected 2145 input power in turn, until the output overload is removed.
5. Exchange the FRUs for new FRUs in the sequence shown, on the overcurrent 2145.
6. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145 UPS.
7. Go to repair verification MAP.

Possible Cause-FRUs or other:
• Power cable assembly (50%)
• Power supply assembly (40%)
• 2145 UPS electronics assembly (10%)

1161  The output load on the 2145 UPS-1U exceeds the specifications (reported by 2145 UPS-1U alarm bits).

**Explanation:** The output load on the 2145 UPS-1U exceeds the specifications (reported by 2145 UPS-1U alarm bits).

**User response:**
1. Ensure that only 2145s are receiving power from the uninterruptible power supply. Also, ensure that no other devices are connected to the 2145 UPS-1U.
2. Exchange, in the sequence shown, the FRUs for new FRUs. If the Overload Indicator is still illuminated with all outputs disconnected, replace the 2145 UPS-1U.
3. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145 UPS-1U.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
- Power cable assembly (50%)
- Power supply assembly (40%)
- 2145 UPS-1U assembly (10%)

**1165**

The 2145 UPS output load is unexpectedly high. The 2145 UPS output is possibly connected to an extra non-2145 load.

**Explanation:** The 2145 UPS output load is unexpectedly high. The 2145 UPS output is possibly connected to an extra non-2145 load.

**User response:**
1. Ensure that only 2145s are receiving power from the uninterruptible power supply. Ensure that there are no switches or disk controllers that are connected to the 2145 UPS.
2. Check node status. If all nodes show a status of “online”, the problem no longer exists. Mark the error that you have just repaired “fixed” and go to the repair verification MAP.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
None

Other:
- Configuration error

**1166**

The 2145 UPS-1U output load is unexpectedly high.

**Explanation:** The uninterruptible power supply output is possibly connected to an extra non-2145 load.

**User response:**
1. Ensure that there are no other devices that are connected to the 2145 UPS-1U.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145 UPS-1U.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145 UPS-1U assembly (5%)

Other:
- Configuration error (95%)

**1170**

2145 UPS electronics fault (reported by the 2145 UPS alarm bits).

**Explanation:** 2145 UPS electronics fault (reported by the 2145 UPS alarm bits).

**User response:**
1. Replace the uninterruptible power supply electronics assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the UPS.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145 UPS-1U electronics assembly (100%)

**1171**

2145 UPS-1U electronics fault (reported by the 2145 UPS-1U alarm bits).

**Explanation:** 2145 UPS-1U electronics fault (reported by the 2145 UPS-1U alarm bits).

**User response:**
1. Replace the uninterruptible power supply assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145 UPS-1U.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- 2145 UPS-1U assembly (100%)

**1175**

A problem has occurred with the uninterruptible power supply frame fault (reported by uninterruptible power supply alarm bits).

**Explanation:** A problem has occurred with the uninterruptible power supply frame fault (reported by the uninterruptible power supply alarm bits).

**User response:**
1. Replace the uninterruptible power supply assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.
Possible Cause-FRUs or other:

Uninterruptible power supply assembly (100%)

1180 2145 UPS battery fault (reported by 2145 UPS alarm bits).

Explanation: 2145 UPS battery fault (reported by 2145 UPS alarm bits).

User response: 
1. Replace the 2145 UPS battery assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS battery assembly (100%)

1181 2145 UPS-1U battery fault (reported by 2145 UPS-1U alarm bits).

Explanation: 2145 UPS-1U battery fault (reported by 2145 UPS-1U alarm bits).

User response: 
1. Replace the 2145 UPS-1U battery assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS-1U battery assembly (100%)

1182 Ambient temperature is too high during system startup.

Explanation: The cluster is reporting that a node is not operational because of critical node error 528. See the details of node error 528 for more information.

User response: See node error 528.

1183 The nodes hardware configuration does not meet the minimum requirements.

Explanation: The cluster is reporting that a node is not operational because of critical node error 562. See the details of node error 562 for more information.

User response: See node error 562.

1185 2145 UPS fault, with no specific FRU identified (reported by uninterruptible power supply alarm bits).

Explanation: 2145 UPS fault, with no specific FRU identified (reported by 2145 UPS alarm bits).

User response: 
1. In the sequence shown, exchange the FRU for a new FRU.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145 UPS.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS electronics assembly (60%)
2145 UPS battery assembly (20%)
2145 UPS assembly (20%)

1186 A problem has occurred in the 2145 UPS-1U, with no specific FRU identified (reported by 2145 UPS-1U alarm bits).

Explanation: A problem has occurred in the 2145 UPS-1U, with no specific FRU identified (reported by 2145 UPS-1U alarm bits).

User response: 
1. In the sequence shown, exchange the FRU for a new FRU.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS-1U assembly (100%)

1187 Node software is inconsistent or damaged

Explanation: The cluster is reporting that a node is not operational because of critical node errors 523, 573, 574. See the details of node errors 523, 573, 574 for more information.

User response: See node errors 523, 573, 574.
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.

The 2145 UPS battery has reached its end of life.

Explanation: The 2145 UPS battery has reached its end of life.

User response:
1. Replace the 2145 UPS battery assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS battery assembly (100%)

The 2145 UPS-1U battery has reached its end of life.

Explanation: The 2145 UPS-1U battery has reached its end of life.

User response:
1. Replace the 2145 UPS-1U battery assembly.
2. Check node status. If all nodes show a status of “online”, mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the uninterruptible power supply.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

2145 UPS-1U battery assembly (100%)

Unexpected node error

Explanation: A node is missing from the cluster. The error that it is reporting is not recognized by the system.

User response: Find the node that is in service state and use the service assistant to determine why it is not active.

The UPS battery charge is not enough to allow the node to start.

Explanation: The cluster is reporting that a node is not operational because of critical node error 587. See the details of node error 587 for more information.

User response:

Automatic recovery of offline node has failed.

Explanation: The cluster has an offline node and has determined that one of the candidate nodes matches the characteristics of the offline node. The cluster has attempted but failed to add the node back into the cluster. The cluster has stopped attempting to automatically add the node back into the cluster.

If a node has incomplete state data, it remains offline after it starts. This occurs if the node has had a loss of power or a hardware failure that prevented it from completing the writing of all of the state data to disk. The node reports a node error 578 when it is in this state.

If three attempts to automatically add a matching candidate node to a cluster have been made, but the node has not returned online for 24 hours, the cluster stops automatic attempts to add the node and logs error code 1194 “Automatic recovery of offline node failed”.

Two possible scenarios when this error event is logged are:

1. The node has failed without saving all of its state data. The node has restarted, possibly after a repair, and shows node error 578 and is a candidate node for joining the cluster. The cluster attempts to add the node into the cluster but does not succeed. After 15 minutes, the cluster makes a second attempt to add the node into the cluster and again does not succeed. After another 15 minutes, the cluster makes a third attempt to add the node into the cluster and again does not succeed. After another 15 minutes, the cluster logs error code 1194. The node never came online during the attempts to add it to the cluster.

2. The node has failed without saving all of its state data. The node has restarted, possibly after a repair, and shows node error 578 and is a candidate node for joining the cluster. The cluster attempts to add the node into the cluster and succeeds and the node
becomes online. Within 24 hours the node fails again without saving its state data. The node restarts and shows node error 578 and is a candidate node for joining the cluster. The cluster again attempts to add the node into the cluster, succeeds, and the node becomes online; however, the node again fails within 24 hours. The cluster attempts a third time to add the node into the cluster, succeeds, and the node becomes online; however, the node again fails within 24 hours. After another 15 minutes, the cluster logs error code 1194. A combination of these scenarios is also possible.

Note: If the node is manually removed from the cluster, the count of automatic recovery attempts is reset to zero.

**User response:**
1. If the node has been continuously online in the cluster for more than 24 hours, mark the error as fixed and go to the Repair Verification MAP.
2. Determine the history of events for this node by locating events for this node name in the event log. Note that the node ID will change, so match on the WWNN and node name. Also, check the service records. Specifically, note entries indicating one of three events: 1) the node is missing from the cluster (cluster error 1195 event 009052), 2) an attempt to automatically recover the offline node is starting (event 980352), 3) the node has been added to the cluster (event 980349).
3. If the node has not been added to the cluster since the recovery process started, there is probably a hardware problem. The node’s internal disk might be failing in a manner that it is unable to modify its software level to match the software level of the cluster. If you have not yet determined the root cause of the problem, you can attempt to manually remove the node from the cluster and add the node back into the cluster. Continuously monitor the status of the nodes in the cluster while the cluster is attempting to add the node. Note: If the node type is not supported by the software version of the cluster, the node will not appear as a candidate node. Therefore, incompatible hardware is not a potential root cause of this error.
4. If the node was added to the cluster but failed again before it has been online for 24 hours, investigate the root cause of the failure. If no events in the event log indicate the reason for the node failure, collect dumps and contact IBM technical support for assistance.
5. When you have fixed the problem with the node, you must use either the cluster console or the command line interface to manually remove the node from the cluster and add the node into the cluster.
6. Mark the error as fixed and go to the verification MAP.

---

### A 2145 is missing from the cluster.

**Explanation:** You can resolve this problem by repairing the failure on the missing 2145.

**User response:**
1. If it is not obvious which node in the cluster has failed, check the status of the nodes and find the 2145 with a status of offline.
2. Go to the Start MAP and perform the repair on the failing node.
3. When the repair has been completed, this error is automatically marked as fixed.
4. Check node status. If all nodes show a status of “online”, but the error in the log has not been marked as fixed, manually mark the error that you have just repaired “fixed”. If any nodes do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the 2145.
5. Go to repair verification MAP.

**Possible Cause-FRUs or other:**
- None

---

### The configuration is not valid. Too many devices, MDisks, or targets have been presented to the system.

**Explanation:** The configuration is not valid. Too many devices, MDisks, or targets have been presented to the system.

**User response:**
1. Remove unwanted devices from the Fibre Channel network fabric.
2. Start a cluster discovery operation to find devices/disks by rescanning the Fibre Channel network.
3. List all connected managed disks. Check with the customer that the configuration is as expected. Mark the error that you have just repaired fixed.
4. Go to repair verification MAP.

**Possible Cause-FRUs or other:**
- None

---

### Fibre Channel network fabric fault (100%)

---
1201 A solid-state drive requires a recovery.

**Explanation:** The solid-state drive that is identified by this error needs to be recovered.

**User response:** To recover this SSD drive, submit the following command: `chdrive -task recover drive_id` where `drive_id` is the identity of the drive that needs to be recovered.

1202 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.

1203 A duplicate Fibre Channel frame has been received.

**Explanation:** A duplicate Fibre Channel frame should never be detected. Receiving a duplicate Fibre Channel frame indicates that there is a problem with the Fibre Channel fabric. Other errors related to the Fibre Channel fabric might be generated.

**User response:**
1. Use the transmitting and receiving WWPNs indicated in the error data to determine the section of the Fibre Channel fabric that has generated the duplicate frame. Search for the cause of the problem by using fabric monitoring tools. The duplicate frame might be caused by a design error in the topology of the fabric, by a configuration error, or by a software or hardware fault in one of the components of the Fibre Channel fabric, including inter-switch links.
2. When you are satisfied that the problem has been corrected, mark the error that you just repaired “fixed”.
3. Go to MAP 5700: Repair verification.

Possible Cause-FRUs or other:
- Fibre Channel cable assembly (75%)
- Small Form-factor Pluggable (SFP) connector (10%)
- Fibre Channel adapter (5%)

Other:
- Fibre Channel network fabric fault (10%)

1215 A solid-state drive is failing.

**Explanation:** The solid-state drive has detected faults that indicate that the drive is likely to fail soon. The drive should be replaced. The cluster event log will identify a drive ID for the solid-state drive that caused the error.

**User response:** In the management GUI, click **Troubleshooting > Recommended Actions** to run the recommended action for this error. If this does not resolve the issue, contact your next level of support.

1216 SAS errors have exceeded thresholds.

**Explanation:** The cluster has experienced a large number of SAS communication errors, which indicates a faulty SAS component that must be replaced.

**User response:** In the sequence shown, exchange the FRUs for new FRUs.

Go to the repair verification MAP.

Possible Cause-FRUs or other:
1. SAS Cable (70%)
2. High speed SAS adapter (20%)
3. SAS drive backplane (5%)
4. solid-state drive (5%)

1217 A solid-state drive has exceeded the temperature warning threshold.

**Explanation:** The solid-state drive identified by this error has reported that its temperature is higher than the warning threshold.

**User response:** Take steps to reduce the temperature of the drive.
1. Determine the temperature of the room, and reduce the room temperature if this action is appropriate.
2. Replace any failed fans.
3. Ensure that there are no obstructions to air flow for the node.
4. Mark the error as fixed. If the error recurs, contact hardware support for further investigation.

---

1201  1217

Chapter 9. Event reporting  181
Possible Cause-FRUs or other:
  • Solid-state drive (10%)

Other:
  • System environment or airflow blockage (90%)

1220 A remote Fibre Channel port has been excluded.

Explanation: A remote Fibre Channel port has been excluded.

User response:
1. View the event log. Note the MDisk ID associated with the error code.
2. From the MDisk, determine the failing disk controller ID.
3. Refer to the service documentation for the disk controller and the Fibre Channel network to resolve the reported problem.
4. After the disk drive is repaired, start a cluster discovery operation to recover the excluded Fibre Channel port by rescanning the Fibre Channel network.
5. To restore MDisk online status, include the managed disk that you noted in step 1.
6. Check the status of the disk controller. If all disk controllers show a “good” status, mark the error that you have just repaired, “fixed”.
7. If all disk controllers do not show a good status, contact your support center to resolve the problem with the disk controller.
8. Go to repair verification MAP.

Possible Cause-FRUs or other:
  • None

Other:
  • Enclosure/controller fault (50%)
  • Fibre Channel network fabric (50%)

1230 A login has been excluded.

Explanation: A port to port fabric connection, or login, between the cluster node and either a controller or another cluster has had excessive errors. The login has therefore been excluded, and will not be used for I/O operations.

User response: Determine the remote system, which might be either a controller or a SAN Volume Controller cluster. Check the event log for other 1230 errors. Ensure that all higher priority errors are fixed.

This error event is usually caused by a fabric problem. If possible, use the fabric switch or other fabric diagnostic tools to determine which link or port is reporting the errors. If there are error events for links from this node to a number of different controllers or clusters, then it is probably the node to switch link that is causing the errors. Unless there are other contrary indications, first replace the cable between the switch and the remote system.

1. From the fabric analysis, determine the FRU that is most likely causing the error. If this FRU has recently been replaced while resolving a 1230 error, choose the next most likely FRU that has not been replaced recently. Exchange the FRU for a new FRU.
2. Mark the error as fixed. If the FRU replacement has not fixed the problem, the error will be logged again; however, depending on the severity of the problem, the error might not be logged again immediately.
3. Start a cluster discovery operation to recover the login by re-scanning the Fibre Channel network.
4. Check the status of the disk controller or remote cluster. If the status is not “good”, go to the Start MAP.
5. Go to repair verification MAP.

Possible Cause-FRUs or other:
  • Fibre Channel cable, switch to remote port, (30%)
  • Switch or remote device SFP connector or adapter, (30%)
  • Fibre Channel cable, local port to switch, (30%)
  • Cluster SFP connector, (9%)
  • Cluster Fibre Channel adapter, (1%)

Note: The first two FRUs are not cluster FRUs.

1310 A managed disk is reporting excessive errors.

Explanation: A managed disk is reporting excessive errors.

User response:
1. Repair the enclosure/controller fault.
2. Check the managed disk status. If all managed disks show a status of “online”, mark the error that you have just repaired as “fixed”. If any managed disks show a status of “excluded”, include the excluded managed disks and then mark the error as “fixed”.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
  • None

Other:

Enclosure/controller fault (100%)
A solid-state drive is offline due to excessive errors.

**Explanation:** The drive that is reporting excessive errors has been taken offline.

**User response:** In the management GUI, click Troubleshooting > Recommended Actions to run the recommended action for this error. If this does not resolve the issue, contact your next level of support.

A disk I/O medium error has occurred.

**Explanation:** A disk I/O medium error has occurred.

**User response:**
1. Check whether the volume the error is reported against is mirrored. If it is, check if there is a “Mirrored volume offline because a hardware read error has occurred” error relating to this volume in the event log. Also check if one of the mirror copies is synchronizing. If all these tests are true then you must delete the volume copy that is not synchronized from the volume. Check that the volume is online before continuing with the following actions. Wait until the medium error is corrected before trying to re-create the volume mirror.
2. If the medium error was detected by a read from a host, ask the customer to rewrite the incorrect data to the block logical block address (LBA) that is reported in the host systems SCSI sense data. If an individual block cannot be recovered it will be necessary to restore the volume from backup. (If this error has occurred during a migration, the host system does not notice the error until the target device is accessed.)
3. If the medium error was detected during a mirrored volume synchronization, the block might not be being used for host data. The medium error must still be corrected before the mirror can be established. It may be possible to fix the block that is in error using the disk controller or host tools. Otherwise, it will be necessary to use the host tools to copy the volume content that is being used to a new volume. Depending on the circumstances, this new volume can be kept and mirrored, or the original volume can be repaired and the data copied back again.
4. Check managed disk status. If all managed disks show a status of “online”, mark the error that you have just repaired as “fixed”. If any managed disks do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the disk controller.
5. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

A suitable managed disk (MDisk) or drive for use as a quorum disk was not found.

**Explanation:** A quorum disk is needed to enable a tie-break when some cluster members are missing. Three quorum disks are usually defined. By default, the cluster automatically allocates quorum disks when managed disks are created; however, the option exists to manually assign quorum disks. This error is reported when there are managed disks or image mode disks but no quorum disks.

To become a quorum disk:
- The MDisk must be accessible by all nodes in the cluster.
- The MDisk must be managed; that is, it must be a member of a storage pool.
- The MDisk must have free extents.
- The MDisk must be associated with a controller that is enabled for quorum support. If the controller has multiple WWNNs, all of the controller components must be enabled for quorum support.

A quorum disk might not be available because of a Fibre Channel network failure or because of a Fibre Channel switch zoning problem.

**User response:**
1. Resolve any known Fibre Channel network problems.
2. Ask the customer to confirm that MDisks have been added to storage pools and that those MDisks have free extents and are on a controller that is enabled for use as a provider of quorum disks. Ensure that any controller with multiple WWNNs has all of its components enabled to provide quorum disks. Either create a suitable MDisk or if possible enable quorum support on controllers with which existing MDisks are associated. If at least one managed disk shows a mode of managed and has a non-zero quorum index, mark the error that you have just repaired as “fixed”.
3. If the customer is unable to make the appropriate changes, ask your software support center for assistance.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:
- Configuration error (100%)
1335  Quorum disk not available.

Explanation: Quorum disk not available.

User response:
1. View the event log entry to identify the managed disk (MDisk) being used as a quorum disk, that is no longer available.
2. Perform the disk controller problem determination and repair procedures for the MDisk identified in step 1.
3. Include the MDisks into the cluster.
4. Check the managed disk status. If the managed disk identified in step 1 shows a status of “online”, mark the error that you have just repaired as “fixed”. If the managed disk does not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the disk controller.
5. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Enclosure/controller fault (100%)

1340  A managed disk has timed out.

Explanation: This error was reported because a large number of disk timeout conditions have been detected. The problem is probably caused by a failure of some other component on the SAN.

User response:
1. Repair problems on all enclosures/controllers and switches on the same SAN as this 2145 cluster.
2. If problems are found, mark this error as “fixed”.
3. If no switch or disk controller failures can be found, take an event log dump and call your hardware support center.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Enclosure/controller fault
• Fibre Channel switch

1360  A SAN transport error occurred.

Explanation: This error has been reported because the 2145 performed error recovery procedures in response to SAN component associated transport errors. The problem is probably caused by a failure of a component of the SAN.

User response:
1. View the event log entry to determine the node that logged the problem. Determine the 2145 node or controller that the problem was logged against.
2. Perform Fibre Channel switch problem determination and repair procedures for the switches connected to the 2145 node or controller.
3. Perform Fibre Channel cabling problem determination and repair procedures for the cables connected to the 2145 node or controller.
4. If any problems are found and resolved in step 2 and 3, mark this error as “fixed”.
5. If no switch or cable failures were found in steps 2 and 3, take an event log dump. Call your hardware support center.
6. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Enclosure/controller fault
1400  The 2145 cannot detect an Ethernet connection.

Explanation: The 2145 cannot detect an Ethernet connection.

User response:
1. Go to the Ethernet MAP.
2. Go to the repair verification MAP.

Possible Cause-FRUs or other:
2145-8G4, 2145-8A4, 2145-CF8, or 2145-CG8
- Ethernet cable (25%)
- System board (25%)

Other:
- Ethernet cable is disconnected or damaged (25%)
- Ethernet hub fault (25%)

1550  A cluster path has failed.

Explanation: One of the 2145 Fibre Channel ports is unable to communicate with all the other 2145s in the cluster.

User response:
1. Check for incorrect switch zoning.
2. Repair the fault in the Fibre Channel network fabric.
3. Check the status of the node ports that are not excluded via the system’s local port mask. If the status of the node ports shows as active, mark the error that you have just repaired as “fixed”. If any node ports do not show a status of active, go to start MAP. If you return to this step contact your support center to resolve the problem with the 2145.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:
Fibre Channel network fabric fault (100%)

1600  Mirrored disk repair halted because of difference.

Explanation: During the repair of a mirrored volume two copy disks were found to contain different data for the same logical block address (LBA). The validate option was used, so the repair process has halted.

Read operations to the LBAs that differ might return the data of either volume copy. Therefore it is important not to use the volume unless you are sure that the host applications will not read the LBAs that differ or can manage the different data that potentially can be returned.

User response: Perform one of the following actions:
- Continue the repair starting with the next LBA after the difference to see how many differences there are for the whole mirrored volume. This can help you decide which of the following actions to take.
- Choose a primary disk and run repair resynchronizing differences.
- Run a repair and create medium errors for differences.
- Restore all or part of the volume from a backup.
- Decide which disk has correct data, then delete the copy that is different and re-create it allowing it to be synchronized.
Then mark the error as “fixed”.

Possible Cause-FRUs or other:
• None

**1610**

| There are too many copied media errors on a managed disk. |

**Explanation:** The cluster maintains a virtual medium error table for each MDisk. This table is a list of logical block addresses on the managed disk that contain data that is not valid and cannot be read. The virtual medium error table has a fixed length. This error event indicates that the system has attempted to add an entry to the table, but the attempt has failed because the table is already full.

There are two circumstances that will cause an entry to be added to the virtual medium error table:

1. FlashCopy, data migration and mirrored volume synchronization operations copy data from one managed disk extent to another. If the source extent contains either a virtual medium error or the RAID controller reports a real medium error, the system creates a matching virtual medium error on the target extent.

2. The mirrored volume validate and repair process has the option to create virtual medium errors on sectors that do not match on all volume copies. Normally zero, or very few, differences are expected; however, if the copies have been marked as synchronized inappropriately, then a large number of virtual medium errors could be created.

**User response:** Ensure that all higher priority errors are fixed before you attempt to resolve this error.

Determine whether the excessive number of virtual medium errors occurred because of a mirrored disk validate and repair operation that created errors for differences, or whether the errors were created because of a copy operation. Follow the corresponding option shown below.

1. If the virtual medium errors occurred because of a mirrored disk validate and repair operation that created medium errors for differences, then also ensure that the volume copies had been fully synchronized prior to starting the operation. If the copies had been synchronized, there should be only a few virtual medium errors created by the validate and repair operation. In this case, it might be possible to rewrite only the data that was not consistent on the copies using the local data recovery process. If the copies had not been synchronized, it is likely that there are now a large number of medium errors on all of the volume copies. Even if the virtual medium errors are expected to be only for blocks that have never been written, it is important to clear the virtual medium errors to avoid inhibition of other operations. To recover the data for all of these virtual medium errors it is likely that the volume will have to be recovered from a backup using a process that rewrites all sectors of the volume.

2. If the virtual medium errors have been created by a copy operation, it is best practice to correct any medium errors on the source volume and to not propagate the medium errors to copies of the volume. Fixing higher priority errors in the event log would have corrected the medium error on the source volume. Once the medium errors have been fixed, you must run the copy operation again to clear the virtual medium errors from the target volume. It might be necessary to repeat a sequence of copy operations if copies have been made of already copied medium errors.

An alternative that does not address the root cause is to delete volumes on the target managed disk that have the virtual medium errors. This volume deletion reduces the number of virtual medium error entries in the MDisk table. Migrating the volume to a different managed disk will also delete entries in the MDisk table, but will create more entries on the MDisk table of the MDisk to which the volume is migrated.

Possible Cause-FRUs or other:
• None

**1620**

| A storage pool is offline. |

**Explanation:** A storage pool is offline.

**User response:**
1. Repair the faults in the order shown.
2. Start a cluster discovery operation by rescanning the Fibre Channel network.
3. Check managed disk (MDisk) status. If all MDisks show a status of “online”, mark the error that you have just repaired as “fixed”. If any MDisks do not show a status of “online”, go to start MAP. If you return to this step, contact your support center to resolve the problem with the disk controller.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Fibre Channel network fabric fault (50%)
• Enclosure/controller fault (50%)

**1623**

| One or more MDisks on a controller are degraded. |

**Explanation:** At least one MDisk on a controller is degraded because the MDisk is not available through one or more nodes. The MDisk is available through at least one node. Access to data might be lost if another failure occurs.
In a correctly configured system, each node accesses all of the MDisks on a controller through all of the controller's ports.

This error is only logged once per controller. There might be more than one MDisk on this controller that has been configured incorrectly, but the error is only logged for one MDisk.

To prevent this error from being logged because of short-term fabric maintenance activities, this error condition must have existed for one hour before the error is logged.

**User response:**
1. Determine which MDisks are degraded. Look for MDisks with a path count lower than the number of nodes. Do not use only the MDisk status, since other errors can also cause degraded MDisks.
2. Ensure that the controller is zoned correctly with all of the nodes.
3. Ensure that the logical unit is mapped to all of the nodes.
4. Ensure that the logical unit is mapped to all of the nodes using the same LUN.
5. Run the console or CLI command to discover MDisks and ensure that the command completes.
6. Mark the error that you have just repaired as “fixed”. When you mark the error as “fixed”, the controller's MDisk availability is tested and the error will be logged again immediately if the error persists for any MDisks. It is possible that the new error will report a different MDisk.
7. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:
- Fibre Channel network fabric fault (50%)
- Enclosure/controller fault (50%)

**Controller configuration has unsupported RDAC mode.**

**Explanation:** The cluster has detected that an IBM DS series disk controller's configuration is not supported by the cluster. The disk controller is operating in RDAC mode. The disk controller might appear to be operating with the cluster; however, the configuration is unsupported because it is known to not work with the cluster.

**User response:**
1. Using the IBM DS series console, ensure that the host type is set to 'IBM TS SAN VCE' and that the AVT option is enabled. (The AVT and RDAC options are mutually exclusive).
2. Mark the error that you have just repaired as “fixed”. If the problem has not been fixed it will be logged again; this could take a few minutes.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:
- Enclosure/controller fault

**The cluster has insufficient redundancy in its controller connectivity.**

**Explanation:** The cluster has detected that it does not have sufficient redundancy in its connections to the disk controllers. This means that another failure in the SAN could result in loss of access to the application data. The cluster SAN environment should have redundant connections to every disk controller. This redundancy allows for continued operation when there is a failure in one of the SAN components.

To provide recommended redundancy, a cluster should be configured so that:
- each node can access each disk controller through two or more different initiator ports on the node.
- each node can access each disk controller through two or more different controller target ports. **Note:** Some disk controllers only provide a single target port.
• each node can access each disk controller target port through at least one initiator port on the node.

If there are no higher-priority errors being reported, this error usually indicates a problem with the SAN design, a problem with the SAN zoning or a problem with the disk controller.

If there are unfixed higher-priority errors that relate to the SAN or to disk controllers, those errors should be fixed before resolving this error because they might indicate the reason for the lack of redundancy. Error codes that must be fixed first are:

• 1210 Local FC port excluded
• 1230 Login has been excluded

Note: This error can be reported if the required action, to rescan the Fibre Channel network for new MDisks, has not been performed after a deliberate reconfiguration of a disk controller or after SAN rezoning.

The 1627 error code is reported for a number of different error IDs. The error ID indicates the area where there is a lack of redundancy. The data reported in an event log entry indicates where the condition was found.

The meaning of the error IDs is shown below. For each error ID the most likely reason for the condition is given. If the problem is not found in the suggested areas, check the configuration and state of all of the SAN components (switches, controllers, disks, cables and cluster) to determine where there is a single point of failure.

010040 A disk controller is only accessible from a single node port.
• A node has detected that it only has a connection to the disk controller through exactly one initiator port, and more than one initiator port is operational.
• The error data indicates the device WWNN and the WWPN of the connected port.
• A zoning issue or a Fibre Channel connection hardware fault might cause this condition.

010041 A disk controller is only accessible from a single port on the controller.
• A node has detected that it is only connected to exactly one target port on a disk controller, and more than one target port connection is expected.
• The error data indicates the WWPN of the disk controller port that is connected.
• A zoning issue or a Fibre Channel connection hardware fault might cause this condition.

010042 Only a single port on a disk controller is accessible from every node in the cluster.
• Only a single port on a disk controller is accessible to every node when there are multiple ports on the controller that could be connected.
• The error data indicates the WWPN of the disk controller port that is connected.
• A zoning issue or a Fibre Channel connection hardware fault might cause this condition.

010043 A disk controller is accessible through only half, or less, of the previously configured controller ports.
• Although there might still be multiple ports that are accessible on the disk controller, a hardware component of the controller might have failed or one of the SAN fabrics has failed such that the operational system configuration has been reduced to a single point of failure.
• The error data indicates a port on the disk controller that is still connected, and also lists controller ports that are expected but that are not connected.
• A disk controller issue, switch hardware issue, zoning issue or cable fault might cause this condition.

010044 A disk controller is not accessible from a node.
• A node has detected that it has no access to a disk controller. The controller is still accessible from the partner node in the I/O group, so its data is still accessible to the host applications.
• The error data indicates the WWPN of the missing disk controller.
• A zoning issue or a cabling error might cause this condition.

User response:
1. Check the error ID and data for a more detailed description of the error.
2. Determine if there has been an intentional change to the SAN zoning or to a disk controller configuration that reduces the cluster’s access to the indicated disk controller. If either action has occurred, continue with step 8.
3. Use the GUI or the CLI command lsfabric to ensure that all disk controller WWPNs are reported as expected.
4. Ensure that all disk controller WWPNs are zoned appropriately for use by the cluster.
5. Check for any unfixed errors on the disk controllers.
6. Ensure that all of the Fibre Channel cables are connected to the correct ports at each end.
7. Check for failures in the Fibre Channel cables and connectors.
8. When you have resolved the issues, use the GUI or the CLI command detectmdisk to rescan the Fibre Channel network for changes to the MDisks.

Note: Do not attempt to detect MDisks unless you
are sure that all problems have been fixed.
Detecting MDisks prematurely might mask an issue.
9. Mark the error that you have just repaired as fixed. The cluster will revalidate the redundancy and will report another error if there is still not sufficient redundancy.
10. Go to MAP 5700: Repair verification.

Possible Cause-FRU$s or other:
• None

1630 The number of device logins was reduced.

Explanation: The number of port to port fabric connections, or logins, between the node and a storage controller has decreased. This might be caused by a problem on the SAN or by a deliberate reconfiguration of the SAN.

User response:
1. Check the error in the cluster event log to identify the object ID associated with the error.
2. Check the availability of the failing device using the following command line: `lscontroller object_ID`. If the command fails with the message “CMMVC6014E The command failed because the requested object is either unavailable or does not exist,” ask the customer if this device was removed from the system.
   • If “yes”, mark the error as fixed in the cluster event log and continue with the repair verification MAP.
   • If “no” or if the command lists details of the failing controller, continue with the next step.
3. Check whether the device has regained connectivity. If it has not, check the cable connection to the remote-device port.
4. If all attempts to log in to a remote-device port have failed and you cannot solve the problem by changing cables, check the condition of the remote-device port and the condition of the remote device.
5. Start a cluster discovery operation by rescanning the Fibre Channel network.
6. Check the status of the disk controller. If all disk controllers show a “good” status, mark the error that you have just repaired as “fixed”. If any disk controllers do not show “good” status, go to start MAP. If you return to this step, contact the support center to resolve the problem with the disk controller.
7. Go to repair verification MAP.

Possible Cause-FRU$s or other:
• None

Other:
• Fibre Channel network fabric fault (50%)
• Enclosure/controller fault (50%)

1660 The initialization of the managed disk has failed.

Explanation: The initialization of the managed disk has failed.

User response:
1. View the event log entry to identify the managed disk (MDisk) that was being accessed when the problem was detected.
2. Perform the disk controller problem determination and repair procedures for the MDisk identified in step 1.
3. Include the MDisk into the cluster.
4. Check the managed disk status. If all managed disks show a status of “online”, mark the error that you have just repaired as “fixed”. If any managed disks do not show a status of “online”, go to the start MAP. If you return to this step, contact your support center to resolve the problem with the disk controller.
5. Go to repair verification MAP.

Possible Cause-FRU$s or other:
• None

Other:
Enclosure/controller fault (100%)

1670 The CMOS battery on the 2145 system board failed.

Explanation: The CMOS battery on the 2145 system board failed.

User response:
1. Replace the CMOS battery.
2. Mark the error that you have just repaired as “fixed”.
3. Go to repair verification MAP.

Possible Cause-FRU$s or other:

CMOS battery (100%)

1691 A background scrub process has found an inconsistency between data and parity on the array.

Explanation: The array has at least one stride where the data and parity do not match. RAID has found an inconsistency between the data stored on the drives and the parity information. This could either mean that
User response: Follow the directed maintenance procedure for inconsistent arrays.

1695 Persistent unsupported disk controller configuration.

Explanation: A disk controller configuration that might prevent failover for the cluster has persisted for more than four hours. The problem was originally logged through a 010032 event, service error code 1625.

User response:
1. Fix any higher priority error. In particular, follow the service actions to fix the 1625 error indicated by this error's root event. This error will be marked as "fixed" when the root event is marked as "fixed".
2. If the root event cannot be found, or is marked as "fixed", perform an MDisk discovery and mark this error as "fixed".
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• Enclosure/controller fault

1710 There are too many cluster partnerships. The number of cluster partnerships has been reduced.

Explanation: A cluster can have a Metro Mirror and Global Mirror cluster partnership with one or more other clusters. Partnership sets consist of clusters that are either in direct partnership with each other or are in indirect partnership by having a partnership with the same intermediate cluster. The topology of the partnership set is not fixed; the topology might be a star, a loop, a chain or a mesh. The maximum supported number of clusters in a partnership set is four. A cluster is a member of a partnership set if it has a partnership with another cluster in the set, regardless of whether that partnership has any defined consistency groups or relationships.

These are examples of valid partnership sets for five unique clusters labelled A, B, C, D, and E where a partnership is indicated by a dash between two cluster names:
• A-B, A-C, A-D. E has no partnerships defined and therefore is not a member of the set.
• A-B, A-D, B-C, B-D, C-D. E has no partnerships defined and therefore is not a member of the set.
• A-B, A-C, A-D, B-C, C-D. E has no partnerships defined and therefore is not a member of the set.
• A-B, A-C, B-D. E. There are two partnership sets. One contains clusters A, B, and C. The other contains clusters D and E.

These are examples of unsupported configurations because the number of clusters in the set is five, which exceeds the supported maximum of four clusters:
• A-B, A-D, B-C, C-D, C-E.
• A-B, B-C, C-D, D-E.

The cluster prevents you from creating a new Metro Mirror and Global Mirror cluster partnership if a resulting partnership set would exceed the maximum of four clusters. However, if you restore a broken link between two clusters that have a partnership, the number of clusters in the set might exceed four. If this
occurs, Metro Mirror and Global Mirror cluster partnerships are excluded from the set until only four clusters remain in the set. A cluster partnership that is excluded from a set has all of its Metro Mirror and Global Mirror cluster partnerships excluded.

Event ID 0x050030 is reported if the cluster is retained in the partnership set. Event ID 0x050031 is reported if the cluster is excluded from the partnership set. All clusters that were in the partnership set report error 1710.

All inter-cluster Metro Mirror or Global Mirror relationships that involve an excluded cluster will lose connectivity. If any of these relationships are in the consistent_synch state and they receive a write I/O, they will stop with error code 1720.

**User response:** To fix this error it is necessary to delete all of the relationships that could not be recovered and then re-create the relationships.

1. Determine which clusters are still connected and members of the partnership set, and which clusters have been excluded.
2. Determine the Metro Mirror and Global Mirror relationships that exist on those clusters.
3. Determine which of the Metro Mirror and Global Mirror relationships you want to maintain, which determines which cluster partnerships you want to maintain. Ensure that the partnership set or sets that would result from configuring the cluster partnerships that you want contain no more than four clusters in each set. NOTE: The reduced partnership set created by the cluster might not contain the clusters that you want in the set.
4. Remove all of the Metro Mirror and Global Mirror relationships that you do not want to retain.
5. Remove all of the Metro Mirror and Global Mirror cluster partnerships that you do not want to retain.
6. Restart all relationships and consistency groups that were stopped.
7. Go to repair verification MAP.

Possible Cause-FRUs or other:

- None

### 1800 The SAN has been zoned incorrectly.

**Explanation:** This has resulted in more than 512 other ports on the SAN logging into one port of a 2145 node.

**User response:**

1. Ask the user to reconfigure the SAN.
2. Mark the error as “fixed”.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:

- None

Other:

- Fibre Channel switch configuration error
- Fibre Channel switch

### 1801 A node has received too many Fibre Channel logins from another node.

**Explanation:** This event was logged because the node has received more than sixteen Fibre Channel logins originating from another node. This indicates that the Fibre Channel storage area network that connects the two nodes is not correctly configured.

**Data:**

- None

**User response:** Change the zoning and/or Fibre Channel port masking so that no more than 16 logins are possible between a pair of nodes.

See Non-critical node error “888” on page 164 for details.

Use the `lsfabric` command to view the current number of logins between nodes.

Possible Cause-FRUs or other cause:

- None

### 1840 The managed disk has bad blocks.

**Explanation:** These are “virtual” medium errors which are created when copying a volume where the source has medium errors. During data moves or duplication, such as during a flash copy, an attempt is made to
move medium errors; to achieve this, virtual medium errors called "bad blocks" are created. Once a bad block has been created, no attempt will be made to read the underlying data, as there is no guarantee that the old data still exists once the "bad block" is created. Therefore, it is possible to have "bad blocks", and thus medium errors, reported on a target vdisk, without medium errors actually existing on the underlying storage. The "bad block" records are removed when the data is overwritten by a host.

**Note:** On an external controller, this error can only result from a copied medium error.

**User response:**
1. The support center will direct the user to restore the data on the affected volumes.
2. When the volume data has been restored, or the user has chosen not to restore the data, mark the error as "fixed".
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

---

### 1850 Compressed volume copy has bad blocks

**Explanation:** A system recovery operation was performed, but data on one or more volumes was not recovered; this is normally caused by a combination of hardware faults. If data containing a medium error is copied or migrated to another volume, bad blocks will be recorded. If a host attempts to read the data in any of the bad block regions, the read will fail with a medium error.

**User response:**
1. The support center will direct the user to restore the data on the affected volumes.
2. When the volume data has been restored, or the user has chosen not to restore the data, mark the error as "fixed".
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

### 1862 Thin-provisioned volume copy offline because of corrupt metadata.

**Explanation:** A thin-provisioned volume has been taken offline because there is an inconsistency in the cluster metadata that describes the disk contents. This might occur because of corruption of data on the physical disk (e.g., medium error or data miscompare), the loss of cached metadata (because of a cluster recovery) or because of a software error. The event data gives information on the reason.

The cluster maintains backup copies of the metadata and it might be possible to repair the thin-provisioned volume using this data.

**User response:** The cluster is able to repair the inconsistency in some circumstances. Run the repair volume option to start the repair process. This repair process, however, can take some time. In some situations it might be more appropriate to delete the thin-provisioned volume and reconstruct a new one from a backup or mirror copy.

If you run the repair procedure and it completes, this error is automatically marked as "fixed"; otherwise, another error event (error code 1860) is logged to indicate that the repair action has failed.

Possible Cause-FRUs or other:
- None

### 1865 Thin-provisioned volume copy offline because of insufficient space.

**Explanation:** A thin-provisioned volume has been taken offline because there is insufficient allocated real capacity available on the volume for the used space to increase further. If the thin-provisioned volume is auto-expand enabled, then the storage pool it is in also has no free space.

**User response:** The service action differs depending on whether the thin-provisioned volume copy is auto-expand enabled or not. Whether the disk is auto-expand enabled or not is indicated in the error event data.

If the volume copy is auto-expand enabled, perform one or more of the following actions. When you have performed all of the actions that you intend to perform, mark the error as "fixed"; the volume copy will then return online.

- Determine why the storage pool free space has been depleted. Any of the thin-provisioned volume copies, with auto-expand enabled, in this storage pool might have expanded at an unexpected rate; this could
indicate an application error. New volume copies might have been created in, or migrated to, the storage pool.

- Increase the capacity of the storage pool that is associated with the thin-provisioned volume copy by adding more MDisks to the group.
- Provide some free capacity in the storage pool by reducing the used space. Volume copies that are no longer required can be deleted, the size of volume copies can be reduced or volume copies can be migrated to a different storage pool.
- Migrate the thin-provisioned volume copy to a storage pool that has sufficient unused capacity.
- Consider reducing the value of the storage pool warning threshold to give more time to allocate extra space.

If the volume copy is not auto-expand enabled, perform one or more of the following actions. In this case the error will automatically be marked as “fixed”, and the volume copy will return online when space is available.

- Determine why the thin-provisioned volume copy used space has grown at the rate that it has. There might be an application error.
- Increase the real capacity of the volume copy.
- Enable auto-expand for the thin-provisioned volume copy.
- Consider reducing the value of the thin-provisioned volume copy warning threshold to give more time to allocate more real space.

Possible Cause-FRUs or other:
- None

1870  Mirrored volume offline because a hardware read error has occurred.

Explanation: While attempting to maintain the volume mirror, a hardware read error occurred on all of the synchronized volume copies.

The volume copies might be inconsistent, so the volume is now offline.

User response:
- Fix all higher priority errors. In particular, fix any read errors that are listed in the sense data. This error event will automatically be fixed when the root event is marked as “fixed”.
- If you cannot fix the root error, but the read errors on some of the volume copies have been fixed, mark this error as “fixed” to run without the mirror. You can then delete the volume copy that cannot read data and re-create it on different MDisks.

Possible Cause-FRUs or other:
- None

1895  Unrecovered FlashCopy mappings

Explanation: This error might be reported after the recovery action for a cluster failure or a complete I/O group failure. The error is reported because some FlashCopies, whose control data is stored by the I/O group, were active at the time of the failure and the current state of the mapping could not be recovered.

User response: To fix this error it is necessary to delete all of the FlashCopy mappings on the I/O group that failed.

1. Note the I/O group index against which the error is logged.
2. List all of the FlashCopy mappings that are using this I/O group for their bitmaps. You should get the detailed view of every possible FlashCopy ID. Note the IDs of the mappings whose IO_group_id matches the ID of the I/O group against which this error is logged.
3. Note the details of the FlashCopy mappings that are listed so that they can be re-created.
4. Delete all of the FlashCopy mappings that are listed. Note: The error will automatically be marked as “fixed” once the last mapping on the I/O group is deleted. New mappings cannot be created until the error is fixed.
5. Using the details noted in step 3, re-create all of the FlashCopy mappings that you just deleted.

Possible Cause-FRUs or other:
- None

1900  A FlashCopy, Trigger Prepare command has failed because a cache flush has failed.

Explanation: A FlashCopy, Trigger Prepare command has failed because a cache flush has failed.

User response:
1. Correct higher priority errors, and then try the Trigger Prepare command again.
2. Mark the error that you have just repaired as “fixed”.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
- None

Other:

Cache flush error (100%)
1910 A FlashCopy mapping task was stopped because of the error that is indicated in the sense data.

Explanation: A stopped FlashCopy might affect the status of other volumes in the same I/O group. Preparing the stopped FlashCopy operations as soon as possible is advised.

User response:
1. Correct higher priority errors, and then prepare and start the FlashCopy task again.
2. Mark the error that you have just repaired as “fixed”.
3. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

1920 Global and Metro Mirror persistent error.

Explanation: This error might be caused by a problem on the primary cluster, a problem on the secondary cluster, or a problem on the inter-cluster link. The problem might be a failure of a component, a component becoming unavailable or having reduced performance because of a service action or it might be that the performance of a component has dropped to a level where the Metro Mirror or Global Mirror relationship cannot be maintained. Alternatively the error might be caused by a change in the performance requirements of the applications using Metro Mirror or Global Mirror.

This error is reported on the primary cluster when the copy relationship has not progressed sufficiently over a period of time. Therefore, if the relationship is restarted before all of the problems are fixed, the error might be reported again when the time period next expires (the default period is five minutes).

This error might also be reported because the primary cluster has encountered read errors.

You might need to refer to the Copy Services features information in the software installation and configuration documentation while diagnosing this error.

User response:
1. If the 1920 error has occurred previously on Metro Mirror or Global Mirror between the same clusters and all the following actions have been attempted, contact your product support center to resolve the problem.
2. On both clusters, check the partner fc port mask to ensure that there is sufficient connectivity. If the partner fc port mask was changed recently, ensure the mask is correct.
3. On the primary cluster reporting the error, correct any higher priority errors.
4. On the secondary cluster, review the maintenance logs to determine if the cluster was operating with reduced capability at the time the error was reported. The reduced capability might be because of a software upgrade, hardware maintenance to a 2145 node, maintenance to a backend disk system or maintenance to the SAN.
5. On the secondary 2145 cluster, correct any errors that are not fixed.
6. On the intercluster link, review the logs of each link component for any incidents that would cause reduced capability at the time of the error. Ensure the problems are fixed.
7. If a reason for the error has been found and corrected, go to Action 11.
8. On the primary cluster reporting the error, examine the 2145 statistics using a SAN productivity monitoring tool and confirm that all the Metro Mirror and Global Mirror requirements described in the planning documentation are met. Ensure that any changes to the applications using Metro Mirror or Global Mirror have been taken into account. Resolve any issues.
9. On the secondary cluster, examine the 2145 statistics using a SAN productivity monitoring tool and confirm that all the Metro Mirror and Global Mirror requirements described in the software installation and configuration documentation are met. Resolve any issues.
10. On the intercluster link, examine the performance of each component using an appropriate SAN productivity monitoring tool to ensure that they are operating as expected. Resolve any issues.
11. Mark the error as “fixed” and restart the Metro Mirror or Global Mirror relationship.

When you restart the Metro Mirror or Global Mirror relationship there will be an initial period during which Metro Mirror or Global Mirror performs a background copy to resynchronize the volume data on the primary and secondary clusters. During this period the data on the Metro Mirror or Global Mirror auxiliary volumes on the secondary cluster is inconsistent and the volumes could not be used as backup disks by your applications.

Note: To ensure the system has the capacity to handle the background copy load you may want to delay restarting the Metro Mirror or Global Mirror relationship until there is a quiet period when the secondary cluster and the SAN fabric (including the intercluster link) have the required capacity. If the required capacity is not available you might experience another 1920 error and the Metro Mirror or Global Mirror relationship will stop in an inconsistent state.
Note: If the Metro Mirror or Global Mirror relationship has stopped in a consistent state (“consistent-stopped”) it is possible to use the data on the Metro Mirror or Global Mirror auxiliary volumes on the secondary cluster as backup disks by your applications. You might therefore want to start a Flash Copy of your Metro Mirror or Global Mirror auxiliary disks on the secondary system before restarting the Metro Mirror or Global Mirror relationship. This means you maintain the current, consistent, image until the time when the Metro Mirror or Global Mirror relationship is again synchronized and in a consistent state.

Possible Cause-FRUs or other:
• None

Other:
• Primary 2145 cluster or SAN fabric problem (10%)
• Primary 2145 cluster or SAN fabric configuration (10%)
• Secondary 2145 cluster or SAN fabric problem (15%)
• Secondary 2145 cluster or SAN fabric configuration (25%)
• Intercluster link problem (15%)
• Intercluster link configuration (25%)

1930  Migration suspended.
Explanation: Migration suspended.
User response:
1. Ensure that all error codes of a higher priority have already been fixed.
2. Ask the customer to ensure that all storage pools that are the destination of suspended migrate operations have available free extents.
3. Mark this error as “fixed”. This causes the migrate operation to be restarted. If the restart fails, a new error is logged.
4. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

2008 A software downgrade has failed.
Explanation: Cluster configuration changes are restricted until the downgrade is completed. The cluster downgrade process waits for user intervention when this error is logged.

User response: The action required to recover from a stalled downgrade depends on the current state of the cluster being downgraded. Call IBM Support for an action plan to resolve this problem.
Possible Cause-FRUs or other:
• None

Other:
• 2145 software (100%)

2010 A software upgrade has failed.
Explanation: Cluster configuration changes are restricted until the upgrade is completed or rolled back. The cluster upgrade process waits for user intervention when this error is logged.

User response: The action required to recover from a stalled upgrade depends on the current state of the cluster being upgraded. Call IBM technical support for an action plan to resolve this problem.
Possible Cause-FRUs or other:
2020  IP Remote Copy link unavailable.

Explanation: IP Remote Copy link is unavailable.

User response: Fix the remote IP link so that traffic can flow correctly. Once the connection is made, the error will auto-correct.

2021  Partner cluster IP address unreachable.

Explanation: Partner cluster IP address unreachable.

User response:
1. Verify the system IP address of the remote system forming the partnership.
2. Check if remote cluster IP address is reachable from local cluster. The following can be done to verify accessibility:
   a. Use `svctask` to ping the remote cluster IP address. If the ping works, there may be a block on the specific port traffic that needs to be opened in the network. If the ping does not work, there may be no route between the system. Check the IP gateway configuration on the SAN Volume Controller nodes and the IP network configuration.
   b. Check the configuration of the routers and firewall to ensure that TCP/IP port 3620 used for IP replication is not blocked.
   c. Use the `ssh` command from another system to attempt to establish a session with the problematic remote cluster IP address to confirm that the remote cluster is operational.

2022  Cannot authenticate with partner cluster.

Explanation: Cannot authenticate with partner cluster.

User response: Verify the CHAP secret set of partnership using `mkppartnership` or `chpartnership` CLIs match remote system CHAP secret set using `chsystem` CLI. If they don’t match, use appropriate commands to set the right CHAP secrets.

2023  Unexpected cluster ID for partner cluster.

Explanation: Unexpected cluster ID for partner cluster.

User response: After deleting all relationships and consistency group, remove the partnership.

This is an unrecoverable error when one of the sites has undergone a T3 recovery and lost all partnership information. Contact IBM support.

2030  Software error.

Explanation: The 2145 software has restarted because of a problem in the cluster, on a disk system or on the Fibre Channel fabric.

User response:
1. Collect the software dump file(s) generated at the time the error was logged on the cluster.
2. Contact your product support center to investigate and resolve the problem.
3. Ensure that the software is at the latest level on the cluster and on the disk systems.
4. Use the available SAN monitoring tools to check for any problems on the fabric.
5. Mark the error that you have just repaired as “fixed”.
6. Go to repair verification Map.

Possible Cause-FRUs or other:
• Your support center might indicate a FRU based on their problem analysis (2%)

Other:
• 2145 software (48%)
• Enclosure/controller software (25%)
• Fibre Channel switch or switch configuration (25%)

2040  A software upgrade is required.

Explanation: The software cannot determine the VPD for a FRU. Probably, a new FRU has been installed and the software does not recognize that FRU.

User response:
1. If a FRU has been replaced, ensure that the correct replacement part was used. The node VPD indicates which part is not recognized.
2. Ensure that the cluster software is at the latest level.
3. Save dump data with configuration dump and logged data dump.
4. Contact your product support center to resolve the problem.
5. Mark the error that you have just repaired as “fixed”.
6. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:
• None

2145 software (100%)
2080 Storage system connected to unsupported port.

**Explanation:** Storage system connected to unsupported port

**User response:**
1. Only one error is logged for one node. The second error will override the first one. To get a complete view of the problems:
   a. Check `lsportfc` command.
   b. Get WWPN from `fc_io_port_id` for ports 7 and 8.
   c. Check if any controller is connected to ports 7 or 8 by `lsfabric`.
2. To manage the storage system from the IO group, change zoning so it is visible on only FC IO ports 1-6, otherwise zone it out.
3. The event will be marked as fixed automatically if the problem is fixed. If not marked as fixed, the problem still exists. Do step 1 again.

Possible Cause-FRUs or other:
• None

2100 A software error has occurred.

**Explanation:** One of the 2145 server software components (sshd, crond, or httpd) has failed and reported an error.

**User response:**
1. Ensure that the software is at the latest level on the cluster.
2. Save dump data with configuration dump and logged data dump.
3. Contact your product support center to resolve the problem.
4. Mark the error that you have just repaired as “fixed”.
5. Go to repair verification MAP.

Possible Cause-FRUs or other:
• None

Other:

2145 software (100%)

2500 A secure shell (SSH) session limit for the cluster has been reached.

**Explanation:** Secure Shell (SSH) sessions are used by applications that manage the cluster. An example of such an application is the command-line interface (CLI). An application must initially log in to the cluster to create an SSH session. The cluster imposes a limit on the number of SSH sessions that can be open at one time. This error indicates that the limit on the number of SSH sessions has been reached and that no more logins can be accepted until a current session logs out.

The limit on the number of SSH sessions is usually reached because multiple users have opened an SSH session but have forgotten to close the SSH session when they are no longer using the application.

**User response:**
• Because this error indicates a problem with the number of sessions that are attempting external access to the cluster, determine the reason that so many SSH sessions have been opened.
• Run the Fix Procedure for this error on the panel at Management GUI Troubleshooting > Recommended Actions to view and manage the open SSH sessions.

2600 The cluster was unable to send an email.

**Explanation:** The cluster has attempted to send an email in response to an event, but there was no acknowledgement that it was successfully received by the SMTP mail server. It might have failed because the cluster was unable to connect to the configured SMTP server, the email might have been rejected by the server, or a timeout might have occurred. The SMTP server might not be running or might not be correctly configured, or the cluster might not be correctly configured. This error is not logged by the test email function because it responds immediately with a result code.

**User response:**
• Ensure that the SMTP email server is active.
• Ensure that the SMTP server TCP/IP address and port are correctly configured in the cluster email configuration.
• Send a test email and validate that the change has corrected the issue.
• Mark the error that you have just repaired as fixed.
• Go to MAP 5700: Repair verification.

Possible Cause-FRUs or other:
• None

2601 Error detected while sending an email.

**Explanation:** An error has occurred while the cluster was attempting to send an email in response to an event. The cluster is unable to determine if the email has been sent and will attempt to resend it. The problem might be with the SMTP server or with the cluster email configuration. The problem might also be caused by a failover of the configuration node. This error is not logged by the test email function because it responds immediately with a result code.
User response:
- If there are higher-priority unfixed errors in the log, fix those errors first.
- Ensure that the SMTP email server is active.
- Ensure that the SMTP server TCP/IP address and port are correctly configured in the cluster email configuration.
- Send a test email and validate that the change has corrected the issue.
- Mark the error that you have just repaired as fixed.
- Go to MAP 5700: Repair verification.

Possible Cause-FRUs or other:
- None

2700 Unable to access NTP network time server
Explanation: Cluster time cannot be synchronized with the NTP network time server that is configured.
User response: There are three main causes to examine:
- The cluster NTP network time server configuration is incorrect. Ensure that the configured IP address matches that of the NTP network time server.
- The NTP network time server is not operational. Check the status of the NTP network time server.
- The TCP/IP network is not configured correctly. Check the configuration of the routers, gateways and firewalls. Ensure that the cluster can access the NTP network time server and that the NTP protocol is permitted.

The error will automatically fix when the cluster is able to synchronize its time with the NTP network time server.

Possible Cause-FRUs or other:
- None

3000 The 2145 UPS temperature is close to its upper limit. If the temperature continues to rise the 2145 UPS will power off.
Explanation: The temperature sensor in the 2145 UPS is reporting a temperature that is close to the operational limit of the unit. If the temperature continues to rise the 2145 UPS will power off for safety reasons. The sensor is probably reporting an excessively high temperature because the environment in which the 2145 UPS is operating is too hot.
User response:
1. Ensure that the room ambient temperature is within the permitted limits.
2. Ensure that the air vents at the front and back of the 2145 UPS are not obstructed.
3. Ensure that other devices in the same rack are not overheating.
4. When you are satisfied that the cause of the overheating has been resolved, mark the error “fixed”.

3010 Internal uninterruptible power supply software error detected.
Explanation: Some of the tests that are performed during node startup did not complete because some of the data reported by the uninterruptible power supply during node startup is inconsistent because of a software error in the uninterruptible power supply. The node has determined that the uninterruptible power supply is functioning sufficiently for the node to continue operations. The operation of the cluster is not affected by this error. This error is usually resolved by power cycling the uninterruptible power supply.
User response:
1. Power cycle the uninterruptible power supply at a convenient time. The one or two nodes attached to the uninterruptible power supply should be powered off before powering off the uninterruptible power supply. Once the nodes have powered down, wait 5 minutes for the uninterruptible power supply to go into standby mode (flashing green AC LED). If this does not happen automatically then check the cabling to confirm that all nodes powered by this uninterruptible power supply have been powered off. Remove the power input cable from the uninterruptible power supply and wait at least 2 minutes for the uninterruptible power supply to
clear its internal state. Reconnect the uninterruptible power supply power input cable. Press the uninterruptible power supply ON button. Power on the nodes connected to this uninterruptible power supply.

2. If the error is reported again after the nodes are restarted replace the 2145 UPS electronics assembly.

Possible Cause-FRU's or other:
- 2145 UPS electronics assembly (5%)

Other:
- Transient 2145 UPS error (95%)

---

### 3025 A virtualization feature license is required.

**Explanation:** The cluster has no virtualization feature license registered. You should have either an Entry Edition Physical Disk virtualization feature license or a Capacity virtualization feature license that covers the cluster.

The cluster will continue to operate, but it might be violating the license conditions.

**User response:**
- If you do not have a virtualization feature license that is valid and sufficient for this cluster, contact your IBM sales representative, arrange a license and change the license settings for the cluster to register the license.
- The error will automatically fix when the situation is resolved.

Possible Cause-FRU's or other:
- None

---

### 3029 Virtualization feature capacity is not valid.

**Explanation:** The setting for the amount of space that can be virtualized is not valid. The value must be an integer number of terabytes.

This error event is created when a cluster is upgraded from a version prior to 4.3.0 to version 4.3.0 or later. Prior to version 4.3.0 the virtualization feature capacity value was in gigabytes and therefore could be set to a fraction of a terabyte. With version 4.3.0 and later the licensed capacity for the virtualization feature must be an integer number of terabytes.

**User response:**
- Review the license conditions for the virtualization feature. If you have one cluster, change the license settings for the cluster to match the capacity that is licensed. If your license covers more than one cluster, apportion an integer number of terabytes to each cluster. You might have to change the virtualization capacity that is set on the other clusters to ensure that the sum of the capacities for all of the clusters does not exceed the licensed capacity.
- You can view the event data or the feature log to ensure that the licensed capacity is sufficient for the space that is actually being used. Contact your IBM sales representative if you want to change the capacity of the license.
- This error will automatically be fixed when a valid configuration is entered.

Possible Cause-FRU's or other:
- None

---

### 3030 Global and Metro Mirror feature capacity not set.

**Explanation:** The Global and Metro Mirror feature is set to On for the cluster, but the capacity has not been set.

This error event is created when a cluster is upgraded from a version prior to 4.3.0 to version 4.3.0 or later. Prior to version 4.3.0 and later the Global and Metro Mirror feature capacity must also be set.

**User response:** Perform one of the following actions:
- Change the Global and Metro Mirror license settings for the cluster either to the licensed Global and Metro Mirror capacity, or if the license applies to more than one cluster, to the portion of the license allocated to this cluster. Set the licensed Global and Metro Mirror capacity to zero if it is no longer being used.
- View the event data or the feature log to ensure that the licensed Global and Metro Mirror capacity is sufficient for the space actually being used. Contact your IBM sales representative if you want to change the licensed Global and Metro Mirror capacity.
- The error will automatically be fixed when a valid configuration is entered.

Possible Cause-FRU's or other:
- None

---

### 3031 FlashCopy feature capacity not set.

**Explanation:** The FlashCopy feature is set to On for the cluster, but the capacity has not been set.

This error event is created when a cluster is upgraded from a version prior to 4.3.0 to version 4.3.0 or later. Prior to version 4.3.0 the feature can only be set to On or Off; with version 4.3.0 and later the licensed capacity for the feature must also be set.

**User response:** Perform one of the following actions:
- Change the FlashCopy license settings for the cluster either to the licensed FlashCopy capacity, or if the license applies to more than one cluster, to the
portion of the license allocated to this cluster. Set the licensed FlashCopy capacity to zero if it is no longer being used.
• View the event data or the feature log to ensure that the licensed FlashCopy capacity is sufficient for the space actually being used. Contact your IBM sales representative if you want to change the licensed FlashCopy capacity.
• The error will automatically be fixed when a valid configuration is entered.

Possible Cause-FRUs or other:
• None

3032 Feature license limit exceeded.

Explanation: The amount of space that is licensed for a cluster feature is being exceeded.
The feature that is being exceeded might be:
• Virtualization feature - event identifier 009172
• FlashCopy feature - event identifier 009173
• Global and Metro Mirror feature - event identifier 009174

The cluster will continue to operate, but it might be violating the license conditions.

User response:
• Determine which feature license limit has been exceeded. This might be:
  • Virtualization feature - event identifier 009172
  • FlashCopy feature - event identifier 009173
  • Global and Metro Mirror feature - event identifier 009174
• Ensure that the feature capacity that is reported by the cluster has been set to match either the licensed size, or if the license applies to more than one cluster, to the portion of the license that is allocated to this cluster.
• Decide whether to increase the feature capacity or to reduce the space that is being used by this feature.
• To increase the feature capacity, contact your IBM sales representative and arrange an increased license capacity. Change the license settings for the cluster to set the new licensed capacity. Alternatively, if the license applies to more than one cluster modify how the licensed capacity is apportioned between the clusters. Update every cluster so that the sum of the license capacity for all of the clusters does not exceed the licensed capacity for the location.
• To reduce the amount of disk space that is virtualized, delete some of the managed disks or image mode volumes. The used virtualization size is the sum of the capacities of all of the managed disks and image mode disks.

• To reduce the FlashCopy capacity delete some FlashCopy mappings. The used FlashCopy size is the sum of all of the volumes that are the source volume of a FlashCopy mapping.
• To reduce Global and Metro Mirror capacity delete some Global Mirror or Metro Mirror relationships. The used Global and Metro Mirror size is the sum of the capacities of all of the volumes that are in a Metro Mirror or Global Mirror relationship; both master and auxiliary volumes are counted.
• The error will automatically be fixed when the licensed capacity is greater than the capacity that is being used.

Possible Cause-FRUs or other:
• None

3035 Physical Disk FlashCopy feature license required

Explanation: The Entry Edition cluster has some FlashCopy mappings defined. There is, however, no Physical Disk FlashCopy license registered on the cluster. The cluster will continue to operate, but it might be violating the license conditions.

User response:
• Check whether you have an Entry Edition Physical Disk FlashCopy license for this cluster that you have not registered on the cluster. Update the cluster license configuration if you have a license.
• Decide whether you want to continue to use the FlashCopy feature or not.
• If you want to use the FlashCopy feature contact your IBM sales representative, arrange a license and change the license settings for the cluster to register the license.
• If you do not want to use the FlashCopy feature, you must delete all of the FlashCopy mappings.
• The error will automatically fix when the situation is resolved.

Possible Cause-FRUs or other:
• None

3036 Physical Disk Global and Metro Mirror feature license required

Explanation: The Entry Edition cluster has some Global Mirror or Metro Mirror relationships defined. There is, however, no Physical Disk Global and Metro Mirror license registered on the cluster. The cluster will continue to operate, but it might be violating the license conditions.

User response:
• Check if you have an Entry Edition Physical Disk Global and Metro Mirror license for this cluster that
you have not registered on the cluster. Update the cluster license configuration if you have a license.
- Decide whether you want to continue to use the Global Mirror or Metro Mirror features or not.
- If you want to use either the Global Mirror or Metro Mirror feature contact your IBM sales representative, arrange a license and change the license settings for the cluster to register the license.
- If you do not want to use both the Global Mirror and Metro Mirror features, you must delete all of the Global Mirror and Metro Mirror relationships.
- The error will automatically fix when the situation is resolved.

Possible Cause-FRUs or other:
- None

3080  Global or Metro Mirror relationship or consistency group with deleted partnership

Explanation: A Global Mirror or Metro Mirror relationship or consistency group exists with a cluster whose partnership is deleted.

Beginning with SAN Volume Controller version 4.3.1 this configuration is not supported and should be resolved. This condition can occur as a result of an upgrade to SAN Volume Controller version 4.3.1 or later.

User response: The issue can be resolved either by deleting all of the Global Mirror or Metro Mirror relationships or consistency groups that exist with a cluster whose partnership is deleted, or by recreating all of the partnerships that they were using.

The error will automatically fix when the situation is resolved.
- List all of the Global Mirror and Metro Mirror relationships and note those where the master cluster name or the auxiliary cluster name is blank. For each of these relationships, also note the cluster ID of the remote cluster.
- List all of the Global Mirror and Metro Mirror consistency groups and note those where the master cluster name or the auxiliary cluster name is blank. For each of these consistency groups, also note the cluster ID of the remote cluster.
- Determine how many unique remote cluster IDs there are among all of the Global Mirror and Metro Mirror relationships and consistency groups that you have identified in the first two steps. For each of these remote clusters, decide if you want to re-establish the partnership with that cluster. Ensure that the total number of partnerships that you want to have with remote clusters does not exceed the cluster limit. In version 4.3.1 this limit is 1. If you re-establish a partnership, you will not have to delete the Global Mirror and Metro Mirror relationships and consistency groups that use the partnership.
- Re-establish any selected partnerships.
- Delete all of the Global Mirror and Metro Mirror relationships and consistency groups that you listed in either of the first two steps whose remote cluster partnership has not been re-established.
- Check that the error has been marked as fixed by the system. If it has not, return to the first step and determine which Global Mirror or Metro Mirror relationships or consistency groups are still causing the issue.

Possible Cause-FRUs or other:
- None

3081  Unable to send email to any of the configured email servers.

Explanation: Either the system was not able to connect to any of the SMTP email servers, or the email transmission has failed. A maximum of six email servers can be configured. Error event 2600 or 2601 is raised when an individual email server is found to be not working. This error indicates that all of the email servers were found to be not working.

User response:
- Check the event log for all unresolved 2600 and 2601 errors and fix those problems.
- If this error has not already been automatically marked fixed, mark this error as fixed.
- Perform the check email function to test that an email server is operating properly.

Possible Cause-FRUs or other:
- None
Appendix. Accessibility features for IBM Storwize V7000

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

These are the major accessibility features in Storwize V7000:
- 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 9.0.
- This product uses standard Windows navigation keys.
- Interfaces are commonly used by screen readers.
- Keys are discernible by touch, but do not activate just by touching them.
- Industry-standard devices, ports, and connectors.
- You can attach alternative input and output devices.

The Storwize V7000 Information Center and its related publications are accessibility-enabled. The accessibility features of the Information Center are described in Viewing information in the information center in the Information Center.

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 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
Blg 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.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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, 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, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

**Electronic emission notices**

This section contains the electronic emission notices or statements for the United States and other countries.

**Federal Communications Commission (FCC) statement**

This explains the Federal Communications Commission's (FCC's) 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 Canadian ICES-003.

Cet appareil numérique de la classe A est conform 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:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2941
Email: lugi@de.ibm.com

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, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Statement
Taiwan Class A compliance statement

警告使用者:
這是一種類的資訊產品，在居住環境中使用時，可能會造成射頻干擾，使用者會被要求採取某些適當的對策。

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

Japan VCCI Council Class A statement

This explains the Japan Voluntary Control Council for Interference (VCCI) 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。VCCI-A

Japan Electronics and Information Technology Industries Association Statement

This explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for less than or equal to 20 A per phase.
This explains the JEITA statement for greater than 20 A per phase.

Korean Communications Commission Class A Statement
This explains the Korean Communications Commission (KCC) statement.

Russia Electromagnetic Interference Class A Statement
This statement explains the Russia Electromagnetic Interference (EMI) statement.