

IBM Storwize V7000 Unified
Version 1.3.0
Machine Type 2073

Problem Determination Guide



Note

Before using this information and the product it supports, read the general information in “Notices” on page 269, the information in the “Safety and environmental notices” on page xi, as well as the information in the *IBM Environmental Notices and User Guide* , which is provided on a DVD.

This edition applies to the IBM Storwize V7000 Unified, Version 1.3.0, and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces GA32-1057-00.

© **Copyright IBM Corporation 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

Safety and environmental notices xi

Safety xi
Safety statements xiii
Sound pressure xvii

About this guide xix

Who should use this guide xix
Emphasis xix
Storwize V7000 Unified library and related publications xix
How to order IBM publications xxii
Sending your comments. xxii

Chapter 1. Storwize V7000 Unified hardware components 1

Chapter 2. Best practices for troubleshooting 3

Record access information 3
Follow power management procedures 4
Set up event notifications 4
Back up your data 5
Manage your spare and failed drives 5
Resolve alerts in a timely manner 5
Keep your software up to date 6
Keep your records up to date. 6
Subscribe to support notifications 6
Know your IBM warranty and maintenance agreement details. 7

Chapter 3. Getting started troubleshooting 9

Installation troubleshooting 10
 Problems with initial configuration 10
 Installation error codes 12
 Problems reported by the CLI commands during software configuration. 18
GUI access issues 19
Health status and recovery 21
Connectivity issues 22
 Host to file modules connectivity 22
 File module to file module 23
 File module to control enclosure 24
 Fibre connectivity between file modules and control enclosure 26
Understanding LED hardware indicators 29
 File node hardware indicators 29
 Enclosure hardware indicators 37
Management GUI interface 42

When to use the management GUI 43
Accessing the Storwize V7000 Unified management GUI 43
Using fix procedures 44

Chapter 4. File module 47

General file module procedures. 47
 Rebooting a file module 47
 Removing a file module to perform a maintenance action 47
 Removing and replacing file module components 49
 Hard disk drive problems 52
 Monitoring memory usage on a file module 72
Errors and messages 72
 Understanding error codes 72
 Understanding event IDs 76
File module hardware problems 77
 Removing and replacing parts 77
File module software problems 152
 Logical devices and physical port locations 152
 Management node role failover procedures 152
Checking CTDB health 155
Checking the GPFS file system mount on each file module 157
 Identifying created and mounted file system mounts 157
 Resolving problems with missing mounted file systems 158
 Resolving stale NFS file systems 159
Checking user and server authentication issues 159
 Error for “Missing SRV record in DNS” 159
 If “netgroup” functionality with NIS is not working 160
 Possible client misconfiguration 160
Checking client access 161
Checking network interface availability. 161
Recovering a GPFS file system 162
Resolving an ANS1267E error 163
Resolving issues reported for **lshhealth** 163
 Error for “MGMTNODE_REPL_STATE ERROR DATABASE_REPLICATION_FAILED” 163
Resolving full condition for GPFS file system. 164
Analyzing GPFS logs 164
Synchronizing time on the file modules 165

Chapter 5. Control enclosure. 167

Storwize V7000 system interfaces. 167
 Service assistant interface 167
 Storage system command-line interface. 169
 Service command-line interface 169
 USB key and Initialization tool interface 170
Event reporting. 175
 Understanding events 176
 Event notifications. 177
 Power-on self-test 178

Understanding events	178
Understanding the error codes	178
Viewing logs and traces	179
Understanding the battery operation for the control enclosure	179
Maintenance discharge cycles	180
Understanding the medium errors and bad blocks	181
Resolving a problem	183
Start here: Use the management GUI recommended actions	183
Problem: Storage system management IP address unknown	184
Problem: Unable to connect to the management GUI	184
Problem: Unable to log on to the storage system management GUI	185
Problem: Cannot create a clustered storage system	185
Problem: Unknown service address of a node canister	186
Problem: Cannot connect to the service assistant	187
Problem: Management GUI or service assistant does not display correctly	188
Problem: Node canister location error	188
Problem: SAS cabling not valid	188
Problem: New expansion enclosure not detected	189
Problem: Mirrored volume copies no longer identical	189
Problem: Code not processed from USB key	190
Procedure: Resetting superuser password	190
Procedure: Identifying which enclosure or canister to service	190
Procedure: Checking the status of your system	191
Procedure: Getting node canister and system information using the service assistant	192
Procedure: Getting node canister and system information using a USB key	192
Procedure: Understanding the system status using the LEDs.	193
Procedure: Finding the status of the Ethernet connections	198
Procedure: Removing system data from a node canister	198
Procedure: Deleting a system completely	199
Procedure: Fixing node errors	199
Procedure: Changing the service IP address of a node canister	200
Procedure: Accessing a canister using a directly attached Ethernet cable	201
Procedure: Reseating a node canister	201
Procedure: Powering off your system	202
Procedure: Collecting information for support	203
Procedure: Rescuing node canister software from another node (node rescue)	203
Removing and replacing parts	204
Preparing to remove and replace parts	204
Replacing a node canister	204
Replacing an expansion canister	206
Replacing an SFP transceiver	208
Replacing a power supply unit for a control enclosure	209

Replacing a power supply unit for an expansion enclosure	213
Replacing a battery in a power supply unit	217
Releasing the cable retention bracket	221
Replacing a 3.5" drive assembly or blank carrier	221
Replacing a 2.5" drive assembly or blank carrier	223
Replacing an enclosure end cap	224
Replacing a SAS cable	224
Replacing a control enclosure chassis	225
Replacing an expansion enclosure chassis	230
Replacing the support rails	233
General storage system procedures	234
SAN problem determination	234
Fibre Channel link failures	235
Ethernet iSCSI host-link problems	235
Recover system procedure	236
When to run the recover system procedure	236
Fix hardware errors	238
Removing system information for node canisters with error code 550 or error code 578 using the service assistant	239
Performing system recovery using the service assistant	239
Recovering from offline VDisks using the CLI	241
What to check after running the system recovery	241
Backing up and restoring the system configuration	242
Backing up the system configuration using the CLI.	243
Deleting backup configuration files using the CLI.	245

Chapter 6. Call home and remote support 247

Configuring the remote support system	247
Establishing an AOS connection	247

Chapter 7. Recovery procedures . . . 251

User ID and system access	251
Accessing a file module as root	251
Recovering from losing the root password.	251
Resetting the NAS ssh key for configuration communications	252
Working with NFS clients that fail to mount NFS shares after a client IP change	253
Working with file modules that report a stale NFS file handle.	254
File module-related issues	254
Restoring System x firmware (BIOS) settings	254
Recovering from a multipath event	255
Recovering from an NFSD service error	256
Recovering from an SCM error	256
Recovering from an httpd service error.	257
Recovering from an sshd_data service error	257
Recovering from an sshd_int service error.	257
Recovering from an sshd_mgmt service error	257
Recovering from an sshd_service service error	258
Control enclosure-related issues	258
Recovering when file volumes come back online	258

Recovering when a file volume does not come back online	258
Recovering from a 1001 error code	258
Restoring data	259
Restoring asynchronous data	260
Restoring Tivoli Storage Manager data	260
Upgrade recovery	261

Appendix. Accessibility 267

Notices 269

Trademarks	271
Electronic emission notices	271
Federal Communications Commission (FCC) statement.	271
Industry Canada compliance statement.	272
Avis de conformité à la réglementation d'Industrie Canada	272
Australia and New Zealand Class A Statement	272

European Union Electromagnetic Compatibility Directive	272
Germany Electromagnetic compatibility directive	273
Japan VCCI Council Class A statement	274
People's Republic of China Class A Electronic Emission Statement	274
International Electrotechnical Commission (IEC) statement.	274
Korean Communications Commission (KCC) Class A Statement	274
Russia Electromagnetic Interference (EMI) Class A Statement	274
Taiwan Class A compliance statement	275
European Contact Information.	275
Taiwan Contact Information	275

Index 277

Figures

1. File module Ethernet network connections	23	32. ServeRAID M5000 advanced feature key and M5014 adapter	120
2. File module node Ethernet network connections. This is a logical diagram of the connectivity and does not reflect the exact physical system.	24	33. Releasing the battery retention clip	121
3. Control enclosure Ethernet network connections. This diagram is conceptual, not a physical representation.	25	34. Disconnecting the remote battery cable	121
4. Fibre connections between the file modules and disk system. This is a logical diagram of the connectivity and does not reflect the exact physical system.	26	35. Removing the battery from the battery carrier	122
5. LEDs on the power supply units of the control enclosure	38	36. Connecting the remote battery cable	123
6. LEDs on the node canisters	40	37. Locating the posts on the battery and battery carrier	123
7. Selecting a file module to display node status	54	38. DIMM locations for the Storwize V7000 Unified System x3650 M2 server	127
8. Displaying node status.	55	39. DIMM locations for the Storwize V7000 Unified System x3650 M3 server	128
9. Example that shows that mirroring is re-synchronizing	57	40. Heat-sink release lever	137
10. Example that shows that a drive is not synchronized	58	41. Microprocessor release latch	138
11. Example that shows that the mirror is not created	59	42. Aligning the microprocessor	140
12. Example of a SMART error	60	43. Bottom surface of the heat sink	142
13. Removing the Ethernet adapter	103	44. Aligning the heat sink above the microprocessor	142
14. Location of the rubber stopper on the chassis	104	45. 240 VA safety cover	150
15. Location of the Ethernet adapter filler panel on the chassis	104	46. 240 VA safety cover	151
16. Location of the port openings on the chassis	105	47. Management GUI showing CTDB status for both file modules	156
17. Aligning the Ethernet adapter port connectors with the port openings	105	48. LEDs on the power supply units of the control enclosure	194
18. Side view of adapter in the server	106	49. LEDs on the node canisters	196
19. Port connector alignment	106	50. LEDs on the node canisters	203
20. 16-drive-capable server model	108	51. Rear of node canisters that shows the handles.	205
21. Tape-enabled server model	108	52. Removing the canister from the enclosure	206
22. SAS riser-card and controller assembly on the 16-drive-capable server model.	109	53. Rear of expansion canisters that shows the handles.	207
23. Controller retention brackets on 16-drive-capable server model	110	54. Removing the canister from the enclosure	208
24. SAS controller front retention brackets	110	55. SFP transceiver	209
25. Removing the rear controller retention bracket	111	56. Directions for lifting the handle on the power supply unit	212
26. Installing the controller retention bracket	111	57. Using the handle to remove a power supply unit.	212
27. Sliding the controller retention bracket inward and pressing the release tab.	112	58. Directions for lifting the handle on the power supply unit	216
28. SAS riser-card assembly on tape-enabled server model.	112	59. Using the handle to remove a power supply unit.	216
29. ServeRAID M1000 advanced feature key and M1015 adapter	117	60. Removing the battery from the control enclosure power-supply unit	220
30. ServeRAID M5000 advanced feature key and M5014 adapter	118	61. Unlocking the 3.5" drive	222
31. ServeRAID M1000 advanced feature key and M1015 adapter	119	62. Removing the 3.5" drive	222
		63. Unlocking the 2.5" drive	223
		64. Removing the 2.5" drive	224
		65. SAS cable	225
		66. Removing a rail assembly from a rack cabinet	233

Tables

1. Storwize V7000 Unified library	xx	25. Ethernet role and port reference.	73
2. Other IBM publications	xxi	26. Ethernet switch error code categories	73
3. IBM documentation and related websites	xxii	27. Originating file module and file module specific hardware code – Code 0, 2, 4	73
4. Access information for your system	3	28. Originating file module specific software code – Code 1, 3, 5	74
5. Installation error code actions	12	29. Storage enclosure hardware code – Code 6	74
6. Error messages and actions	13	30. Error code break down.	75
7. CLI command problems	19	31. Error code break down.	76
8. Ethernet connections available with the file modules	23	32. Components identified as customer replaceable units (CRUs) and field replaceable units (FRUs)	77
9. Ethernet ports and type of connections.	24	33. System board fan locations	131
10. Error code port location mapping	27	34. System status with 460-watt power supplies installed	133
11. HBA cabling from the file module to Storwize V7000 system	28	35. Storwize V7000 Unified logical devices and physical port locations	152
12. LED states and associated actions. For the HBA adapters on the file module check the amber LED lights next to the port.	28	36. Hostname and service IP reference	153
13. Fibre connection on the Storwize V7000 node canister LED state and associated actions	28	37. Description of data fields for the event log	176
14. LED indicators, corresponding problem causes, and corrective actions	32	38. Notification types	177
15. Power-supply LEDs.	36	39. Bad block errors	182
16. Power-supply unit LEDs	38	40. Power-supply unit LEDs.	194
17. Power LEDs	40	41. Power LEDs	195
18. System status and fault LEDs	40	42. System status and fault LEDs	196
19. Control enclosure battery LEDs	41	43. Control enclosure battery LEDs	197
20. Status of volume.	55	44. Upgrade error codes from using the applysoftware command and recommended actions	261
21. State of drives.	56	45. Upgrade error codes and recommended actions	263
22. SMART ASC/ASCQ error codes and messages	61		
23. Error code information.	72		
24. Originating role information	72		

Safety and environmental notices

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

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

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

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

CAUTION:

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

DANGER

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

2. Locate *IBM Systems Safety Notices* with the user publications that were provided with the Storwize V7000 Unified hardware.
3. Find the matching identification number in the *IBM Systems 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 Unified website. Go to the Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified and click the documentation link.

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 **Safety Information** (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Safety statements

Each caution and danger statement in this document is labeled with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the *Safety Information* document. For example, if a caution statement is labeled “Statement 1”, translations for that caution statement are in the *Safety Information* document under “Statement 1.”

Important:

Be sure to read all caution and danger statements in this document before you perform the procedures. Read any additional safety information that comes with the system or optional device before you install the device.

Statement 1



DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet.
- Connect to properly wired outlets any equipment that will be attached to this product.
- 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 table when installing, moving, or opening covers on this product or attached devices.

To Connect:

1. Turn everything OFF.
2. First, attach all cables to devices.
3. Attach signal cables to connectors.
4. Attach power cords to outlet.
5. Turn device ON.

To Disconnect:

1. Turn everything OFF.
2. First, remove power cords from outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

Statement 2



CAUTION:

When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- Throw or immerse into water
- Heat to more than 100°C (212°F)
- Repair or disassemble

Dispose of the battery as required by local ordinances or regulations.

Statement 3



CAUTION:

When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.



DANGER

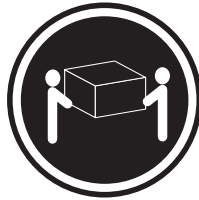
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.



Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaite
Appareil À Laser de Classe 1

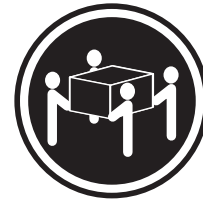
Statement 4



≥ 18 kg (39.7 lb)



≥ 32 kg (70.5 lb)



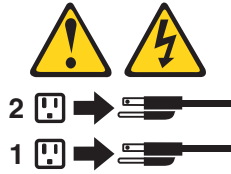
≥ 55 kg (121.2 lb)

CAUTION:
Use safe practices when lifting.

Statement 5



CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 8



CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 26



CAUTION:

Do not place any object on top of rack-mounted devices.



This node is suitable for use on an IT power-distribution system whose maximum phase-to-phase voltage is 240 V under any distribution fault condition.

Important: This product is not suitable for use with visual display workplace devices according to Clause 2 of the German Ordinance for Work with Visual Display Units.

Sound pressure

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

About this guide

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

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

The troubleshooting procedures can help you analyze failures that occur in a Storwize V7000 Unified 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 Unified.

Emphasis

Different typefaces are used in this guide to show emphasis.

The following typefaces are used to show emphasis:

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

Storwize V7000 Unified library and related publications

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

Storwize V7000 Unified Information Center

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

Storwize V7000 Unified library

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

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

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

Table 1. Storwize V7000 Unified library

Title	Description	Order number
<i>Storwize V7000 Unified Quick Installation Guide</i>	This guide provides instructions for unpacking your shipping order and installing your system. The first of three chapters describes verifying your order, becoming familiar with the hardware components, and meeting environmental requirements. The second chapter describes installing the hardware and attaching data cables and power cords. The last chapter describes accessing the management GUI to initially configure your system.	GA32-1056
<i>Storwize V7000 Unified Problem Determination Guide</i>	This guide describes how to service, maintain, and troubleshoot the Storwize V7000 Unified system.	GA32-1057
<i>IBM Systems Safety Notices</i>	This guide contains translated caution and danger statements for the node canister documentation. Each caution and danger statement in the Storwize V7000 Unified documentation has a number that you can use to locate the corresponding statement in your language in the <i>IBM Systems Safety Notices</i> document.	G2229-9054

Table 1. Storwize V7000 Unified library (continued)

Title	Description	Order number
<i>Safety Information</i>	This guide contains translated caution and danger statements for the file module documentation. Each caution and danger statement in the Storwize V7000 Unified documentation has a number that you can use to locate the corresponding statement in your language in the <i>Safety Information</i> document.	P/N 59Y7218
<i>Storwize V7000 Unified Read First Flyer</i>	This document introduces the major components of the Storwize V7000 Unified system and describes how to get started with the <i>Storwize V7000 Unified Quick Installation Guide</i> .	GA32-1055
<i>IBM Statement of Limited Warranty (2145 and 2076)</i>	This multilingual document provides information about the IBM warranty for machine types 2145 and 2076.	Part number: 85Y5978
<i>IBM Statement of Limited Warranty (2073)</i>	This multilingual document provides information about the IBM warranty for machine type 2073.	Part number: 00L4547
<i>IBM License Agreement for Machine Code</i>	This multilingual guide contains the License Agreement for Machine Code for the Storwize V7000 Unified product.	Z125-5468

Other IBM publications

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

Table 2. Other IBM publications

Title	Description	Order number
<i>IBM Storage Management Pack for Microsoft System Center Operations Manager User Guide</i>	This guide describes how to install, configure, and use the IBM Storage Management Pack for Microsoft System Center Operations Manager (SCOM).	GC27-3909 publibfp.dhe.ibm.com/epubs/pdf/c2739092.pdf
<i>IBM Storage Management Console for VMware vCenter, version 2.6.0, Installation Guide</i>	This publication provides installation, configuration, and usage instructions for the IBM Storage Management Console for VMware vCenter.	GA32-0929 publibfp.dhe.ibm.com/epubs/pdf/a3209295.pdf

IBM documentation and related websites

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

Table 3. IBM documentation and related websites

Website	Address
Support for Storwize V7000 Unified (2073)	Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified
Support for IBM System Storage® and IBM TotalStorage products	www.ibm.com/storage/support/
IBM Publications Center	www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss
IBM Redbooks® publications	www.redbooks.ibm.com/

Related accessibility information

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

www.adobe.com/support/downloads/main.html

How to order IBM publications

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

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

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

Sending your comments

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

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

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

- Publication form number: GA32-1057-00
- Page, table, or illustration numbers that you are commenting on
- A detailed description of any information that should be changed

Chapter 1. Storwize V7000 Unified hardware components

A Storwize V7000 Unified system consists of one or more machine type 2076 rack-mounted enclosures and two machine type 2073 rack-mounted file modules.

There are several model types for the 2076 machine type. 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 for the file module is 2073-700.

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.
- The number of LEDs on the power supplies. Control enclosure power supplies have six; expansion enclosure power supplies have four.

Chapter 2. Best practices for troubleshooting

Troubleshooting is made easier by taking advantage of certain configuration options and ensuring that you have recorded vital information that is required to access your system.

Record access information

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

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

- The management IP addresses. This address connects to the system using the management GUI or starts a session that runs the command-line interface (CLI) commands. Record this address and any limitations regarding where it can be accessed from within your Ethernet network.
- The service IP addresses for the file module are used to access the root console on each of the file modules when needed to perform some investigation and recovery procedures.
- The root password for the file modules. The root password might be needed to perform some recovery procedures. For security reasons, the root password must be changed from its default value of `Passw0rd` using the `chrootpwd` CLI command. If you lose the root password, see “Recovering from losing the root password” on page 251.
- The control enclosure management IP address. This address is normally not needed. You might need it to access the control enclosure management GUI or the CLI during some recovery procedures. Use this address if the file modules lose their connection to the control enclosure CLI.
- 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 Unified system, but you can set these IP addresses later by using the `chserviceip` CLI command.

Table 4. Access information for your system

Item	Value	Notes
The management IP address for the GUI and CLI		
The management user ID (the default is admin)		
The management user ID password (the default is admin)		
The network gateway IP address		
File module 1 service IP address		

Table 4. Access information for your system (continued)

Item	Value	Notes
File module 2 service IP address		
The root password for the file modules (the default is Passw0rd)		
The control enclosure management IP address		
The control enclosure superuser password (the default is passw0rd)		
Control enclosure canister 1 service IP address		
Control enclosure canister 2 service IP address		

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 system fails properly in the case of powering down individual file modules and that data that is cached in the node canister memory is correctly flushed to the RAID arrays for the disk system.

The Storwize V7000 Unified system uses a pair of file modules for redundancy. Follow the appropriate power down procedures to minimize impacts to the system operations. See “Turning off the system” in the Storwize V7000 Unified information center.

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 that use the management GUI, configure your system to send notifications when a new event is reported. Select the type of event that you want to be notified about. For example, restrict notifications to just events that require immediate action. Several event notification mechanisms exist:

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

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

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

Back up your data

Back up your system configuration data, volume data, and file systems.

The file modules back up their configuration after each configuration change. Download the backup files regularly to your management workstation to protect the 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 or files in the file systems are susceptible to failures in your host application or your Storwize V7000 Unified 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 or the files 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 management GUI provides the capability to review these issues from the Events panel.

For file module issues, use the Storwize V7000 Unified information center to look up the events and perform the actions listed for the events.

For Storwize V7000 issues, resolve these problems through the **Recommended actions only** option from the Events panel.

Perform the recommended actions as quickly as possible after the problem is reported. Your system is designed to be resilient to most single hardware failures. However, if you operate for any period of time with a hardware failure, the possibility increases that a second hardware failure can result in some volume data that is unavailable.

If there are a number of unfixed alerts, fixing any one alert might become more difficult because of the effects of the other alerts.

Keep your software up to date

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

Check the IBM support website to see if new code releases are available:

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

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 and file modules.

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 file modules, control enclosure, and 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:

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

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 and the serial number of the enclosure or file module that has the problem. The machine type is always 2076 for a control enclosure or 2073 for a file module. 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. Getting started troubleshooting

This topic is an entry point to troubleshooting your system. The content provides help in correctly identifying which of the recovery procedures must be run to recover a Storwize V7000 Unified system from a problem.

Important: After you successfully fix a problem by using the instructions that follow, use the “Health status and recovery” on page 21 procedure to set the health status back to green.

If you are here because you installed a new system and cannot initialize it by using the USB key, go to “Installation troubleshooting” on page 10.

If one of the file modules does not boot up and join the GPFS™ cluster, look for a hardware problem by using the light-path diagnostics LEDs. See “File node hardware indicators” on page 29. If you suspect that the boot software is corrupted, call IBM support.

If any orange fault LEDs are illuminated on the control enclosure, front or rear, see “Resolving a problem” on page 183.

If you are having problems accessing the management GUI or the CLI, see “GUI access issues” on page 19. For information about accessing the management GUI, see “Accessing the Storwize V7000 Unified management GUI” on page 43.

If the health status indicator in the lower right corner of management GUI is not green, hover over the icon on the left side of the indicator to see the type of error that is causing the poor health status. Select an error type, and you are shown the critical errors in the event log. First try to fix the critical errors under the **Block** tab of the **Monitoring > Events** page before trying to fix the critical errors under the **File** tab of the **Monitoring > Events** page.

Log into the CLI interface and run the CLI command, **lslog**. Review the results for problems that may need to be resolved.

If users or applications are having trouble accessing data that is held on the Storwize V7000 Unified system, or if the management GUI is not accessible or is running slowly, the Storwize V7000 control enclosure might have a problem.

If you cannot ping the management IP address for the Storwize V7000 control enclosure, try to access the control enclosure service assistant. Use the service IP address of the node canisters in the control enclosure to resolve any reported node errors. See “Procedure: Fixing node errors” on page 199.

Note: Use the access information that you previously recorded for the service IP address of the node canisters in the control enclosure. See “Record access information” on page 3. If you do not know the service IP addresses for the node canisters in the control enclosure, see “Problem: Unknown service address of a node canister” on page 186.

If all nodes show either node error 550 or node error 578, you might need to perform a system recovery. See “Recover system procedure” on page 236 for more details.

For more information about determining and solving block storage problems that relate to the control enclosure, see “Resolving a problem” on page 183.

Check the intrasystem connectivity by using the management GUI. Navigate to **Monitoring > System**. Use the interactive graphic to determine the connection state by hovering over each connection in the graphic.

If either of the Fibre Channel links from the file modules shows an error or degraded state, see “Fibre connectivity between file modules and control enclosure” on page 26.

If mgmt0, the direct Ethernet link between the file modules, shows an error or degraded state, see “File module to file module” on page 23.

If one or both of the Fibre Channel links from the file module to the control enclosure show an error or a degraded state, see “File module to control enclosure” on page 24.

Check the core component health. Navigate to **Monitoring > System Details > Interface Nodes > nodename > NAS Services**. In the Status panel, check the CTDB state and the GPFS state.

If the GPFS state is Active, but the CTDB state is not Active, see “Checking CTDB health” on page 155; otherwise, see “Checking the GPFS file system mount on each file module” on page 157.

If you have lost access to the files, but there is no sign that anything is wrong with the Storwize V7000 Unified system, see “Host to file modules connectivity” on page 22.

Installation troubleshooting

This topic provides information for troubleshooting problems encountered during the installation.

Software issues are often reported through CLI commands at system configuration and through error codes. Power problems can often be solved through identifying visual symptoms.

Problems with initial configuration

This topic helps you to solve configuration problems.

If USB key is missing or faulty:

- Contact the IBM Support Center.
- Install the latest InitTool.exe (or reinstall if tool is not launching). Go to <http://www-933.ibm.com/support/fixcentral/options> and select the following options to locate the tool. The options are listed under the **Select product** tab, at the bottom of the page:
 - Product Group: **Storage Systems**
 - Product Family: **Disk Systems**
 - Product: **IBM Storwize V7000 Unified**
 - Release: **All**
 - Platform: **All**

Before loading the USB key verify it has a FAT32 formatted file system. Plug the USB key into the laptop. Go to Start (my computer), right-click the USB drive. The general tab next to File system should say FAT32.

- If the USB key is not formatted as FAT32, format it. To format, right-click it, select format, under filesystem. Select FAT32 and then click Start. Continue as prompted.

InitTool.exe is not loaded on the USB key, or fails to launch:

- Install the latest InitTool.exe (or reinstall if tool is not launching). Go to <http://www-933.ibm.com/support/fixcentral/options> and select the following options to locate the tool. The options are listed under the **Select product** tab, at the bottom of the page:
 - Product Group: **Storage Systems**
 - Product Family: **Disk Systems**
 - Product: **IBM Storwize V7000 Unified**
 - Release: **All**
 - Platform: **All**

Amber LED on node canister does not stop flashing during install:

Allow at least 15 minutes for the LED to stop flashing. If flashing continues beyond 15 minutes, remove the USB key and insert in your laptop. Navigate to the `satask_results.html` file and scan for errors and follow the service action recommendation. Take that action and retry installation.

An error is posted in the `satask_results.html`:

Take the recommended action, reboot the node, and restart the procedure.

File module code (CD) not loading:

- Check CD for blemishes and clean the problem CD.
- Reboot the server and try again.
- Try another CD if one is available.

Blue LED on file module, where the USB key was inserted, keeps flashing (does not turn solid as stated in the instructions):

- Allow 5 minutes at least, remove the USB key, insert it into your laptop. Verify that the InitTool set up information is correct, navigate to the `SONAS_results.txt` file, and open it. Check for errors and corrective actions. Refer to *IBM Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide* PDF on the CD.
- If no errors are listed, reboot the server (allow server to start), reinsert the USB key, and try again.

Blue LED on the other file module (without USB key) keeps flashing (does not turn solid or off as listed in instructions):

Wait for the primary file module to start flashing, remove the USB key, insert it into you laptop, verify the InitTool set up information is correct , navigate to the `SONAS_results.txt` file and open it. Check for errors and corrective actions (refer to *IBM Storwize V7000 Troubleshooting, Recovery, and Maintenance Guide* PDF on the CD). If no errors are listed, reboot both file modules, allow file modules to boot completely, reinsert the USB key as originally instructed and try again.

Installation error codes

The system generates an error code that provides a recommended action if the installation fails.

Guide to using the error code table

1. Always check the entire system for any illuminated error lights first and refer to the problem systems appropriate maintenance manual. If no lights are illuminated, continue to step 2.
2. Match the error code noted in the results.txt file to the installation error codes list in Table 6 on page 13. If there are multiple errors, the first error listed is the most critical and should be addressed first.
3. Refer to Table 5 to match the code (A-H) to the recommended action. Follow the suggested action, in order, completing one before trying the next.
4. If the recommended action or actions fail, call the IBM Support Center.

Table actions defined

This table serves as a legend for defining the precise action to follow. The action legend defines the action that is correlated with each action key.

Table 5. Installation error code actions

Action key	Action to be taken
A	Power cycle both file modules with the power button. Wait for the file modules to come up and the flashing blue light on each to come on before proceeding, then reinsert the USB key into the original file module. The installation continues from the last good checkpoint.
B	Power down both file modules, remove power from the power source (unplug it), reapply power, power up, wait for the file modules to come up and the flashing blue light on each to come on before proceeding, then reinsert the USB key into the original file module. The installation continues from the last good checkpoint.
C	Verify that the cabling between file modules is correct and that the connections are seated properly. Then reinsert the USB key into the original file module. The installation will continue from the last good checkpoint.
D	Verify that all IP/gateway/subnet address information is correct (InitTool) and that there are no duplicate IP's on the network. If a change is made, reinsert the USB key. The installation continues from the last good checkpoint.
E	Insert the USB key into the other file module and try again
F	Retrieve the NAS private key from the Storwize V7000 by doing the following: <ul style="list-style-type: none">• Create a text file with the following line: satask chnaskey -privkeyfile NAS.ppk• Save the file as satask.txt on the USB key. Insert the USB key into one of the top control enclosure USB ports and wait at least 20 seconds. Reinsert the USB key into the original management node. The installation continues from the last good checkpoint.
G	Verify that the Ethernet cabling connections are seated properly between the Storwize V7000 Unified control enclosure and the customer network, as well as the file modules cabling to the customer network. Then reinsert the USB key into the original file module. The installation will continue from last good checkpoint.

Table 5. Installation error code actions (continued)

Action key	Action to be taken
H	Use the Storwize V7000 management GUI to check its status. Refer to the <i>IBM Storwize V7000 Unified Information Center</i> for additional information.

Installation error codes

Table 6 lists the error messages and keyed actions. To match the actions, see Table 5 on page 12.

Table 6. Error messages and actions

Error code	Error message	Action key
0A01	Unable to open /tmp/setup_hosts_\$\$.	A
0A02	Unable to create default users.	A
0A05	Unable to determine management IP address.	A
0A06	Unable to determine Management Mask Address.	A
0A07	Error updating /etc/hosts.	A
0A08	Unable to update VPD field.	A
0A0A	Error opening /etc/sysconfig/network.	A
0A0B	Error writing /etc/sysconfig/network.	A
0A0C	Error updating host name.	A
0A0D	Error querying settings through ASU.	B
0A0E	Error setting ASU command.	B
0A0F	Unable to determine adapter name from VPD.	A
0A10	Unable to open the ifcfg file.	A
0A11	Unable to write to the ifcfg file.	A
0A12	Unable to bring adapter down.	A
0A13	Unable to bring adapter up.	D then C then B
0A14	Unable to determine adapter name from VPD.	A
0A15	Unable to open the ifcfg-alias file.	A
0A16	Unable to write to the ifcfg-alias file.	A
0A17	Unable to bring adapter-alias down.	A
0A18	Unable to bring adapter-alias up.	D then C then B
0A19	Unable to retrieve adapter name.	A
0A1A	Incorrect parameters.	D
0A1B	Adapter value not valid.	A
0A1C	Alias value not valid.	A
0A1D	DHCP is not valid on this adapter.	A
0A1E	DHCP is not valid on aliases.	A
0A1F	Invalid IP address.	D
0A20	Invalid netmask.	D
0A21	Invalid Gateway IP Address.	D
0A22	Gateway, netmask, and IP are incompatible.	D

Table 6. Error messages and actions (continued)

Error code	Error message	Action key
0A23	Gateway is not valid on this adapter.	D
0A24	Alias is null.	A
0A25	Could not drop aliases.	A
0A26	Invalid adapter for Storwize V7000.	A
0A27	Invalid alias state argument.	A
0AA5	Invalid inputs.	A
0AA6	Called with invalid host name.	A
0AA7	Error sending password.	A
0AA8	A node name was not provided.	A
0AA9	Invalid management IP address.	A
0AAB	Invalid RSA IP address.	A
0AAC	Invalid IP for management node.	A
0AAD	The node is already a part of a cluster.	A
0AAE	Error while setting storage node peer.	A
0AAF	Unable to get node roles from VPD.	A
0AB0	Error opening /etc/sysconfig/rsyslog.	A
0AB1	Error writing to /etc/sysconfig/rsyslog.	A
0AB2	Error reading /etc/rsyslog.conf.	A
0AB3	Unable to open /opt/IBM/sonas/etc/rsyslog_template_mgmt.conf.	A
0AB4	Unable to open /opt/IBM/sonas/etc/rsyslog_template_int.conf.	A
0AB5	Unable to open /opt/IBM/sonas/etc/rsyslog_template_strg.conf.	A
0AB6	Unknown node roles.	A
0AB7	Error writing /etc/rsyslog.conf.	A
0ABB	Unable to gather shared SSH keys.	A
0ABC	Unable to copy new private keys.	A
0ABD	Unable to copy new public keys.	A
0ABE	Unable to copy shared keys to the remote system.	A
0ABF	Unable to copy user keys on remote system.	A
0AC0	Unable to copy host keys on remote system.	A
0AC1	Unable to open local public RSA key file.	A
0AC2	Unable to parse local host's RSA public key file.	A
0AC3	Unable to open the local host public RSA key file.	A
0AC4	Unable to send local key to the remote system.	A
0AC5	Unable to access remote system after sending local key.	A
0AC6	Unable to gather remote system's public key.	A
0AC7	Unable to gather remote system's host public key.	A
0AC8	Unable to generate public/private keys.	A

Table 6. Error messages and actions (continued)

Error code	Error message	Action key
0AC9	Unable to copy user SSH keys.	A
0ACA	Unable to copy host SSH keys.	A
0ACB	Unable to copy shared keys to remote host.	A
0ACC	Unable to update keys on remote host.	A
0ACD	Unable to read in shared user key.	A
0ACE	Unable to read in shared host key.	A
0ACF	Unable to open authorized keys file for reading.	A
0AD0	Unable to open temp file for writing.	A
0AD1	Error moving temporary file.	A
0AD2	Error opening known hosts file.	A
0AD3	Error opening temporary file.	A
0AD4	No host name provided to exchange keys with.	A
0AD5	Host name is invalid.	A
0AD6	Invalid parameters.	D
0AD7	Unable to open vpdnew.txt file.	A
0AD8	VPD failed to update a value.	A
0AD9	Invalid option.	D
0ADA	Error while parsing adapter ID.	B
0ADB	Unable to open /proc/scsi/scsi.	B
0AF8	Trying to install management stack on non-management node.	A
0AF9	Invalid site ID. Curently only 'st001' is supported on physical systems.	A
0AFA	This node is already a part of a cluster. Unable to configure.	E
0AFB	Unable to generate public/private keys.	A
0AFC	Unable to copy user SSH keys.	A
0AFD	Unable to copy host SSH keys.	A
0AFE	Unable to set the system's timezone.	A
0AFF	Unable to write clock file.	A
0B00	Unable to write to /etc/ntp.conf.	A
0B01	Unable to parse internal IP range.	D
0B08	Unable to open dhcpd.conf template file.	A
0B09	Unable to open dhcpd.conf for writing.	A
0B0A	Unable to copy dhcpd.conf to /etc/.	A
0B0B	Unable to copy tftp to /etc/xinetd.d.	A
0B0E	Unable to enable the TFTP server.	A
0B12	sonas_setup_security is not present.	A
0B13	No service IP provided.	D
0B14	Unable to create RSA1 SSH keys.	A
0B15	Unable to create RSA SSH keys.	A

Table 6. Error messages and actions (continued)

Error code	Error message	Action key
0B16	Unable to create DSA SSH keys.	A
0B17	Exiting on trap.	A
0B18	No controllers found in this cluster.	A
0B2F	Unable to set GPFS setting. Check logs for more details.	A
0B30	Unable to query current GPFS settings from mmlscluster.	A
0B31	There was an error while attempting to enable CTDB.	A
0B32	Unable to query current GPFS settings mmlsconfig.	A
0B33	Unable to open settings file. Check logs for more details.	A
0B34	Invalid arguments passed to the script.	A
0B4F	add_new called with improper parameters.	A
0B50	Invalid serial number.	B
0B51	Invalid forced ID.	A
0B52	Invalid site.	A
0B53	Node with serial was not found in available list.	B
0B54	Storage nodes must be added in pairs. Invalid peer serial.	A
0B55	Storage node peer must be a different serial.	A
0B56	Peer node is not a storage node.	A
0B57	There is already a node with ID.	A
0B58	There is a node at the peer's ID.	A
0B59	No existing cluster found. Node ID must be specified.	A
0B5A	Unable to determine management IP address of this node.	A
0B5B	Unknown node type.	B
0B5C	IP address conflict detected with the management IP. There is a node that already has this IP address.	D
0B5E	IP address conflict detected with its peer management IP. There is a node that already has this IP address.	D
0B5F	Error updating node's data in newnodes.dat.	B
0B60	Error writing temporary file.	A
0B62	Node did not finish configuration before timeout.	B
0B7F	All nodes must be up before adding a new node.	A

Table 6. Error messages and actions (continued)

Error code	Error message	Action key
0B80	Unable to find the peer storage node.	Check Fibre Channel cabling between the file modules and the control enclosure. Verify that the control enclosure is up. Refer to "Powering the system on and off" in the <i>IBM Storwize V7000 Unified Information Center</i> .
0B81	The host name was not set properly.	A
0B82	Unable to create temp file nodes.lst.	A
0B85	Error copying cluster configuration to node.	A
0B86	Error restoring cluster configuration on node.	A
0B87	There was an error while adding nodes to the GPFS cluster.	A
0B88	There was an error while configuring GPFS licensing.	A
0B89	There was an error while configuring GPFS quorum.	A
0B8C	There was an error in updating the configuration on the new node.	A
0B8D	Error reading checkpoint file.	A
0B8E	Error writing to checkpoint file.	A
0B8F	There was an error while installing GPFS callbacks.	A
0B92	Rsync failed between management nodes.	C
0B94	There were too many potential peer storage nodes. Storage controllers may be cabled incorrectly or UUIDs might not be set properly.	A
0B95	Invalid parameters.	D
0B96	Failed to configure the management processes on mgmt001st001	D then A then B
0B97	IP is invalid.	D
0B98	Netmask is invalid.	D
0B99	IP, gateway, and netmask are not a valid combination.	D
0B9A	There was an internal error.	A
0B9B	Invalid NAS private key file.	F
0B9C	Unable to copy the NAS private key file.	F
0B9D	Internal error setting permissions on NAS private key file.	A
0B9E	No NAS private key file found. Verify that the Storwize V7000 configuration ran properly.	F
0B9F	Unable to find local serial number in new nodes.	B
0BA0	Unable to find node at new IP address. Check the node cabling.	C
0BA1	Remote node is at a higher code level.	E

Table 6. Error messages and actions (continued)

Error code	Error message	Action key
0BA2	Management IP for node not found.	D
0BA3	The disk IP was not found in VPD.	D
0BA4	Unable to attach to Storwize V7000 system. Private key files might not match.	F then G
0BA5	Unable to add Storwize V7000 system to CLI.	A
0BA6	Unable to add Storwize V7000 storage system to CLI.	G
0BAC	Cannot find node pair.	C then D then A
0BAD	Remote node is at a higher code level.	E
0BAE	Incorrect parameters.	A
0BAF	Unable retrieve the node serial number.	A
0BB0	Unable to open pxeboot data file.	A
0BB1	Unable to update pxeboot data file for node.	A
0BB2	Unable to set file permissions.	A
0BB3	Unable to find node serial in pxeboot data file.	A
0BB4	Node had an internal error during configuration.	A
01B2	Unable to start performance collection daemon.	Contact your next level of support.
01B3	Failed to copy upgrade package to Storwize V7000 system.	H then G
01B4	Failed to start upgrade on Storwize V7000 with the svctask applysoftware command.	H
01B5	Storwize V7000 multipaths are unhealthy.	H then G
01B6	Storwize V7000 volumes are unhealthy as indicated using the lsvdisk command.	Check Fibre Channel cabling to storage and verify storage is up.
01B7	Failed to query status of upgrade by using the lssoftwareupgradestatus command.	H
01B8	Failed to query status of Storwize V7000 nodes using the lsnodes command.	H
01D5	Storwize V7000 stalled.	Contact your next level of support.
01D6	Storwize V7000 stalled_non_redundant	H

Problems reported by the CLI commands during software configuration

Use this information when troubleshooting problems reported by the CLI commands during software configurations.

The following table contains error messages that might be displayed when running the CLI commands during software configuration.

Table 7. CLI command problems

CLI Command	Symptom/Message	Action
mkfs	SG0002C Command exception found : Disk <arrayname> might still belong to file system <filesystemname>.	<p>This message indicates that the arrays listed in the error message appear to already be part of a file system.</p> <ol style="list-style-type: none"> 1. Check the list of array names that you specified in the mkfs command. If the mkfs command has been used to create multiple file systems, you might have used the same array name in more than one file system. If this is the case, correct the list of array names. 2. If you are certain there is no data on the system, this problem might have been caused by an error during the manufacturing cleanup process before the machine was shipped. In this case, you can work around the problem by appending the --noverify parameter to the mkfs command. Never use the --noverify parameter on a system with customer data unless directed to do so by support personnel; improper use can cause unrecoverable data loss.

GUI access issues

This topic provides assistance in isolating and resolving problems with the GUI.

This section covers GUI access issues that allow you to isolate and resolve GUI problems. This section extends beyond the GUI in the case where a file module is not responding and requires a management switchover to the other file module. Accessing the GUI is critical to isolating and resolving system problems.

1. Does the GUI launch and are there problems logging into the system?

- **Yes:** Check that the user ID being used was set up to access the GUI. Refer to “Authentication basic concepts” in the *IBM Storwize V7000 Unified Information Center*.
- **No:** Proceed to next question.

2. Does the GUI launch and are there problems logging into the system?

- **Yes:** Verify that you are using a supported browser and the browser settings are correct. Refer to “Checking your web browser settings for the management GUI” in the *IBM Storwize V7000 Unified Information Center*.
- **No:** Proceed to next question.

Note: If the GUI does not load complete these steps.

3. Are you able to initiate an ssh connection to either file node and log in to either file node?

- **Yes:**
 - a. Run the CLI command **lsnode** and determine the status of the file nodes.
 - b. If the **lsnode** reports the management service is not running, refer to “Management node role failover procedures” on page 152.
 - c. If **lsnode** provides the system configuration information, check the connection status under the appropriate heading. Is the status set to **OK**:

Note: The Sample Output shown has been adjusted in regards to spacing and layout to accommodate this publication. It might not match exactly what is seen on your system.

```
Sample Output:
[root@kq186wx.mgmt001st001 ~]# lsnode

```

Hostname	IP	Description	Role	Product version	Connection status	GPFS status	CTDB status	Last updated
mgmt001st001	172.31.8.2	active	management, management interface, node	1.3.0.0-51c	OK	active	active	9/19/11 8:02 AM
mgmt002st001	172.31.8.3	passive	management, management interface, node	1.3.0.0-51c	OK	active	active	9/19/11 8:02 AM

```
EFSSG1000I The command completed successfully.
```

- **Yes:** Run the CLI command **lshealth**. Reference the active management node Hostname (mgmt001st001 or mgmt002st002) obtained from the **lsnode** command. Ensure that **HOST_STATE**, **SERVICE**, and **NETWORK** from **lshealth** is set to **OK**.

```
Sample Output:
mgmt001st001 HOST_STATE OK OK
SERVICE OK All services are running OK
CTDB OK CTDBSTATE_STATE_ACTIVE
GPFS OK ACTIVE
SCM OK SCM system running as expected
NETWORK ERROR Network interfaces have a degraded state
CHECKOUT OK Disk Subsystem have a online state
mgmt002st001 HOST_STATE OK OK
SERVICE OK All services are running OK
CTDB OK CTDBSTATE_STATE_ACTIVE
GPFS OK ACTIVE
SCM OK SCM system running as expected
MGMTNODE_REPL_STATE OK OK
NETWORK ERROR Network interfaces have a degraded state
V7000 CLUSTER ERROR Alert found in component cluster
ENCLOSURE ERROR Alert found in component enclosure
IO_GRP OK The component io_grp is running OK
MDISK OK The component mdisk is running OK
NODE OK The component node is running OK
PORT ERROR Alert found in component port
EFSSG1000I The command completed successfully.
```

- **No:** Perform network connectivity isolation procedures. Refer to “Management node role failover procedures” on page 152.

No: Perform network connectivity isolation procedures. Refer to “Management node role failover procedures” on page 152.

If none of the previous steps resolved the GUI connectivity issues, perform the following procedure.

Network port isolation for GUI:

If none of the previous steps have resolved the problem and the network connectivity and system reports nothing wrong, there might be an issue with the port configuration of your network that is not detected in any of the previous steps. The internal management services use both port 443 and port 1081. Port 443 is redirected to port 1081 that the management service listens.

1. Check to see if you can access the GUI on the default https port (no port included in the URL). If all is good with firewall and management IP, the GUI will listen on **https://<Management IP>/** and provide a login prompt.
2. Check network port settings and firewall settings. If the previous step fails, investigate the following issues:
 - The firewall is open between the administrative browser and the Primary Node Service IP but not between the administrative browser and the management IP. The firewall settings must have rules that allow port 1081 but not 443 between the administrative browser and the management IP.
 - The management IP is up but the port redirection on the switch/router is not working as expected. Check the network settings.

Health status and recovery

Use this information to review the outstanding issues that cause the **Health Status** indicator at the bottom of all management GUI panels to be red (critical errors) or yellow (warnings or degradations).

Use this procedure after you resolve the events from the **Monitoring > Events** page to resolve the overall system health status indicators.

Within the Storwize V7000 Unified system, the system **Health Status** is based on a set of pre-defined software and hardware health status sensors that are reflected in the System Details page under the **Status** section for the corresponding logical host name.

For storage problems, resolve events and health status by running the recommended repair action or actions from the **Block** tab of **Monitoring > Events**.

For file module problems, the software and hardware sensors are different. Some of the sensors are automatic and actively reflect the current status of the system; whereas, some of the sensors, such as the hardware sensors, require a reset after the service actions are completed.

This topic instructs you where to go to view the information that is displayed, how to check the status of the various sensors, and how to manually close out sensor events. By performing these tasks, you ensure that the overall **Health Status** reflects the current system health.

Note: For the file modules, the System Details page and sensors are separate from the events. Events that are displayed in the log might be reflected within a corresponding sensor with the **System Details > Status** indicator for the failing host name. However, be aware that resolving events and resetting the corresponding sensor changes the health status of the system but does not clear the corresponding event from the event log.

To resolve the overall health status indicators, perform the following steps:

1. Log on to the management GUI.
2. Navigate to **Monitoring > System Details**.

3. From the System Details page, use the navigation tree on the left to display the hardware components of the system.

The navigation reflects the overall hardware layout of the system. The structure begins with the overall cluster host name. Under the cluster host name are the subcomponent areas of the system in which the interface nodes reflect the file module components, and the enclosure number represents the storage system.

- a. Expand the interface nodes to display the two individual file modules that are represented by the host names `mgmt001st001` and `mgmt002st001`. Expand each of these file modules to display further details.

For any critical or warning level events, the corresponding hardware reflects the status with a small red circle or yellow triangle next to the corresponding device.

- b. Navigate to the status by expanding the `mgmt00xst001` system that shows a problem.
 - c. Select **Status** to produce a list of statuses.
4. Expand any `mgmt00xst001` subcomponent that shows a critical or warning event indication and select **Status**.

- a. Review the **Sensor** column and the **Level** column for **Critical Error**, **Major Warning**, or **Minor Warning** items.

If the problem that caused the **Level** item is resolved, right-click the event and select the **Mark Event as Resolved** action.

- b. Follow the online instructions to complete the change.
- c. Review the status list for the other events that might cause the **Health Status** to be red or yellow.
- d. Perform the same steps.

As long as there is a single sensor that is marked as **Critical Error**, **Major Warning**, or **Minor Warning**, the **Health Status** is red or yellow. When you use the **Mark Event as Resolved** action against the sensor, the sensor no longer shows in the status view. If the problem is still not resolved, a new sensor update occurs that reflects the problem. An example might be if a software error event is marked as resolved but the system still detects the problem; then the status is properly reflected in the **Status** display.

Connectivity issues

This topic provides information for troubleshooting connectivity issues. The major focus is on connectivity between the file modules and the control enclosure. Good connectivity is required to troubleshoot control enclosure problems.

Host to file modules connectivity

This procedure is used to troubleshoot Ethernet network connectivity between the host and the file modules. These network paths are used for all system requests and management operations. The paths are also needed for Ethernet network connectivity between the file module and the Storwize V7000.

Within the file modules, two internal 1 GB network ports and two 10 GbE network ports can be configured for system operations.

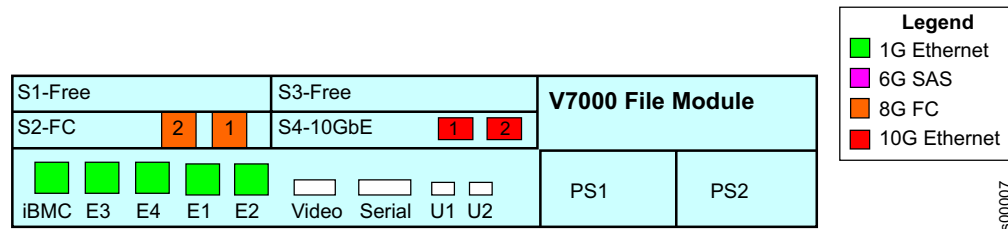


Figure 1. File module Ethernet network connections

Table 8. Ethernet connections available with the file modules

Port	Purpose
Built-in Ethernet port 1	1 GB file module-to-file module interconnect
Built-in Ethernet port 2	1 GB file module-to-file module interconnect
Built-in Ethernet port 3	1 GB external network connection
Built-in Ethernet port 4	1 GB external network connection
PCI slot 4, port 1	10 GbE external network connection
PCI slot 4, port 2	10 GbE external network connection

If you are looking at a problem regarding built-in Ethernet port 1 or built-in Ethernet port 2, refer to “File module to file module.”

Isolation procedures:

Ensure that the file module is powered up before you begin this procedure. The network connection being diagnosed must be connected to an active port on your Ethernet network.

- Determine the state of the Ethernet LEDs examining the LEDs of the Ethernet ports.
- The activity LED flashes when there is activity on the connection. The link state LED must be permanently on. If it is off, the link is not connected.

If your link is not connected, perform 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. Contact your network administrator to verify the switch and network configuration information.
3. Connect the cable to a different port on your Ethernet network.
4. Replace the Ethernet cable.
5. For the 10 GbE Ethernet port, replace the small form-factor pluggable (SFP) transceiver. Refer to “Removing a PCI adapter from a PCI riser-card assembly” on page 98 and “Installing a PCI adapter in a PCI riser-card assembly” on page 99.

File module to file module

This topic covers troubleshooting network connectivity issues between the file modules. These connections are used for internal management operations between the file modules.

This procedure is used to troubleshoot Ethernet network connectivity between both of the file module. These network paths are used for all internal system communication. Between both file module, there are two separate network paths for internal communication, two separate network paths

Table 9. Ethernet ports and type of connections.

Port	Purpose
Built-in Ethernet port 1	1 GB file module-to-file module interconnect
Built-in Ethernet port 2	1 GB file module-to-file module interconnect
Built-in Ethernet port 3	1 GB external network connection
Built-in Ethernet port 4	1 GB external network connection
PCI slot 4, port 1	10 GbE external network connection
PCI slot 4, port 2	10 GbE external network connection

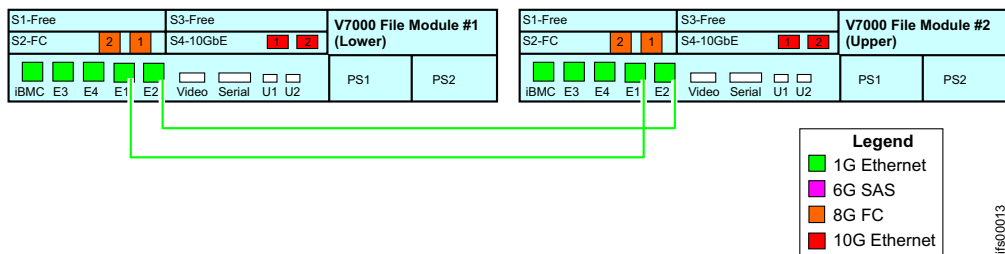


Figure 2. File module node Ethernet network connections. This is a logical diagram of the connectivity and does not reflect the exact physical system.

If you are looking at a problem regarding built-in Ethernet port 3, built-in Ethernet port 4, or any network connections to PCI slot 4, refer to “Host to file modules connectivity” on page 22.

Isolation procedures:

Ensure that both the file module are powered up before you begin this procedure. The network connection being diagnosed must be connected to an active port on your Ethernet network:

- Determine the state of the Ethernet LEDs by examining the Ethernet port LEDs.
- The activity LED flashes when there is activity on the connection. The link state LED must be permanently on. If it is off, the link is not connected.

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

1. Verify that each end of the cable is securely connected.
2. Replace the Ethernet cable.
3. Replace the failed Ethernet port on the server by replacing the system planer. Refer to “Removing the system board” on page 145 and “Installing the system board” on page 147.

File module to control enclosure

This topic covers troubleshooting network connectivity issues between the file modules and the attached control enclosure. These connections are used for block storage system configuration as well command-line interface (CLI) operations to the control enclosure.

This procedure is used to troubleshoot Ethernet network connectivity between the file modules and the control enclosure. These network paths are used for all management operations between the file module and the control enclosure.

There are no direct physical network connections between the file module hardware and the control enclosure. All network connections are done through the customer's network infrastructure. When configuring your customer-supplied network switches, be sure that there is an available communication path between the file module network connections and the control enclosure network connections.

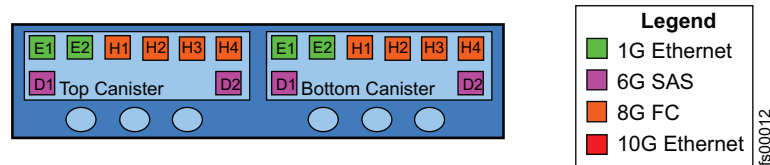


Figure 3. Control enclosure Ethernet network connections. This diagram is conceptual, not a physical representation.

The Storwize V7000 control enclosure diagram shows both canisters side by side; however, the exact physical configuration has an upper and lower canister with the bottom canister inverted.

Connectivity of the control enclosure to the file modules requires that all four of the physical network paths that are available on the control enclosure are connected to the customer network. Ethernet port 1 must be connected to an active port on your Ethernet network.

Verify that the IP configuration is properly set on the Storwize V7000 Unified controller by doing the following:

- Use the USB key to obtain the most comprehensive information for the control enclosure node canister status. The status, speed, and MAC address are returned for each port. Information is returned that identifies whether the node is the configuration node and if any node errors were reported. The service IP address of the control enclosure is also returned. Refer to "Problem: Storage system management IP address unknown" on page 184.
- To find the service IP address for the control enclosure used by the file modules, use the Storwize V7000 Unified management CLI to issue the **lsstoragesystem** command.

Here is an example:

```
>ssh admin@ifsc1uster-ivt
[kd01ghf.ibm]$ lsstoragesystem
name          primaryIP      secondaryIP    id
StorwizeV7000 9.11.137.130  9.11.137.130  00000200A2601508
EFSSG1000I The command completed successfully.
[root@kq186wx.mgmt001st001 ~]#
```

- If the primary and secondary IP address shown by the **lsstoragesystem** CLI do not match the service IP addresses found, put the USB key in the Storwize V7000 enclosure, then use the **chstoragesystem** CLI to change the Storwize V7000 Unified service IPs to match. For example, **chstoragesystem** changes the Service IP address of the Storwize V7000 control enclosure and the address used for the file modules, so you can configure the control enclosure. Here is an example:

```

>ssh admin@ifsccluster-ivt
[kd01ghf.ibm]$ chstoragesystem --ip1 9.71.50.154
EFSSG1000I The command completed successfully.

```

Note: The following procedures require physical access to the system.

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

1. Examine the LEDs of the Ethernet ports. The activity LED flashes when there is activity on the connection. The link state LED must be permanently on. If it is off, the link is not connected.
2. Verify that each end of the cable is securely connected.
3. Verify that the port on the Ethernet switch or hub is configured correctly.
4. Connect the cable to a different port on your Ethernet network.
5. If the status is obtained using the USB key, review all the node errors that are reported.
6. Replace the Ethernet cable.
7. For the 10 Gbps Ethernet port, replace the small form-factor pluggable (SFP) transceiver.
8. Follow the hardware replacement procedure for a node canister.

Fibre connectivity between file modules and control enclosure

This procedure is used to troubleshoot fibre connectivity issues between the file modules and the Storwize V7000 system. The fibre paths are the paths used for transferring data between the file module and the Storwize V7000 system.

Each file module has a dual port FCP adapter card located in PCI slot 2. Both ports are used to connect to the Storwize V7000 system with a connection going to each Storwize V7000 control canister.

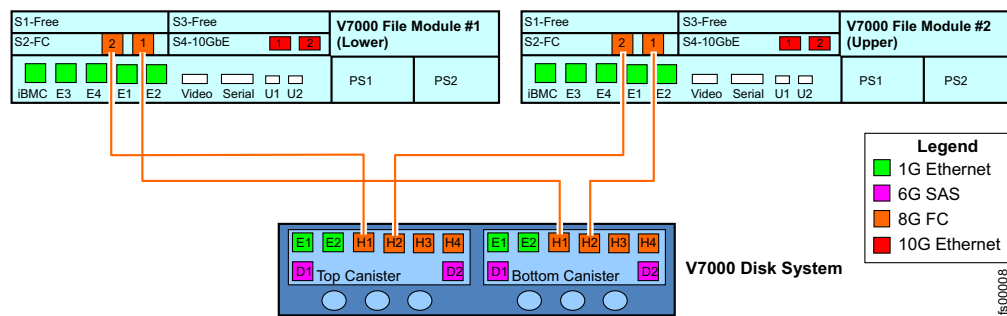


Figure 4. Fibre connections between the file modules and disk system. This is a logical diagram of the connectivity and does not reflect the exact physical system.

The file modules use a dual port FCP adapter card where port 1 is toward the PCI adapter plug thus the diagram reflects that port 2 is to the left of port 1.

The Storwize V7000 system diagram shows both canisters side by side; however, the exact physical configuration has an upper and lower canister with the bottom canister inverted.

In isolating problems, be sure to review the labels on the rear of the systems for exact port plugging.

Software detected problems via event codes:

If you have been directed to this procedure by a software event code, refer to the following procedure to determine the logical to physical mapping of the event then proceed to the physical hardware isolation procedures.

The isolation of fibre connections based on a single error event is not simple. As Figure 4 on page 26 shows, there are two file modules attached to the Storwize V7000 system; however, the logical host name of these systems does not map directly to the connections. The logical host name of the file module depends on which file module is used for initial USB key installation. For example, in Figure 4 on page 26 the file module on the left can have a host name of **mgmt001st001** if the installation was initiated on that node or it might have a host name of **mgmt002st001** if the installation was initiated on the second file module. Each error event is reported against the logical host name where the problem occurred.

For isolation of fibre connections, it is important with a single file module that both fibre connections go to the same port number on both the upper and lower Storwize V7000 node canisters. Port 1 always goes to the upper canister, and port 2 goes to the lower canister.

Use the table for correlating the error code with the physical connections and follow the procedures after the table for enabling the LED indicator on the front of the file module.

Table 10. Error code port location mapping

Error code	Description	File Module HBA Location	Storage Node Canister HBA Port
4B0800	Link failure. Fibre Channel adapter 1, port 1 not up.	PCI slot #2 – port 1 (right port when facing rear of system)	Upper node canister, port H1. OR Upper node canister, port H2.
4B0801	Link failure. Fibre Channel adapter 1, port 2 not up.	PCI slot #2 – port 2 (left port when facing rear of system)	Lower node canister, port H1. OR lower node canister, port H2.
4B0803	Slow connection on Fibre Channel adapter 1, port 1.	PCI slot #2 – port 1 (right port when facing rear of system)	Upper node canister, port H1. OR upper node canister, port H2.
4B0804	Slow connection on Fibre Channel adapter 1, port 2.	PCI slot #2 – port 2 (left port when facing rear of system)	Lower node canister, port H1. OR lower node canister, port H2.

To enable the LED indicator for the node reporting the problem:

1. Log onto the active file module via the CLI interface.
2. Run the command: **cnlocatenode #HOSTNAME on #SECONDS**. **HOSTNAME** is the hostname associated with the error... either **mgmt001st001** or **mgmt002st001**. **#SECONDS** is the number of seconds for the LED indicator to be turned on.

Physical connection and repair:

Each file module has a dual port FCP adapter card located in PCI slot 2. Both ports are used to connect to the Storwize V7000 system with a connection going to each Storwize V7000 node canister.

Table 11. HBA cabling from the file module to Storwize V7000 system

File Module Node # 1		File Module Storage Node # 2	
PCI slot #2, port 1	PCI slot #2, port 2	PCI slot #2, port 1	PCI slot #2, port 2
Connects to Storwize V7000	Connects to Storwize V7000	Connects to Storwize V7000	Connects to Storwize V7000
Lower canister – Fibre port 1	Upper canister – Fibre port 1	Lower canister – Fibre port 2	Upper canister – Fibre port 2

If a problem is detected with a fibre path between the storage node and the control enclosure, check the LED indicators next to the fibre connection ports on both the file module and the Storwize V7000 node canister.

Table 12. LED states and associated actions. For the HBA adapters on the file module check the amber LED lights next to the port.

LED State	Definition and Action
Solid amber LED	This state indicates a good connection status.
Slow flashing amber LED	This state indicates a good connection at the fibre port but a broken connection at the Storwize V7000 node canister. This broken connection is most likely either a fibre cable or the fibre port is bad on the Storwize V7000 node canister.
Rapid flashing amber LED	This state indicates the HBA adapter is attempting to resync the fibre connection. This situation is normally seen after a fibre connection is unplugged and then plugged back in.
No LED	There is no connection detected at all at the file module HBA port. This broken connection is most likely caused by a fibre cable or the HBA adapter has failed.

Table 13. Fibre connection on the Storwize V7000 node canister LED state and associated actions

LED State	Definition and Action
Solid green LED	This state indicates a good connection status.
No LED	There is no connection detected at all at the node canister HBA port.

The recommended repair actions for fibre connections are as follows:

1. Reseat the fibre cable at both the HBA connection and the node canister.
2. Replace the fibre cable.
3. Replace the HBA adapter in the file module. Refer to “Removing a PCI adapter from a PCI riser-card assembly” on page 98 and “Installing a PCI adapter in a PCI riser-card assembly” on page 99

4. Replace the Storwize V7000 node canister. Refer to “Replacing a node canister” on page 204.

Understanding LED hardware indicators

This topic provides information for understanding the LED status of all system components. If you do not have an LED issue or direct access to the system, proceed to the next troubleshooting topic.

File node hardware indicators

Use this information to evaluate the system LEDs, which can often identify the source of an error.

Light path diagnostics is a system of LEDs on various external and internal components of the server. When an error occurs, LEDs are lit throughout the server. By viewing the LEDs in a particular order, you can often identify the source of the error.

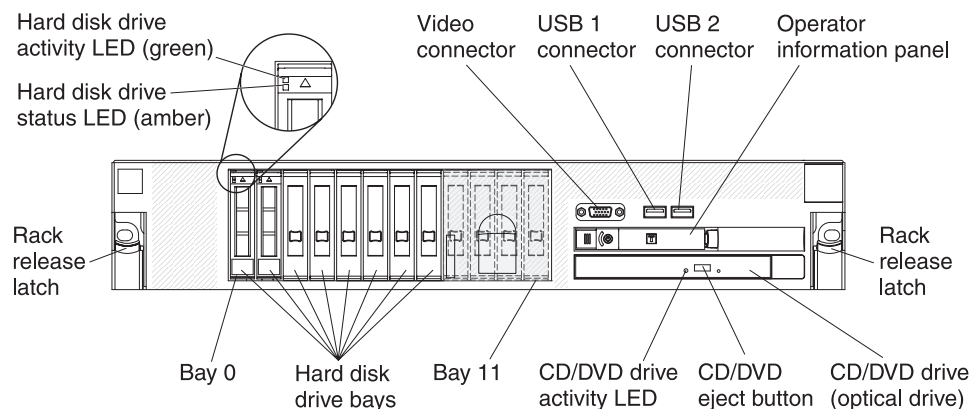
When LEDs are lit to indicate an error, they remain lit when the server is turned off, provided that the server is still connected to power and the power supply is operating correctly.

Before you work inside the server to view light path diagnostics LEDs, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.

If an error occurs, view the light path diagnostics LEDs in the following order:

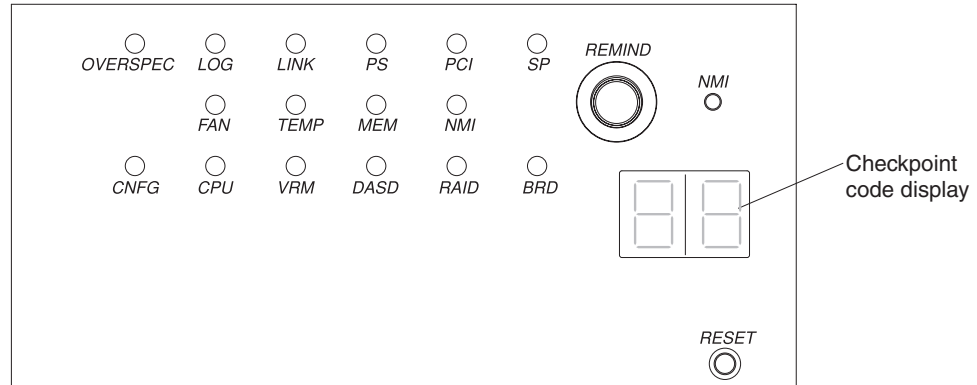
1. Look at the operator information panel on the front of the server.
 - If the information LED is lit, it indicates that information about a suboptimal condition in the server is available in the IMM event log or in the system event log.
 - If the system-error LED is lit, it indicates that an error has occurred; go to step 2.

The following illustration shows the operator information panel on the front of the file node.



2. To view the light path diagnostics panel, slide the latch to the left on the front of the operator information panel and pull the panel forward. This reveals the light path diagnostics panel. Lit LEDs on this panel indicate the type of error that has occurred.

The following illustration shows the light path diagnostics panel.



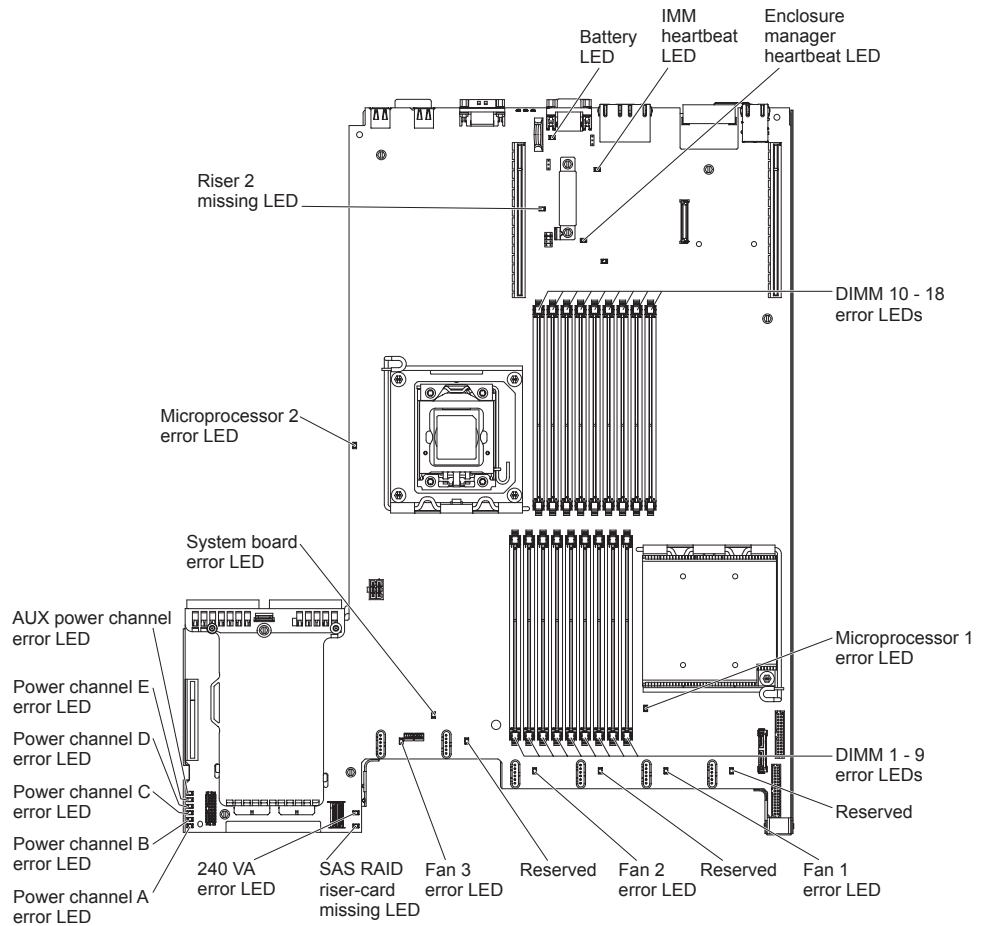
Note any LEDs that are lit, and then push the light path diagnostics panel back into the server.

Note:

- Do not run the server for an extended period of time while the light path diagnostics panel is pulled out of the server.
- Light path diagnostics LEDs remain lit only while the server is connected to power.

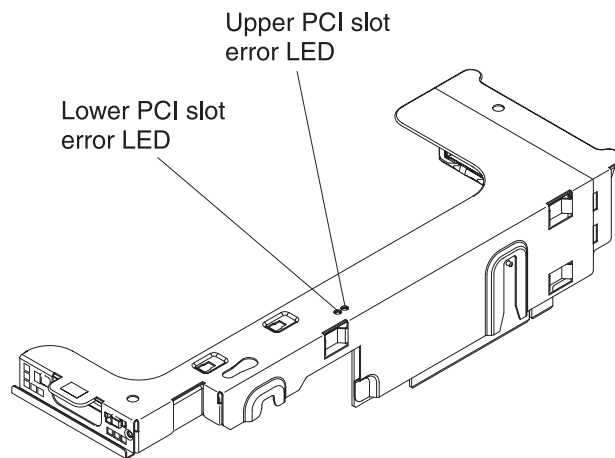
Look at the system service label on the top of the server, which gives an overview of internal components that correspond to the LEDs on the light path diagnostics panel. This information and the information in “Light path diagnostics LEDs” on page 32 can often provide enough information to diagnose the error.

3. Remove the server cover and look inside the server for lit LEDs. A lit LED on or beside a component identifies the component that is causing the error. The following illustration shows the LEDs on the system board.



12v channel error LEDs indicate an overcurrent condition. Refer to the procedure “Solving power problems” in the “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center* to identify the components that are associated with each power channel, and the order in which to troubleshoot the components.

The following illustration shows the LEDs on the riser card.



4. Check the “Power-supply LEDs” on page 35 for the correct combination of power LEDs that should be displayed during typical operation.

Light path diagnostics LEDs

LEDs on the light path diagnostics panel of a Storwize V7000 Unified file module indicate the cause of a problem.

Table 14 shows suggested actions to correct detected problems.

Note: Check the system-event log for additional information before you replace a FRU.

Table 14. LED indicators, corresponding problem causes, and corrective actions

LED	Problem	Action
None, but the system-error LED is lit.	An error has occurred and cannot be diagnosed, or the IMM has failed. The error is not represented by a light path diagnostics LED.	Use the Setup utility to check the system-event log for information about the error.
BRD	An error has occurred on the system board.	<ol style="list-style-type: none"> 1. Check the LEDs on the system board to identify the component that is causing the error. The BRD LED can be lit for the following conditions: <ul style="list-style-type: none"> • Battery • Missing PCI riser-card assembly • Failed voltage regulator 2. Check the system-event log for information about the error. 3. Replace any failed or missing replaceable components, such as the battery or PCI riser-card assembly (refer to the "Troubleshooting the System x3650" in the <i>IBM Storwize V7000 Unified Information Center</i> for more information). 4. If a voltage regulator has failed, replace the system board.
CNFG	<p>A hardware configuration error has occurred.</p> <p>This LED is used with the MEM and CPU LEDs.</p>	
CPU	<p>When only the CPU LED is lit, a microprocessor has failed.</p> <p>When the CPU and CNFG LEDs are lit, an invalid microprocessor configuration has occurred.</p>	<ol style="list-style-type: none"> 1. Determine whether the CNFG LED is also lit. If the CNFG LED is not lit, a microprocessor has failed. <ol style="list-style-type: none"> a. Make sure that the failing microprocessor, which is indicated by a lit LED on the system board, is installed correctly. Refer to "Troubleshooting the System x3650" in the <i>IBM Storwize V7000 Unified Information Center</i> for information about installing a microprocessor. b. If the failure remains, call your next level of support. 2. If the CNFG LED is lit, then an invalid microprocessor configuration has occurred. <ol style="list-style-type: none"> a. Make sure that the microprocessors are compatible with each other. They must match in speed and cache size. To compare the microprocessor information, run the Setup utility and select System Information, then select System Summary, and then select Processor Details. b. Replace an incompatible microprocessor. c. If the failure remains, call your next level of support.

Table 14. LED indicators, corresponding problem causes, and corrective actions (continued)

LED	Problem	Action
DASD	A hard disk drive error has occurred. A hard disk drive has failed or is missing.	<ol style="list-style-type: none"> 1. Check the LEDs on the hard disk drives for the drive with a lit status LED and reseal the hard disk drive. 2. Reseat the hard disk drive backplane. 3. For more information, see “Hard disk drive problems” on page 52. 4. If the error remains, replace the following components in the order listed, restarting the server after each: <ol style="list-style-type: none"> a. Replace the hard disk drive, as described in “Removing a hot-swap hard disk drive” on page 115. 5. If the problem remains, call your next level of support.
FAN	A fan has failed, is operating too slowly, or has been removed. The TEMP LED might also be lit.	<ol style="list-style-type: none"> 1. Reseat the failing fan, which is indicated by a lit LED near the fan connector on the system board. 2. Replace the failing fan, which is indicated by a lit LED near the fan connector on the system board. See “Removing a hot-swap fan” on page 129 for more information. <p>Note: If an LED that is next to an <i>unused</i> fan connector on the system board is lit, a PCI riser-card assembly might be missing; replace the PCI riser-card assembly. Both PCI riser-card assemblies must always be present.</p>
LINK	Reserved.	
LOG	An error message has been written to the system-event log	Check the system logs for information about the error. Replace any components that are identified in the error logs.

Table 14. LED indicators, corresponding problem causes, and corrective actions (continued)

LED	Problem	Action
MEM	<p>When only the MEM LED is lit, a memory error has occurred.</p> <p>When both the MEM and CNFG LEDs are lit, the memory configuration is invalid or the PCI Option ROM is out of resource</p>	<p>Note: Each time you install or remove a DIMM, you must disconnect the server from the power source; then, wait 10 seconds before restarting the server.</p> <ol style="list-style-type: none"> 1. If the MEM LED and the CNFG LED are lit, complete the following steps: <ol style="list-style-type: none"> a. Check the system-event log in the Setup utility. If a PCI Option ROM out-of-resource error log is present, reduce the base system ROM or change the ROM order. b. Run the DSA memory test to isolate the problem. <p>If the test reports that a memory error has occurred, replace the failing DIMM, which is indicated by the lit DIMM latch on the system board (the DIMM LED is underneath the DIMM latch).</p> <p>If the test reports the memory configuration is invalid, repopulate the DIMMs to a supported configuration. (See “Installing a memory module” on page 126 about memory configuration.)</p> 2. If the CNFG LED is not lit, the system might detect a memory error. Complete the following steps to correct the problem: <ul style="list-style-type: none"> • The server did not boot and a failing DIMM LED is lit. <ol style="list-style-type: none"> a. Reseat the DIMM. b. Run the memory test to isolate the problem. c. If the test indicates that a memory error has occurred (check the system log), replace the failing DIMM, which is indicated by the lit DIMM latch on the system board (the DIMM LED is underneath the DIMM latch).
NMI	<p>A non-maskable interrupt has occurred, or the NMI button has been pressed.</p>	<p>Check the system-event log for information about the error.</p>
OVER SPEC	<p>The server was shut down because of a power-supply overload condition on one of the power channels. The power supplies are using more power than their maximum rating.</p>	<ol style="list-style-type: none"> 1. If any of the power channel error LEDs (A, B, C, D, E, or AUX) on the system board are lit also, refer to the section on “Power problems” in the appropriate server guide in “Troubleshooting the System x3650” in the <i>IBM Storwize V7000 Unified Information Center</i>. (For the location of power channel error LEDs, see the section on “Internal connectors, LEDs, and jumpers”.) 2. Check the power-supply LEDs for an error indication (AC LED and DC LED are not both lit, or the information LED is lit). Replace a failing power supply. 3. Remove optional devices from the server.
PCI	<p>An error has occurred on a PCI bus or on the system board. An additional LED is lit next to a failing PCI slot.</p>	<ol style="list-style-type: none"> 1. Check the LEDs on the PCI slots to identify the component that is causing the error. 2. Check the system-event log for information about the error. 3. If you cannot isolate the failing adapter through the LEDs and the information in the system-event log, remove one adapter at a time from the failing PCI bus, and restart the server after each adapter is removed. 4. If the failure remains, call your next level of support.

Table 14. LED indicators, corresponding problem causes, and corrective actions (continued)

LED	Problem	Action
PS	<p>A power supply has failed.</p> <p>Power supply 1 or 2 has failed.</p> <p>When both the PS and CNFG LEDs are lit, the power supply configuration is invalid.</p>	<ol style="list-style-type: none"> 1. Check the power-supply that has an lit amber LED. (See Table 15 on page 36 for more information.) 2. Make sure that the power supplies are seated correctly. 3. Remove one of the power supplies to isolate the failed power supply. 4. Make sure that both power supplies installed in the server are of the same type. 5. Replace the failed power supply.
RAID	Reserved	
SP	The service processor (the IMM) has failed.	<ol style="list-style-type: none"> 1. Remove power from the server; then, reconnect the server to power and restart the server. 2. Update the firmware on the IMM. 3. If the failure remains, call your next level of support.
TEMP	The system temperature has exceeded a threshold level. A failing fan can cause the TEMP LED to be lit. This condition can also be caused by a room temperature that is too high.	<ol style="list-style-type: none"> 1. Check the error log. If a fan has failed, replace it. 2. Make sure that the room temperature is not too high. For server temperature information, see the “Features and specifications” section in the appropriate server guide in “Troubleshooting the System x3650” in the <i>IBM Storwize V7000 Unified Information Center</i>. Also, check the IMM log to see how often the temperature problem occurs and, as appropriate, address possible root causes in the environment if there appears to be an on-going problem. 3. Make sure that the air vents are not blocked. 4. After the over-temperature condition is fixed, the IMM must be rebooted to clear the TEMP LED and return the fan speed to normal. <ul style="list-style-type: none"> Note: An IMM reboot is a concurrent action. <ol style="list-style-type: none"> a. If you are not already logged into the Management Node, log in and start a Terminal session. b. Type <code>ssh <node name></code> and press Enter. <ul style="list-style-type: none"> Note: Example: <code>ssh strg001st001</code> c. Type <code>asu rebootimm --kcs</code> and press Enter. <ul style="list-style-type: none"> Note: If you are using a telnet connection, you can reboot using <code>resetsp</code>. d. Wait for the IMM reboot to complete (typically about 3 minutes). If the reboot is successful, the output of the previous command will be similar to the following: <pre>IBM Advanced Settings Utility version 3.01.67N Licensed Materials - Property of IBM (C) Copyright IBM Corp. 2010 All Rights Reserved Connected via IPMI device driver (KCS interface) Issuing reset command to IMM. The IMM has started the reset. Waiting for the reset to complete. Connected via IPMI device driver (KCS interface) Reset completed successfully.</pre> 5. If the failure remains, call your next level of support.
VRM	Reserved.	

Power-supply LEDs

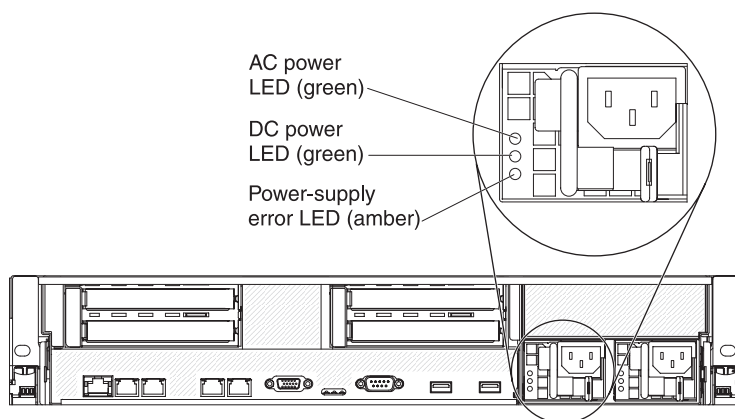
The following minimum configuration is required for the DC LED on the power supply to be lit:

- Power supply
- Power cord

The following minimum configuration is required for the server to start:

- One microprocessor (slot 1)
- One 2 GB DIMM per microprocessor on the system board (slot 3 if only one microprocessor is installed)
- One power supply
- Power cord
- Three cooling fans
- One PCI riser-card assembly in PCI riser connector 2

The following illustration shows the locations of the power-supply LEDs.



The following table describes the problems that are indicated by various combinations of the power-supply LEDs and the power-on LED on the operator information panel and suggested actions to correct the detected problems.

Table 15. Power-supply LEDs

<ul style="list-style-type: none"> • Follow the suggested actions in the order in which they are listed in the Action column until the problem is solved. • If an action is preceded by “(Trained service technician only),” that action must be performed only by a trained service technician. • Refer to “Removing and replacing parts” on page 77 to determine which components are customer replaceable units (CRU) and which components are field replaceable units (FRU). • Go to the IBM support website at Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified to check for technical information, hints, tips, and new device drivers, or to submit a request for information. 					
Power-supply LEDs			Description	Action	Notes
AC	DC	Error			
Off	Off	Off	No ac power to the server or a problem with the ac power source	<ol style="list-style-type: none"> 1. Check the ac power to the server. 2. Make sure that the power cord is connected to a functioning power source. 3. Turn the server off and then turn the server back on. 4. If the problem remains, replace the power supply. 	This is a normal condition when no ac power is present.

Table 15. Power-supply LEDs (continued)

Power-supply LEDs			Description	Action	Notes
AC	DC	Error			
Off	Off	On	No ac power to the server or a problem with the ac power source and the power supply had detected an internal problem	<ol style="list-style-type: none"> 1. Replace the power supply. 2. Make sure that the power cord is connected to a functioning power source. 	This happens only when a second power supply is providing power to the server.
Off	On	Off	Faulty power supply	Replace the power supply.	
Off	On	On	Faulty power supply	Replace the power supply.	
On	Off	Off	Power supply not fully seated, faulty system board, or faulty power supply	<ol style="list-style-type: none"> 1. (Trained service technician only) Reseat the power supply. 2. If a power channel error LED on the system board is not lit, replace the power-supply. (See the documentation that comes with the power supply for instructions.) 3. If a power channel error LED on the system board is lit, (trained service technician only) replace the system board. 	Typically indicates that a power supply is not fully seated.
On	Off or Flashing	On	Faulty power supply	Replace the power supply.	
On	On	Off	Normal operation		
On	On	On	Power supply is faulty but still operational	Replace the power supply.	

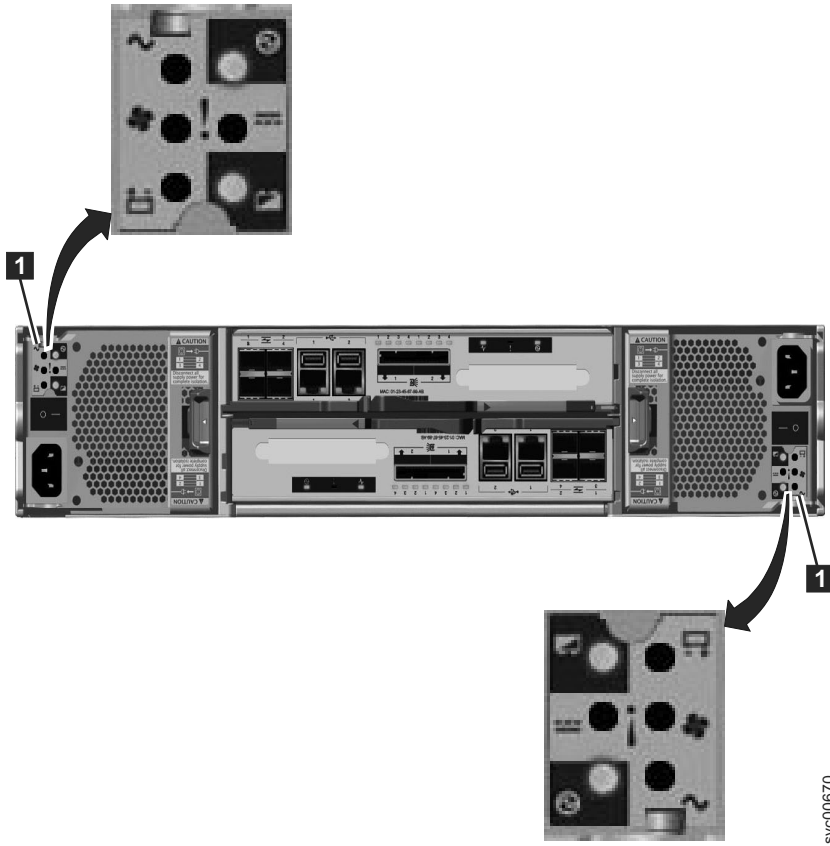
Enclosure hardware indicators

The LEDs provide a general idea of the system status.

This topic shows the status for the control enclosure chassis, power supply units and batteries, and canisters. It does not show the status for the drives.

Table 16 on page 38 shows the power supply LEDs. Figure 5 on page 38 shows the LEDs on the power supply unit for the 2076-112 or the 2076-124. The LEDs on the power supply units for the 2076-312 and 2076-324 are similar, but they are not

shown here.



svc00670

Figure 5. LEDs on the power supply units of the control enclosure

Table 16. Power-supply unit LEDs





Power supply OK 	ac failure 	Fan failure 	dc failure 	Status	Action
On	On	On	On	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.
Off	Off	Off	Off	No ac power to the enclosure.	Turn on power.
Off	Off	Off	On	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.

Table 16. Power-supply unit LEDs (continued)





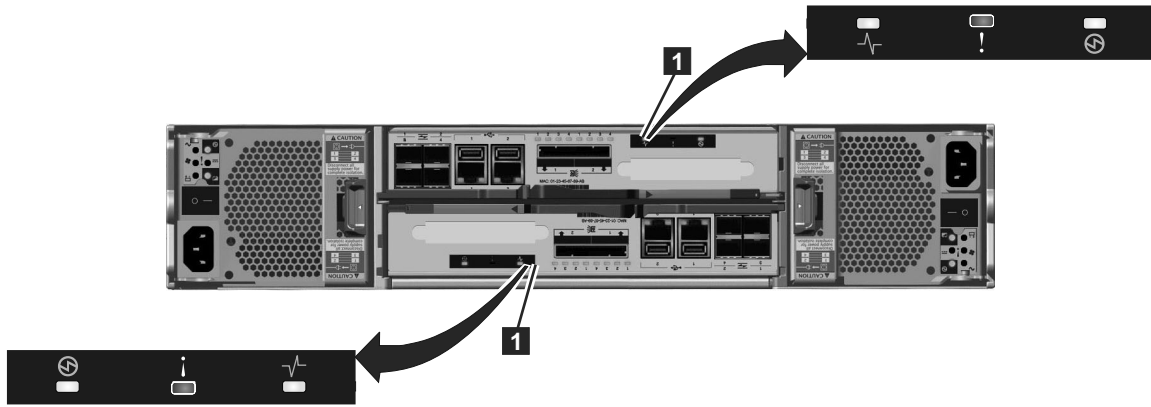
Power supply OK 	ac failure 	Fan failure 	dc failure 	Status	Action
Off	On	Off	On	No ac power to this power supply	<ol style="list-style-type: none"> 1. Check that the switch on the power supply unit is on. 2. Check that the ac power is on. 3. Reseat and replace the power cable.
On	Off	Off	Off	Power supply is on and operational.	No actions
Off	Off	On	Off	Fan failure	Replace the power supply unit.
Off	On	On	On	Communication failure and power supply problem	Replace the power supply unit. If replacing the power supply unit does not fix the problem, replace the enclosure chassis.
Flashing	X	X	X	No canister is operational.	Both canisters are either off or not seated correctly. Turn off the switch on both power supply units and then turn on both switches. If this action does not resolve the problem, remove both canisters slightly and then push the canisters back in.
Off	Flashing	Flashing	Flashing	Firmware is downloading.	No actions. Do not remove ac power. Note: In this case, if there is a battery in a power supply unit, its LEDs also flash.

Table 17 on page 40 shows the three canister status LEDs on each of the node canisters. Figure 6 on page 40 shows the LEDs on the node canister.



svc00672

Figure 6. LEDs on the node canisters

Table 17. Power LEDs


Power LED status 	Description
Off	There is no power to the canister. Try reseating the canister. Go to “Procedure: Reseating a node canister” on page 201. If the state persists, follow the hardware replacement procedures for the parts in the following order: node canister, enclosure chassis.
Slow flashing (1 Hz)	Power is available, but the canister is in standby mode. Try to start the node canister by reseating it. Go to “Procedure: Reseating a node canister” on page 201.
Fast flashing (2 Hz)	The canister is running its power-on self-test (POST). Wait for the test to complete. If the canister remains in this state for more than 10 minutes, try reseating the canister. Go to “Procedure: Reseating a node canister” on page 201. If the state persists, follow the hardware replacement procedure for the node canister.

Table 18 shows the states of the system status and fault LEDs.

Table 18. System status and fault LEDs




System status LED 	Fault LED 	Status 	Action
Off	Off	Code is not active.	<ul style="list-style-type: none"> Follow procedures for reviewing power LEDs. If the power LEDs show green, reseat the node canister. See “Procedure: Reseating a node canister” on page 201. If the LED status does not change, see “Replacing a node canister” on page 204.
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.

Table 18. System status and fault LEDs (continued)




System status LED 	Fault LED 	Status 	Action
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 199.
Flashing	Off	Code is active. Node state is candidate.	Create a clustered system on the node canister, or add the node canister to the clustered system. If the other node canister in the enclosure is in active state, it automatically adds this node canister into the clustered system. A node canister in this state can be managed using the service assistant.
Flashing	On	Code is active. Node state is service.	The node canister cannot become active in a clustered system. Several problems can exist: hardware problem, a problem with the environment or its location, or problems with the code or data on the canister. Follow the procedure to fix the node errors. Go to "Procedure: Fixing node errors" on page 199.
Any	Flashing	The node canister is being identified so that you can locate it.	The fix procedures in the management GUI might have identified the component because it requires servicing. Continue to follow the fix procedures. The service assistant has a function to identify node canisters. If the identification LED is on in error, use the service assistant node actions to turn off the LED.

Table 19 shows the status of the control enclosure batteries.

Table 19. Control enclosure battery LEDs





Battery Good 	Battery Fault 	Description	Action
On	Off	Battery is good and fully charged.	None
Flashing	off	Battery is good but not fully charged. The battery is either charging or a maintenance discharge is being performed.	None

Table 19. Control enclosure battery LEDs (continued)

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

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.

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.

Two tabs are available for monitoring events:

- A **Block** tab for monitoring the SAN volume events and the file system volume events from the control enclosure.
- A **File** tab for monitoring the NAS events from the Storwize V7000 file modules.

When you click the **Block** tab, a **Next recommended action** is shown. Perform the next recommended action before attempting any other recommended actions.

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

Recommended actions (default)

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

- Run a fix procedure.
- View the properties.

Unfixed messages and alerts

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

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

Show all

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

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

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

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

When to use the management GUI

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

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

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

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

If there is an error that is reported, always use the fix procedures within the management GUI to resolve the problem. Always use the fix procedures for both software 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 Storwize V7000 Unified management GUI

This procedure describes how to access the Storwize V7000 Unified management GUI.

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

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

You can use the management GUI to manage your system as soon as you have completed the USB key initialization.

1. Start a supported web browser and point the browser to the management IP address of the file module.
The management IP address is set during the USB key initialization.
2. When the connection is successful, you see a login panel.
3. Log on by using your user name and password. The default user name is admin.
4. When you have logged on, select **Monitoring > Events**.
5. Ensure that the events log is filtered by 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.

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 storage system management GUI” on page 185 or “Problem: Unable to connect to the management GUI” on page 184.

Using fix procedures

You can use fix procedures to diagnose and resolve problems with the Storwize V7000 Unified.

For example, to repair a Storwize V7000 Unified system, you might perform the following tasks:

- Analyze the event log
- Replace failed components
- Verify the status of a repaired device
- Restore a device to an operational state in the system
- Mark the error as fixed in the event log

Fix procedures help simplify these tasks by automating as many of the tasks as possible.

Many of the file module fix procedures are not automated. In these cases, you are directed to a documented procedure in the Storwize V7000 Unified Information Center.

The example uses the management GUI to repair a Storwize V7000 Unified system. Perform the following steps to start the fix procedure:

1. Click **Monitoring > Events** and ensure that you are filtering the event log to display **Recommended actions**.

The list might contain any number of errors that must be repaired. If there is more than one error on the list, the error at the top of the list has the highest priority and must always be fixed first. If you do not fix the higher priority errors first, you might not be able to fix the lower priority errors.

2. Select the error at the top of the list or select the **Next recommended action**.
3. Click **Run Fix Procedure**.

The panel displays the error code and provides a description of the condition.

4. Click **Next** to go forward or **Cancel** to return to the previous panel.

5. One or more panels might be displayed with instructions for you to replace parts or perform other repair activity. If you are not able to complete the actions at this time, click **Cancel** until you return to the previous panel. Click **Cancel** until you are returned to the Next Recommended Actions panel. When you return to the fix procedures, the repair can be restarted from step 1 on page 44. When the actions that you are instructed to perform are complete, click **OK**. When the last repair action is completed, the procedures might attempt to restore failed devices to the system.
6. After you complete the fix, you see the statement Click OK to mark the error as fixed. Click **OK**. This action marks the error as fixed in the event log and prevents this instance of the error from being listed again.
7. When you see the statement The repair has been completed., click **Exit**. If other errors must be fixed, those errors are displayed and the fix procedures continue.
8. If no errors remain, you are shown the following statement: There are no unfixed errors in the event log.

Chapter 4. File module

This topic provides information about troubleshooting the file module, which includes error codes, problem scenarios, software troubleshooting, and removal and replacement instructions.

General file module procedures

This section covers file module general maintenance and repair issues.

Rebooting a file module

Use this procedure to initiate a file module reboot.

Events can occur on a file module that require the hardware to be rebooted.

1. Verify that the file module that the reboot is to be performed against is the passive management node. If the file module is not the passive management node, perform the management node failover procedure. See “Performing management node role failover on a “good” system” on page 153.
2. Log in to the active management node.
3. Shut down and reboot the passive node by using the following CLI command: **stopcluster -node mgmt00Xst001 -restart** (where X is the logical ID of the passive management node being rebooted).
4. The node reboot restarts all services that were previously running.

Removing a file module to perform a maintenance action

You can remove an IBM Storwize V7000 Unified file module to perform maintenance. The procedure that you follow differs slightly, depending on whether you must unplug the power cables.

If you receive an alert event that requires you to service a file module, use the following procedure to remove the file module from the system and perform the required service.

Some field replaceable units (FRUs) are redundant and hot swappable, such as power supplies. When replacing a hot-swap FRU, you have the option of leaving the file module turned on and the power cables connected. Always follow the remove and replace procedure for the FRU. The procedure for the FRU indicates whether the FRU is hot swappable.

If the removal and replacement procedure does not indicate whether the FRU is hot swappable, assume that it is not. In that case use the file module-removal procedure that requires you to disconnect the power cords.

Note: Before removing an file module, you must suspend the file module.

- Remove a file module from the system to replace a hot swappable FRU, as described in “Removing a file module without disconnecting power” on page 48.
- Remove a file module from the system, turn off the node, and disconnect the power cords, as described in “Removing a file module and disconnecting power” on page 48.

Removing a file module and disconnecting power

You can remove an IBM Storwize V7000 Unified file module and disconnect it from its power line cords before performing a maintenance action that requires the file module to have no power.

To identify and perform a service action on any file module that requires you to turn off the power before performing the service action, perform the following procedure.

1. Access and log in to the Storwize V7000 Unified system from the command-line interface.
2. Use the **stopcluster** command to stop the cluster. Alternatively, you can use the **initnode** command to remove the file module from the system and shut down the file module.

If you are shutting down the mgmt001st001 file module, for example, issue the following command:

```
stopcluster -n mgmt001st001
```

3. After the file module shuts down and the power indicator light on the front of the file module is flashing slowly, pull the file module out on its rails.

Note: Label and disconnect both power cords and all external cables from the file module.

4. Remove the file module from the rack if necessary, or locate and use the service ladder, if necessary, to perform the maintenance action on the file module when it is fully extended from the rack.
5. Locate and perform the correct removal and replacement procedure, as described in “Removing and replacing parts” on page 77.

Attention: You can replace only one of the disk drives in the file module. If you must replace both disk drives, contact your next level of support.

6. After replacing the failing part and replacing the file module cover, replace the file module in the rack, if necessary, and reconnect the power cords.

After reconnecting the power cords, the power indicator LED on the front of the file module begins to flash quickly.

7. Push the file module back into the rack.
8. After the power indicator LED on the front of the file module begins to flash slowly, press the power switch that surrounds the indicator light to turn on the file module.

As the file module reboots, the Storwize V7000 Unified system reintegrates it back into the cluster.

You can now perform maintenance on another file module that requires it. After completing all maintenance, perform the system checkout procedure and return the system to the customer.

Removing a file module without disconnecting power

You can work on an IBM Storwize V7000 Unified file module to perform a maintenance action that does not require you to remove its power cords.

Perform the following procedure to remove and replace a hot swappable field replaceable unit (FRU) in a file module when you do not have to remove the file module from the rack to work on it.

1. Access and log in to the Storwize V7000 Unified system from the command-line interface.

2. Issue the **suspendnode** command to remove the file module from the system so that you can work on it.

To remove the mgmt001st001 file module from the system, for example, issue the following command:

```
# suspendnode mgmt001st001
```

3. Wait for the Storwize V7000 Unified system to stop the file module at the clustered trivial database (CTDB) level. The command does not unmount any mounted file systems.

A stopped file module does not participate in the cluster and does not host any records for the clustered trivial database. The IP address of an file module is taken over by another file module and no services are hosted.

You can log on as root and issue the `onnode all service ctdb status` command to view the state of the file module in comparison to another file module in the system. Or you can issue the **lsnode -r** command as a non-root user to view the state of the file module.

The results from running the **lsnode -r** command are similar to the following example:

```
# lsnode -r

Hostname      IP           Description                                     Role
mgmt001st001  10.254.8.2  active management node                       management,interface,storage
mgmt002st001  10.254.8.3  passive management node                     management,interface,storage

Product Version Connection status GPFS status CTDB status Last updated
1.3.0.0-40g OK           active      active      6/27/11 1:51 PM
1.3.0.0-40g OK           active      active      6/27/11 1:51 PM
```

4. Pull the file module out from the rack on its rails.
5. Locate and use the service ladder, if necessary, to perform the maintenance action on the file module when it is fully extended from the rack.
6. Locate and perform the correct removal and replacement procedure, as described in “Removing and replacing parts” on page 77.

Attention: You can replace only one of the disk drives in the file module. If you must replace both disk drives, contact your next level of support.

7. After replacing the failing part and replacing the file module cover, push the file module back in the rack.
8. Use the **resumenode** command to add the file module back into the system so that it can begin to host services.

To add the mgmt001st001 file module back into the system, for example, issue the following command:

```
# resumenode mgmt001st001
```

9. After the Storwize V7000 Unified system reintegrates the file module back into the cluster, the `ctdb status` command shows that the service is active on the file module.

You can now perform maintenance on another file module that requires it. After completing all maintenance, perform the system checkout procedure and return the system to the customer.

Removing and replacing file module components

All replaceable parts are field replaceable units (FRUs) in the IBM Storwize V7000 Unified system. All FRUs must be installed by trained service technicians.

Installation guidelines

To help you work safely with IBM Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and these guidelines.

Before you remove or replace a component, read the following information:

- When you install a file module, take the opportunity to download and apply the most recent firmware updates. This step helps to ensure that any known issues are addressed and that your file module is ready to function at maximum levels of performance.
- Before you install any hardware, make sure that the file module is working correctly. Start the file module, and make sure that the Linux operating system starts. If the file module is not working correctly, see Chapter 3, “Getting started troubleshooting,” on page 9 for diagnostic information.
- Observe good housekeeping in the area where you are working. Place removed covers and other parts in a safe place.
- If you must start the file module while the cover is removed, make sure that no one is near the file module and that no tools or other objects have been left inside the file module.
- Do not attempt to lift an object that you think is too heavy for you. If you have to lift a heavy object, observe the following precautions:
 - Make sure that you can stand safely without slipping.
 - Distribute the weight of the object equally between your feet.
 - Use a slow lifting force. Never move suddenly or twist when you lift a heavy object.
 - To avoid straining the muscles in your back, lift by standing or by pushing up with your leg muscles.
- Make sure that you have an adequate number of properly grounded electrical outlets for the PDUs.
- Back up all important data before you make changes to disk drives.
- Have a small flat-blade screwdriver available.
- To view the error LEDs on the system board and internal components, leave the file module connected to power.
- You do not have to turn off the file module to install or replace hot-swap fans, redundant hot-swap ac power supplies, or hot-plug Universal Serial Bus (USB) devices. However, you must turn off the file module before performing any steps that involve removing or installing adapter cables or non-hot-swap optional devices or components.
- Blue on a component indicates touch points, where you can grip the component to remove it from or install it in the file module, open or close a latch, and so on.
- Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped, which means that if the file module and operating system support hot-swap capability, you can remove or install the component while the file module is running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.
- When you are finished working on the file module, reinstall all safety shields, guards, labels, and ground wires.

Node reliability guidelines

To help ensure proper cooling and system reliability, make sure that:

- Each of the drive bays has a drive or a filler panel and electromagnetic compatibility (EMC) shield installed in it.
- If the server has redundant power, each of the power-supply bays has a power supply installed in it.
- There is adequate space around the server to allow the server cooling system to work properly. Leave approximately 50 mm (2.0 in.) of open space around the front and rear of the server. Do not place objects in front of the fans. For proper cooling and airflow, replace the server cover before turning on the server. Operating the server for extended periods of time (more than 30 minutes) with the server cover removed might damage server components.
- You have followed the cabling instructions that come with optional adapters.
- You have replaced a failed fan within 48 hours.
- You have replaced a hot-swap drive within 2 minutes of removal.
- You operate the server with the air baffles installed. Operating the server without the air baffles might cause the microprocessor to overheat.

Working inside the file module with the power on

Attention: Static electricity that is released to internal file module components when the file module is powered-on might cause the file module to halt, which could result in the loss of data. To avoid this potential problem, always use an electrostatic-discharge wrist strap or other grounding system when working inside the file module with the power on.

The file module supports hot-plug, hot-add, and hot-swap devices and is designed to operate safely while it is turned on and the cover is removed. Follow these guidelines when you work inside a file module that is turned on:

- Avoid wearing loose-fitting clothing on your forearms. Button long-sleeved shirts before working inside the file module; do not wear cuff links while you are working inside the file module.
- Do not allow your necktie or scarf to hang inside the file module.
- Remove jewelry, such as bracelets, necklaces, rings, and loose-fitting wrist watches.
- Remove items from your shirt pocket, such as pens and pencils, that could fall into the file module as you lean over it.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws, into the file module.

Handling static-sensitive devices

Attention: Static electricity can damage the server and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

To reduce the possibility of damage from electrostatic discharge, observe the following precautions:

- Limit your movement. Movement can cause static electricity to build up around you.

- The use of a grounding system is recommended. For example, wear an electrostatic-discharge wrist strap, if one is available. Always use an electrostatic-discharge wrist strap or other grounding system when working inside the server with the power on
- Handle the device carefully, holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an unpainted metal surface on the outside of the server for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it directly into the server without setting down the device. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on the server cover or on a metal surface.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Returning a device or component

When returning a device or component, follow all packaging instructions and use any supplied packaging materials for shipping.

Hard disk drive problems

Use this information to address various hard disk drive issues.

- Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.
- Follow the suggested actions for a Symptom in the order in which they are listed in the Action column until the problem is solved.
- See “Removing and replacing parts” on page 77 to determine which components are customer replaceable units (CRUs) and which components are field replaceable units (FRUs).
- If an action step is preceded by “(Trained service technician only),” that step must be performed only by a trained service technician.

Symptom	Action
A hard disk drive has failed, and the associated amber hard disk drive status LED is lit.	Replace the failed hard disk drive. See “Removing a hot-swap hard disk drive” on page 115 and “Installing a hot-swap hard disk drive” on page 116.

<ul style="list-style-type: none"> • Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47. • Follow the suggested actions for a Symptom in the order in which they are listed in the Action column until the problem is solved. • See “Removing and replacing parts” on page 77 to determine which components are customer replaceable units (CRUs) and which components are field replaceable units (FRUs). • If an action step is preceded by “(Trained service technician only),” that step must be performed only by a trained service technician. 	
Symptom	Action
An installed hard disk drive is not recognized.	<ol style="list-style-type: none"> 1. Observe the associated amber hard disk drive status LED. If the LED is lit, it indicates a drive fault. 2. If the LED is lit, remove the drive from the bay, wait 45 seconds, and reinsert the drive, making sure that the drive assembly connects to the hard disk drive backplane. 3. Observe the associated green hard disk drive activity LED and the amber status LED: <ul style="list-style-type: none"> • If the green activity LED is flashing and the amber status LED is not lit, the drive is recognized by the controller and is working correctly. Run the DSA hard disk drive test to determine whether the drive is detected. • If the green activity LED is flashing and the amber status LED is flashing slowly, the drive is recognized by the controller and is rebuilding. • If neither LED is lit or flashing, check the hard disk drive backplane (go to step 4). • If the green activity LED is flashing and the amber status LED is lit, replace the drive. If the activity of the LEDs remains the same, go to step 4. If the activity of the LEDs changes, return to step 1. 4. Make sure that the hard disk drive backplane is correctly seated. When it is correctly seated, the drive assemblies correctly connect to the backplane without bowing or causing movement of the backplane. 5. Move the hard disk drives to different bays to determine if the drive or the backplane is not functioning. 6. Reseat the backplane power cable and repeat steps 1 through 3. 7. Reseat the backplane signal cable and repeat steps 1 through 3. 8. Suspect the backplane signal cable or the backplane: <ul style="list-style-type: none"> • If the server has eight hot-swap bays: <ol style="list-style-type: none"> a. Replace the affected backplane signal cable. b. Replace the affected backplane. • If the server has 12 hot-swap bays: <ol style="list-style-type: none"> a. Replace the backplane signal cable. b. Replace the backplane. c. Replace the SAS expander card.
Multiple hard disk drives fail.	<p>Make sure that the hard disk drive, SAS RAID controller, and server device drivers and firmware are at the latest level.</p> <p>Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.</p>
Multiple hard disk drives are offline.	<ol style="list-style-type: none"> 1. Review the storage subsystem logs for indications of problems within the storage subsystem, such as backplane or cable problems.
A replacement hard disk drive does not rebuild.	<ol style="list-style-type: none"> 1. Make sure that the hard disk drive is recognized by the controller (the green hard disk drive activity LED is flashing). 2. Review the SAS RAID controller documentation to determine the correct configuration parameters and settings.

<ul style="list-style-type: none"> • Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47. • Follow the suggested actions for a Symptom in the order in which they are listed in the Action column until the problem is solved. • See “Removing and replacing parts” on page 77 to determine which components are customer replaceable units (CRUs) and which components are field replaceable units (FRUs). • If an action step is preceded by “(Trained service technician only),” that step must be performed only by a trained service technician. 	
Symptom	Action
A green hard disk drive activity LED does not accurately represent the actual state of the associated drive.	<ol style="list-style-type: none"> 1. If the green hard disk drive activity LED does not flash when the drive is in use, run the DSA Preboot diagnostic programs to collect error logs. Refer to the “Diagnostics” or “Running the diagnostic programs” section in “Troubleshooting the System x3650” in the <i>IBM Storwize V7000 Unified Information Center</i>. 2. Use one of the following procedures: <ul style="list-style-type: none"> • If the drive passes the test, replace the backplane. • If the drive fails the test, replace the drive.
An amber hard disk drive status LED does not accurately represent the actual state of the associated drive.	<ol style="list-style-type: none"> 1. If the amber hard disk drive LED and the RAID controller software do not indicate the same status for the drive, complete the following steps: <ol style="list-style-type: none"> a. Turn off the server. b. Reseat the SAS controller. c. Reseat the backplane signal cable, backplane power cable, and SAS expander card (if the server has 12 drive bays). d. Reseat the hard disk drive. e. Turn on the server and observe the activity of the hard disk drive LEDs.

Displaying node mirror and hard drive status

The Storwize V7000 Unified system provides a method to check the node mirror status and hard drive status for each file module.

As the root user, you can run a perl script to verify whether or not mirroring is configured. By displaying the mirror status, you can view information that shows the location of each hard drive, the status values of each hard drive, and any errors, if applicable. If the mirror status is re-synchronizing, information that shows the percentage complete for the resynchronization is displayed.

1. Ensure that you are logged into the file module as root.
2. To display mirror status and hard drive status, run the following perl script:

```
# /opt/IBM/sonas/bin/cnrspromptnode.pl -a -c "/opt/IBM/sonas/bin/cnrsQueryNodeDrives.pl"
```

File modules in this Storwize V7000 Unified Cluster

Node	Node Name	Node Details
1.	mgmt001st001	x3650m3 KQ186WX
2.	mgmt002st001	x3650m3 KQ186WV

B. Back to Menus
Choice:

Figure 7. Selecting a file module to display node status

3. Select the number for a file module to display its status. For example, type **1** to select **mgmt001st001**. Press **Enter** to display the information in Figure 8 on page 55, which shows an example of a healthy status for the mirroring and drive

status. The output shows a file module with two hard disk drives.

```

Mirror Information:
  Volume ID                : 3
  Status of volume         : Okay (OKY)
  RAID level               : 1
  Size (in MB)             : 285148
  Physical hard disks (Target ID) : 6 5
  Current operation        : None
  Physical disk I/Os       : Not quiesced

Drive Information:
Total number of drives found: 2

Target on ID #5
  Device is a Hard disk
  Enclosure #              : 1
  Slot #                   : 1
  Connector ID             : 1
  Target ID                : 5
  State                    : Online (ONL)
  Size (in MB)/(in sectors) : 286102/585937500
  Manufacturer             : IBM-ESXS
  Model Number             : XXXXXXXXXXXXX
  Firmware Revision        : XXXX
  Serial No                : XXXXXXXXXXXXXXXXXXXXX
  Drive Type               : SAS
  Protocol                 : SAS
  Error Information
    SMART Error Count      : none
    SMART ASC              : none
    SMART ASCQ             : none

Target on ID #6
  Device is a Hard disk
  Enclosure #              : 1
  Slot #                   : 0
  Connector ID             : 0
  Target ID                : 6
  State                    : Online (ONL)
  Size (in MB)/(in sectors) : 286102/585937500
  Manufacturer             : IBM-ESXS
  Model Number             : XXXXXXXXXXXXX
  Firmware Revision        : XXXX
  Serial No                : XXXXXXXXXXXXXXXXXXXXX
  Drive Type               : SAS
  Protocol                 : SAS
  Error Information
    SMART Error Count      : none
    SMART ASC              : none
    SMART ASCQ             : none

```

Figure 8. Displaying node status

- Review the section for **Mirror Information** and the value for **Status of volume**, then see Table 20 for the possible values for **Status of volume**.

Table 20. Status of volume

Status of volume	Description
Okay (OKY)	The volume is Active and the drives are functioning correctly. The user data is protected if the volume is integrated mirroring or integrated mirroring enhanced.
Degraded (DGD)	The volume is Active. The user data is not fully protected due to a configuration change or drive failure.

Table 20. Status of volume (continued)

Status of volume	Description
Rebuilding (RBLD) or Resyncing (RSY)	A data resynchronization or rebuild might be in progress.
Inactive, Okay (OKY)	The volume is inactive and the drives are functioning correctly. The user data is protected if the current RAID level is RAID 1 (IM) or RAID 1E (IME).
Inactive, Degraded (DGD)	The volume is inactive and the user data is not fully protected due to a configuration change or drive failure; a data resync or rebuild might be in progress.

- Review the section for **Drive information** and the value for **State** Figure 8 on page 55, then see Table 21 to see the possible values for **State** of the drives.

Table 21. State of drives

Status of drives	Description
Online (ONL)	The drive is operational and is part of a logical drive.
Hot Spare (HSP)	The drive is a hot spare that is available for replacing a failed drive in an array.
Ready (RDY)	The drive is ready for use as a normal disk drive; or it is available to be assigned to a disk array or hot spare pool.
Available (AVL)	The drive might or might not be ready, and it is not suitable for inclusion in an array or hot spare pool (for example, it did not spin up, its block size is incorrect, or its media is removable).
Failed (FLD)	The drive was part of a logical drive or was a hot spare drive, and it has failed. It has been taken offline.
Standby (SBY)	This status is used to tag all non-hard disk drive devices.
Missing (MIS)	The hard drive might be removed.
Out of Sync (OSY)	A data resynchronization or rebuild might be in progress.

- See Figure 9 on page 57 for an example that shows that mirroring is re-synchronizing. If a hard disk drive is removed and reinserted, the array starts to resynchronize automatically.

Notelist: You can tell that the mirroring is re-synchronizing when the following conditions are true:

- **State of volume** is **Resyncing (RSY)**
- **Current operation** is **Synchronize**
- **Percentage complete** is displayed

A mirror/volume consists of two hard drives. In Figure 9 on page 57, the section for **Mirror Information** has a status line called **Physical hard disk (Target ID)**. The line shows which drives are part of the mirror/volume.

The **Status of volume** shows **Resyncing (RSY)**.

The mirror consists of **Physical hard disk (Target ID)** of 6 and 9. Drive 9 is in a **State** of **Out of Sync (OSY)**. The **Mirror Information** will also show you the percentage complete for the resynchronization. For example, the percentage complete in Figure 9 on page 57 is **5.23%**.


```

Mirror Information:
Volume ID : 3 <---
Status of volume : Resyncing (RSY) <---
RAID level : 1
Size (in MB) : 285148
Physical hard disks (Target ID) : 6 5 <---
Current operation : Synchronize <---
Physical disk I/Os : Not quiesced
Volume size (in sectors) : 583983104
Number of remaining sectors : 553462899
Percentage complete : 5.23% <---

```

Drive Information:

Total number of drives found: 2

Target on ID #5

```

Device is a Hard disk
Enclosure # : 1
Slot # : 1
Connector ID : 1
Target ID : 5
State : Ready (RDY)
Size (in MB)/(in sectors) : 286102/585937500
Manufacturer : IBM-ESXS
Model Number : XXXXXXXXXXXXX
Firmware Revision : XXXX
Serial No : XXXXXXXXXXXXXXXXXXXXX
Drive Type : SAS
Protocol : SAS
Error Information
  SMART Error Count : none
  SMART ASC : none
  SMART ASCQ : none

```

Target on ID #6

<---

```

Device is a Hard disk
Enclosure # : 1
Slot # : 0
Connector ID : 0
Target ID : 6
State : Online (ONL)
Size (in MB)/(in sectors) : 286102/585937500
Manufacturer : IBM-ESXS
Model Number : XXXXXXXXXXXXX
Firmware Revision : XXXX
Serial No : XXXXXXXXXXXXXXXXXXXXX
Drive Type : SAS
Protocol : SAS
Error Information
  SMART Error Count : none
  SMART ASC : none
  SMART ASCQ : none

```

Figure 9. Example that shows that mirroring is re-synchronizing

If a drive were not synchronized, the status might appear like the status shown in Figure 10 on page 58:

```

Target on ID #5
Device is a Hard disk
Enclosure #           : 1
Slot #               : 1
Connector ID         : 1
Target ID            : 5
State                : Out of Sync (OSY) <---
Size (in MB)/(in sectors) : 286102/585937500
Manufacturer          : IBM-ESXS
Model Number         : XXXXXXXXXXXXX
Firmware Revision    : XXXX
Serial No            : XXXXXXXXXXXXXXXXXXXXX
Drive Type           : SAS
Protocol             : SAS
Error Information
  SMART Error Count   : none
  SMART ASC           : none
  SMART ASCQ         : none

```

Figure 10. Example that shows that a drive is not synchronized

7. See Figure 11 on page 59 for an example of status when there is no mirror. If mirroring is not enabled, the output under **Mirror Information** displays a message that says: **The mirror is not created/configured.** If the mirror is not created, refer to “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center* for information on launching the LSI configuration tool.

```

Mirror Information:
  NOTICE: The mirror is not created/configured.      <---

Drive Information:
Total number of drives found: 2
Target on ID #4
  Device is a Hard disk
  Enclosure #                : 1
  Slot #                     : 1
  Connector ID               : 1
  Target ID                  : 4
  State                      : Ready (RDY)
  Size (in MB)/(in sectors)  : 286102/585937500
  Manufacturer               : IBM-ESXS
  Model Number               : XXXXXXXXXXXXX
  Firmware Revision          : XXXX
  Serial No                  : XXXXXXXXXXXXXXXXXXXXX
  Drive Type                 : SAS
  Protocol                   : SAS
  Error Information
    SMART Error Count       : none
    SMART ASC               : none
    SMART ASCQ              : none

Target on ID #6
  Device is a Hard disk
  Enclosure #                : 1
  Slot #                     : 0
  Connector ID               : 0
  Target ID                  : 6
  State                      : Ready (RDY)
  Size (in MB)/(in sectors)  : 286102/585937500
  Manufacturer               : IBM-ESXS
  Model Number               : XXXXXXXXXXXXX
  Firmware Revision          : XXXX
  Serial No                  : XXXXXXXXXXXXXXXXXXXXX
  Drive Type                 : SAS
  Protocol                   : SAS
  Error Information
    SMART Error Count       : none
    SMART ASC               : none
    SMART ASCQ              : none

```

Figure 11. Example that shows that the mirror is not created

8. See Figure 12 on page 60 for an example of a Self-Monitoring, Analysis and Reporting Technology (**SMART**) error found for a hard drive. SMART adds monitoring and troubleshooting functionality by automatically checking a disk drive's health and reporting potential problems. If any **SMART** errors are detected for a hard drive, you can see the status in the section for **Error Information** as shown in Figure 12 on page 60.

Note: In Figure 12 on page 60 the hard disk drive with **Target ID #6** has a **ASC/ ASCQ** error of **05/00**.

For isolation and the repair of hard disk problems, refer to “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center*.

For a list of **SMART** (ASC/ASCQ) error codes and their descriptions, go to “SMART ASC/ASCQ error codes and messages” on page 60.

```

Mirror Information:
  Volume ID                : 4
  Status of volume         : Resyncing (RSY)
  RAID level               : 1
  Size (in MB)             : 285148
  Physical hard disks (Target ID) : 6 9
  Current operation        : Synchronize
  Physical disk I/Os       : Not quiesced

```

```

Drive Information:
Total number of drives found: 2

```

```

Target on ID #6
  Device is a Hard disk
  Enclosure #              : 1
  Slot #                   : 0
  Connector ID             : 0
  Target ID                : 6
  State                    : Online (ONL)
  Size (in MB)/(in sectors) : 286102/585937500
  Manufacturer             : IBM-ESXS
  Model Number             : MBD2300RC
  Firmware Revision       : SB19
  Serial No                : D009P9A01SJC
  Drive Type               : SAS
  Protocol                 : SAS
  Error Information
    SMART Error Count     : 1
    SMART ASC              : 05*          <---
    SMART ASCQ            : 00*          <---

```

*See Infocenter for SMART ASC/ASCQ error codes and messages

```

Target on ID #9
  Device is a Hard disk
  Enclosure #              : 1
  Slot #                   : 1
  Connector ID             : 1
  Target ID                : 9
  State                    : Out of Sync (OSY)
  Size (in MB)/(in sectors) : 286102/585937500
  Manufacturer             : IBM-ESXS
  Model Number             : MBD2300RC
  Firmware Revision       : SB19
  Serial No                : D009P990184N
  Drive Type               : SAS
  Protocol                 : SAS
  Error Information
    SMART Error Count     : none
    SMART ASC              : none
    SMART ASCQ            : none

```

Figure 12. Example of a SMART error

SMART ASC/ASCQ error codes and messages

Table 22 on page 61 shows descriptions for common Self-Monitoring, Analysis and Reporting Technology (SMART) ASC/ASCQ error codes that are classified for a direct access device. The ASC (additional sense code) and ASCQ (additional sense code qualifier) are known as SCSI additional sense data codes, as defined by SCSI standards. SMART adds monitoring and troubleshooting functionality by automatically checking a disk drive's health and reporting potential problems.

Note: Values in the following table such as “5D” are the same as the “5DH” displayed in the tool; some values such as “0” might have additional padding, so that “0” will be the same as “00.”

Table 22. SMART ASC/ASCQ error codes and messages

ASC	ASCQ	Description
00	00	NO ADDITIONAL SENSE INFORMATION
00	06	I/O PROCESS TERMINATED
00	16	OPERATION IN PROGRESS
00	17	CLEANING REQUESTED
00	1D	ATA PASS THROUGH INFORMATION AVAILABLE
00	1E	CONFLICTING SA CREATION REQUEST
00	1F	LOGICAL UNIT TRANSITIONING TO ANOTHER POWER CONDITION
01	00	NO INDEX/SECTOR SIGNAL
02	00	NO SEEK COMPLETE
03	00	PERIPHERAL DEVICE WRITE FAULT
04	00	LOGICAL UNIT NOT READY
04	01	LOGICAL UNIT IS IN PROCESS OF BECOMING READY
04	02	LOGICAL UNIT NOT READY, INITIALIZING COMMAND REQUIRED
04	03	LOGICAL UNIT NOT READY, MANUAL INTERVENTION REQUIRED
04	04	LOGICAL UNIT NOT READY, FORMAT IN PROGRESS
04	05	LOGICAL UNIT NOT READY, REBUILD IN PROGRESS
04	06	LOGICAL UNIT NOT READY, RECALCULATION IN PROGRESS
04	07	LOGICAL UNIT NOT READY, OPERATION IN PROGRESS
04	09	LOGICAL UNIT NOT READY, SELF-TEST IN PROGRESS
04	0A	LOGICAL UNIT NOT ACCESSIBLE, ASYMMETRIC ACCESS STATE TRANSITION
04	0B	LOGICAL UNIT NOT ACCESSIBLE, TARGET PORT IN STANDBY STATE
04	0C	LOGICAL UNIT NOT ACCESSIBLE, TARGET PORT IN UNAVAILABLE STATE
04	10	LOGICAL UNIT NOT READY, AUXILIARY MEMORY NOT ACCESSIBLE
04	11	LOGICAL UNIT NOT READY, NOTIFY (ENABLE SPINUP) REQUIRED
04	13	LOGICAL UNIT NOT READY, SA CREATION IN PROGRESS
04	14	LOGICAL UNIT NOT READY, SPACE ALLOCATION IN PROGRESS
04	1A	LOGICAL UNIT NOT READY, START STOP UNIT COMMAND IN PROGRESS
05	00	LOGICAL UNIT DOES NOT RESPOND TO SELECTION
06	00	NO REFERENCE POSITION FOUND
07	00	MULTIPLE PERIPHERAL DEVICES SELECTED
08	00	LOGICAL UNIT COMMUNICATION FAILURE
08	01	LOGICAL UNIT COMMUNICATION TIME-OUT
08	02	LOGICAL UNIT COMMUNICATION PARITY ERROR

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
08	03	LOGICAL UNIT COMMUNICATION CRC ERROR (ULTRA-DMA/32)
08	04	UNREACHABLE COPY TARGET
09	00	TRACK FOLLOWING ERROR
09	04	HEAD SELECT FAULT
0A	00	ERROR LOG OVERFLOW
0B	00	WARNING
0B	01	WARNING - SPECIFIED TEMPERATURE EXCEEDED
0B	02	WARNING - ENCLOSURE DEGRADED
0B	03	WARNING - BACKGROUND SELF-TEST FAILED
0B	04	WARNING - BACKGROUND PRE-SCAN DETECTED MEDIUM ERROR
0B	05	WARNING - BACKGROUND MEDIUM SCAN DETECTED MEDIUM ERROR
0B	06	WARNING - NON-VOLATILE CACHE NOW VOLATILE
0B	07	WARNING - DEGRADED POWER TO NON-VOLATILE CACHE
0B	08	WARNING - POWER LOSS EXPECTED
0C	02	WRITE ERROR - AUTO REALLOCATION FAILED
0C	03	WRITE ERROR - RECOMMEND REASSIGNMENT
0C	04	COMPRESSION CHECK MISCOMPARE ERROR
0C	05	DATA EXPANSION OCCURRED DURING COMPRESSION
0C	06	BLOCK NOT COMPRESSIBLE
0C	0B	AUXILIARY MEMORY WRITE ERROR
0C	0C	WRITE ERROR - UNEXPECTED UNSOLICITED DATA
0C	0D	WRITE ERROR - NOT ENOUGH UNSOLICITED DATA
0D	00	ERROR DETECTED BY THIRD PARTY TEMPORARY INITIATOR
0D	01	THIRD PARTY DEVICE FAILURE
0D	02	COPY TARGET DEVICE NOT REACHABLE
0D	03	INCORRECT COPY TARGET DEVICE TYPE
0D	04	COPY TARGET DEVICE DATA UNDERRUN
0D	05	COPY TARGET DEVICE DATA OVERRUN
0E	00	INVALID INFORMATION UNIT
0E	01	INFORMATION UNIT TOO SHORT
0E	02	INFORMATION UNIT TOO LONG
0E	03	INVALID FIELD IN COMMAND INFORMATION UNIT
10	00	ID CRC OR ECC ERROR
10	01	LOGICAL BLOCK GUARD CHECK FAILED
10	02	LOGICAL BLOCK APPLICATION TAG CHECK FAILED
10	03	LOGICAL BLOCK REFERENCE TAG CHECK FAILED
11	00	UNRECOVERED READ ERROR
11	01	READ RETRIES EXHAUSTED

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
11	02	ERROR TOO LONG TO CORRECT
11	03	MULTIPLE READ ERRORS
11	04	UNRECOVERED READ ERROR - AUTO REALLOCATE FAILED
11	0A	MISCORRECTED ERROR
11	0B	UNRECOVERED READ ERROR - RECOMMEND REASSIGNMENT
11	0C	UNRECOVERED READ ERROR - RECOMMEND REWRITE THE DATA
11	0D	DE-COMPRESSION CRC ERROR
11	0E	CANNOT DECOMPRESS USING DECLARED ALGORITHM
11	12	AUXILIARY MEMORY READ ERROR
11	13	READ ERROR - FAILED RETRANSMISSION REQUEST
11	14	READ ERROR - LBA MARKED BAD BY APPLICATION CLIENT
12	00	ADDRESS MARK NOT FOUND FOR ID FIELD
13	00	ADDRESS MARK NOT FOUND FOR DATA FIELD
14	00	RECORDED ENTITY NOT FOUND
14	01	RECORD NOT FOUND
14	05	RECORD NOT FOUND - RECOMMEND REASSIGNMENT
14	06	RECORD NOT FOUND - DATA AUTO-REALLOCATED
15	00	RANDOM POSITIONING ERROR
15	01	MECHANICAL POSITIONING ERROR
15	02	POSITIONING ERROR DETECTED BY READ OF MEDIUM
16	00	DATA SYNCHRONIZATION MARK ERROR
16	01	DATA SYNC ERROR - DATA REWRITTEN
16	02	DATA SYNC ERROR - RECOMMEND REWRITE
16	03	DATA SYNC ERROR - DATA AUTO-REALLOCATED
16	04	DATA SYNC ERROR - RECOMMEND REASSIGNMENT
17	00	RECOVERED DATA WITH NO ERROR CORRECTION APPLIED
17	01	RECOVERED DATA WITH RETRIES
17	02	RECOVERED DATA WITH POSITIVE HEAD OFFSET
17	03	RECOVERED DATA WITH NEGATIVE HEAD OFFSET
17	05	RECOVERED DATA USING PREVIOUS SECTOR ID
17	06	RECOVERED DATA WITHOUT ECC - DATA AUTO-REALLOCATED
17	07	RECOVERED DATA WITHOUT ECC - RECOMMEND REASSIGNMENT
17	08	RECOVERED DATA WITHOUT ECC - RECOMMEND REWRITE
17	09	RECOVERED DATA WITHOUT ECC - DATA REWRITTEN
18	00	RECOVERED DATA WITH ERROR CORRECTION APPLIED
18	01	RECOVERED DATA WITH ERROR CORR. & RETRIES APPLIED
18	02	RECOVERED DATA - DATA AUTO-REALLOCATED
18	05	RECOVERED DATA - RECOMMEND REASSIGNMENT

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
18	06	RECOVERED DATA - RECOMMEND REWRITE
18	07	RECOVERED DATA WITH ECC - DATA REWRITTEN
19	00	DEFECT LIST ERROR
19	01	DEFECT LIST NOT AVAILABLE
19	02	DEFECT LIST ERROR IN PRIMARY LIST
19	03	DEFECT LIST ERROR IN GROWN LIST
1A	00	PARAMETER LIST LENGTH ERROR
1B	00	SYNCHRONOUS DATA TRANSFER ERROR
1C	00	DEFECT LIST NOT FOUND
1C	01	PRIMARY DEFECT LIST NOT FOUND
1C	02	GROWN DEFECT LIST NOT FOUND
1D	00	MISCOMPARE DURING VERIFY OPERATION
1D	01	MISCOMPARE VERIFY OF UNMAPPED LBA
1E	00	RECOVERED ID WITH ECC CORRECTION
1F	00	PARTIAL DEFECT LIST TRANSFER
20	00	INVALID COMMAND OPERATION CODE
20	01	ACCESS DENIED - INITIATOR PENDING-ENROLLED
20	02	ACCESS DENIED - NO ACCESS RIGHTS
20	03	ACCESS DENIED - INVALID MGMT ID KEY
20	08	ACCESS DENIED - ENROLLMENT CONFLICT
20	09	ACCESS DENIED - INVALID LU IDENTIFIER
20	0A	ACCESS DENIED - INVALID PROXY TOKEN
20	0B	ACCESS DENIED - ACL LUN CONFLICT
21	00	LOGICAL BLOCK ADDRESS OUT OF RANGE
21	01	INVALID ELEMENT ADDRESS
22	00	ILLEGAL FUNCTION (USE 20 00, 24 00, OR 26 00)
24	00	INVALID FIELD IN CDB
24	01	CDB DECRYPTION ERROR
24	08	INVALID XCDB
25	00	LOGICAL UNIT NOT SUPPORTED
26	00	INVALID FIELD IN PARAMETER LIST
26	01	PARAMETER NOT SUPPORTED
26	02	PARAMETER VALUE INVALID
26	03	THRESHOLD PARAMETERS NOT SUPPORTED
26	04	INVALID RELEASE OF PERSISTENT RESERVATION
26	05	DATA DECRYPTION ERROR
26	06	TOO MANY TARGET DESCRIPTORS
26	07	UNSUPPORTED TARGET DESCRIPTOR TYPE CODE
26	08	TOO MANY SEGMENT DESCRIPTORS
26	09	UNSUPPORTED SEGMENT DESCRIPTOR TYPE CODE

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
26	0A	UNEXPECTED INEXACT SEGMENT
26	0B	INLINE DATA LENGTH EXCEEDED
26	0C	INVALID OPERATION FOR COPY SOURCE OR DESTINATION
26	0D	COPY SEGMENT GRANULARITY VIOLATION
26	0E	INVALID PARAMETER WHILE PORT IS ENABLED
27	00	WRITE PROTECTED
27	01	HARDWARE WRITE PROTECTED
27	02	LOGICAL UNIT SOFTWARE WRITE PROTECTED
27	07	SPACE ALLOCATION FAILED WRITE PROTECT
28	00	NOT READY TO READY CHANGE, MEDIUM MAY HAVE CHANGED
28	01	IMPORT OR EXPORT ELEMENT ACCESSED
29	00	POWER ON, RESET, OR BUS DEVICE RESET OCCURRED
29	01	POWER ON OCCURRED
29	02	SCSI BUS RESET OCCURRED
29	03	BUS DEVICE RESET FUNCTION OCCURRED
29	04	DEVICE INTERNAL RESET
29	05	TRANSCEIVER MODE CHANGED TO SINGLE-ENDED
29	06	TRANSCEIVER MODE CHANGED TO LVD
29	07	I_T NEXUS LOSS OCCURRED
2A	00	PARAMETERS CHANGED
2A	01	MODE PARAMETERS CHANGED
2A	02	LOG PARAMETERS CHANGED
2A	03	RESERVATIONS PREEMPTED
2A	04	RESERVATIONS RELEASED
2A	05	REGISTRATIONS PREEMPTED
2A	06	ASYMMETRIC ACCESS STATE CHANGED
2A	07	IMPLICIT ASYMMETRIC ACCESS STATE TRANSITION FAILED
2A	08	PRIORITY CHANGED
2A	09	CAPACITY DATA HAS CHANGED
2A	0A	ERROR HISTORY I_T NEXUS CLEARED
2A	0B	ERROR HISTORY SNAPSHOT RELEASED
2A	10	TIMESTAMP CHANGED
2A	14	SA CREATION CAPABILITIES DATA HAS CHANGED
2B	00	COPY CANNOT EXECUTE SINCE HOST CANNOT DISCONNECT
2C	00	COMMAND SEQUENCE ERROR
2C	05	ILLEGAL POWER CONDITION REQUEST
2C	07	PREVIOUS BUSY STATUS
2C	08	PREVIOUS TASK SET FULL STATUS
2C	09	PREVIOUS RESERVATION CONFLICT STATUS

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
2C	0C	ORWRITE GENERATION DOES NOT MATCH
2F	00	COMMANDS CLEARED BY ANOTHER INITIATOR
2F	01	COMMANDS CLEARED BY POWER LOSS NOTIFICATION
2F	02	COMMANDS CLEARED BY DEVICE SERVER
30	00	INCOMPATIBLE MEDIUM INSTALLED
30	01	CANNOT READ MEDIUM - UNKNOWN FORMAT
30	02	CANNOT READ MEDIUM - INCOMPATIBLE FORMAT
30	03	CLEANING CARTRIDGE INSTALLED
30	04	CANNOT WRITE MEDIUM - UNKNOWN FORMAT
30	05	CANNOT WRITE MEDIUM - INCOMPATIBLE FORMAT
30	06	CANNOT FORMAT MEDIUM - INCOMPATIBLE MEDIUM
30	07	CLEANING FAILURE
30	0A	CLEANING REQUEST REJECTED
31	00	MEDIUM FORMAT CORRUPTED
31	01	FORMAT COMMAND FAILED
32	00	NO DEFECT SPARE LOCATION AVAILABLE
32	01	DEFECT LIST UPDATE FAILURE
34	00	ENCLOSURE FAILURE
35	00	ENCLOSURE SERVICES FAILURE
35	01	UNSUPPORTED ENCLOSURE FUNCTION
35	02	ENCLOSURE SERVICES UNAVAILABLE
35	03	ENCLOSURE SERVICES TRANSFER FAILURE
35	04	ENCLOSURE SERVICES TRANSFER REFUSED
35	05	ENCLOSURE SERVICES CHECKSUM ERROR
37	00	ROUNDED PARAMETER
38	07	THIN PROVISIONING SOFT THRESHOLD REACHED
39	00	SAVING PARAMETERS NOT SUPPORTED
3A	00	MEDIUM NOT PRESENT
3A	01	MEDIUM NOT PRESENT - TRAY CLOSED
3A	02	MEDIUM NOT PRESENT - TRAY OPEN
3A	03	MEDIUM NOT PRESENT - LOADABLE
3A	04	MEDIUM NOT PRESENT - MEDIUM AUXILIARY MEMORY ACCESSIBLE
3B	0D	MEDIUM DESTINATION ELEMENT FULL
3B	0E	MEDIUM SOURCE ELEMENT EMPTY
3B	11	MEDIUM MAGAZINE NOT ACCESSIBLE
3B	12	MEDIUM MAGAZINE REMOVED
3B	13	MEDIUM MAGAZINE INSERTED
3B	14	MEDIUM MAGAZINE LOCKED
3B	15	MEDIUM MAGAZINE UNLOCKED

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
3D	00	INVALID BITS IN IDENTIFY MESSAGE
3E	00	LOGICAL UNIT HAS NOT SELF-CONFIGURED YET
3E	01	LOGICAL UNIT FAILURE
3E	02	TIMEOUT ON LOGICAL UNIT
3E	03	LOGICAL UNIT FAILED SELF-TEST
3E	04	LOGICAL UNIT UNABLE TO UPDATE SELF-TEST LOG
3F	00	TARGET OPERATING CONDITIONS HAVE CHANGED
3F	01	MICROCODE HAS BEEN CHANGED
3F	02	CHANGED OPERATING DEFINITION
3F	03	INQUIRY DATA HAS CHANGED
3F	04	COMPONENT DEVICE ATTACHED
3F	05	DEVICE IDENTIFIER CHANGED
3F	06	REDUNDANCY GROUP CREATED OR MODIFIED
3F	07	REDUNDANCY GROUP DELETED
3F	08	SPARE CREATED OR MODIFIED
3F	09	SPARE DELETED
3F	0A	VOLUME SET CREATED OR MODIFIED
3F	0B	VOLUME SET DELETED
3F	0C	VOLUME SET DEASSIGNED
3F	0D	VOLUME SET REASSIGNED
3F	0E	REPORTED LUNS DATA HAS CHANGED
3F	0F	ECHO BUFFER OVERWRITTEN
3F	10	MEDIUM LOADABLE
3F	11	MEDIUM AUXILIARY MEMORY ACCESSIBLE
3F	12	ISCSI IP ADDRESS ADDED
3F	13	ISCSI IP ADDRESS REMOVED
3F	14	ISCSI IP ADDRESS CHANGED
40	00	RAM FAILURE
40	NN	DIAGNOSTIC FAILURE ON COMPONENT NN
41	00	DATA PATH FAILURE
42	00	POWER-ON OR SELF-TEST FAILURE
43	00	MESSAGE ERROR
44	00	INTERNAL TARGET FAILURE
44	71	ATA DEVICE FAILED SET FEATURES
45	00	SELECT OR RESELECT FAILURE
46	00	UNSUCCESSFUL SOFT RESET
47	00	SCSI PARITY ERROR
47	01	DATA PHASE CRC ERROR DETECTED
47	02	SCSI PARITY ERROR DETECTED DURING ST DATA PHASE
47	03	INFORMATION UNIT IUCRC ERROR DETECTED

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
47	04	ASYNCHRONOUS INFORMATION PROTECTION ERROR DETECTED
47	05	PROTOCOL SERVICE CRC ERROR
47	06	PHY TEST FUNCTION IN PROGRESS
47	7F	SOME COMMANDS CLEARED BY ISCSI PROTOCOL EVENT
48	00	INITIATOR DETECTED ERROR MESSAGE RECEIVED
49	00	INVALID MESSAGE ERROR
4A	00	COMMAND PHASE ERROR
4B	00	DATA PHASE ERROR
4B	01	INVALID TARGET PORT TRANSFER TAG RECEIVED
4B	02	TOO MUCH WRITE DATA
4B	03	ACK/NAK TIMEOUT
4B	04	NAK RECEIVED
4B	05	DATA OFFSET ERROR
4B	06	INITIATOR RESPONSE TIMEOUT
4B	07	CONNECTION LOST
4C	00	LOGICAL UNIT FAILED SELF-CONFIGURATION
4D	NN	TAGGED OVERLAPPED COMMANDS (NN = TASK TAG)
4E	00	OVERLAPPED COMMANDS ATTEMPTED
53	00	MEDIA LOAD OR EJECT FAILED
53	02	MEDIUM REMOVAL PREVENTED
55	01	SYSTEM BUFFER FULL
55	02	INSUFFICIENT RESERVATION RESOURCES
55	03	INSUFFICIENT RESOURCES
55	04	INSUFFICIENT REGISTRATION RESOURCES
55	05	INSUFFICIENT ACCESS CONTROL RESOURCES
55	06	AUXILIARY MEMORY OUT OF SPACE
55	0B	INSUFFICIENT POWER FOR OPERATION
5A	00	OPERATOR REQUEST OR STATE CHANGE INPUT
5A	01	OPERATOR MEDIUM REMOVAL REQUEST
5A	02	OPERATOR SELECTED WRITE PROTECT
5A	03	OPERATOR SELECTED WRITE PERMIT
5B	00	LOG EXCEPTION
5B	01	THRESHOLD CONDITION MET
5B	02	LOG COUNTER AT MAXIMUM
5B	03	LOG LIST CODES EXHAUSTED
5C	00	RPL STATUS CHANGE
5C	01	SPINDLES SYNCHRONIZED
5C	02	SPINDLES NOT SYNCHRONIZED
5D	00	FAILURE PREDICTION THRESHOLD EXCEEDED

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
5D	10	HARDWARE IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	11	HARDWARE IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	12	HARDWARE IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	13	HARDWARE IMPENDING FAILURE SEEK ERROR RATE TOO HIGH
5D	14	HARDWARE IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	15	HARDWARE IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	16	HARDWARE IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	17	HARDWARE IMPENDING FAILURE CHANNEL PARAMETRICS
5D	18	HARDWARE IMPENDING FAILURE CONTROLLER DETECTED
5D	19	HARDWARE IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	1A	HARDWARE IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	1B	HARDWARE IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	1C	HARDWARE IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT
5D	20	CONTROLLER IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	21	CONTROLLER IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	22	CONTROLLER IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	23	CONTROLLER IMPENDING FAILURE SEEK ERROR RATE TOO HIGH
5D	24	CONTROLLER IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	25	CONTROLLER IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	26	CONTROLLER IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	27	CONTROLLER IMPENDING FAILURE CHANNEL PARAMETRICS
5D	28	CONTROLLER IMPENDING FAILURE CONTROLLER DETECTED
5D	29	CONTROLLER IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	2A	CONTROLLER IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	2B	CONTROLLER IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	2C	CONTROLLER IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT
5D	30	DATA CHANNEL IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	31	DATA CHANNEL IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	32	DATA CHANNEL IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	33	DATA CHANNEL IMPENDING FAILURE SEEK ERROR RATE TOO HIGH

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
5D	34	DATA CHANNEL IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	35	DATA CHANNEL IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	36	DATA CHANNEL IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	37	DATA CHANNEL IMPENDING FAILURE CHANNEL PARAMETRICS
5D	38	DATA CHANNEL IMPENDING FAILURE CONTROLLER DETECTED
5D	39	DATA CHANNEL IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	3A	DATA CHANNEL IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	3B	DATA CHANNEL IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	3C	DATA CHANNEL IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT
5D	40	SERVO IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	41	SERVO IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	42	SERVO IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	43	SERVO IMPENDING FAILURE SEEK ERROR RATE TOO HIGH
5D	44	SERVO IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	45	SERVO IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	46	SERVO IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	47	SERVO IMPENDING FAILURE CHANNEL PARAMETRICS
5D	48	SERVO IMPENDING FAILURE CONTROLLER DETECTED
5D	49	SERVO IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	4A	SERVO IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	4B	SERVO IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	4C	SERVO IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT
5D	50	SPINDLE IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	51	SPINDLE IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	52	SPINDLE IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	53	SPINDLE IMPENDING FAILURE SEEK ERROR RATE TOO HIGH
5D	54	SPINDLE IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	55	SPINDLE IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	56	SPINDLE IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	57	SPINDLE IMPENDING FAILURE CHANNEL PARAMETRICS
5D	58	SPINDLE IMPENDING FAILURE CONTROLLER DETECTED
5D	59	SPINDLE IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	5A	SPINDLE IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	5B	SPINDLE IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	5C	SPINDLE IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT

Table 22. SMART ASC/ASCQ error codes and messages (continued)

ASC	ASCQ	Description
5D	60	FIRMWARE IMPENDING FAILURE GENERAL HARD DRIVE FAILURE
5D	61	FIRMWARE IMPENDING FAILURE DRIVE ERROR RATE TOO HIGH
5D	62	FIRMWARE IMPENDING FAILURE DATA ERROR RATE TOO HIGH
5D	63	FIRMWARE IMPENDING FAILURE SEEK ERROR RATE TOO HIGH
5D	64	FIRMWARE IMPENDING FAILURE TOO MANY BLOCK REASSIGNS
5D	65	FIRMWARE IMPENDING FAILURE ACCESS TIMES TOO HIGH
5D	66	FIRMWARE IMPENDING FAILURE START UNIT TIMES TOO HIGH
5D	67	FIRMWARE IMPENDING FAILURE CHANNEL PARAMETRICS
5D	68	FIRMWARE IMPENDING FAILURE CONTROLLER DETECTED
5D	69	FIRMWARE IMPENDING FAILURE THROUGHPUT PERFORMANCE
5D	6A	FIRMWARE IMPENDING FAILURE SEEK TIME PERFORMANCE
5D	6B	FIRMWARE IMPENDING FAILURE SPIN-UP RETRY COUNT
5D	6C	FIRMWARE IMPENDING FAILURE DRIVE CALIBRATION RETRY COUNT
5D	FF	FAILURE PREDICTION THRESHOLD EXCEEDED (FALSE)
5E	00	LOW POWER CONDITION ON
5E	01	IDLE CONDITION ACTIVATED BY TIMER
5E	02	STANDBY CONDITION ACTIVATED BY TIMER
5E	03	IDLE CONDITION ACTIVATED BY COMMAND
5E	04	STANDBY CONDITION ACTIVATED BY COMMAND
5E	05	IDLE_B CONDITION ACTIVATED BY TIMER
5E	06	IDLE_B CONDITION ACTIVATED BY COMMAND
5E	07	IDLE_C CONDITION ACTIVATED BY TIMER
5E	08	IDLE_C CONDITION ACTIVATED BY COMMAND
5E	09	STANDBY_Y CONDITION ACTIVATED BY TIMER
5E	0A	STANDBY_Y CONDITION ACTIVATED BY COMMAND
65	00	VOLTAGE FAULT
67	0A	SET TARGET PORT GROUPS COMMAND FAILED
67	0B	ATA DEVICE FEATURE NOT ENABLED
74	08	DIGITAL SIGNATURE VALIDATION FAILURE
74	0C	UNABLE TO DECRYPT PARAMETER LIST
74	10	SA CREATION PARAMETER VALUE INVALID
74	11	SA CREATION PARAMETER VALUE REJECTED
74	12	INVALID SA USAGE
74	30	SA CREATION PARAMETER NOT SUPPORTED
74	40	AUTHENTICATION FAILED
74	71	LOGICAL UNIT ACCESS NOT AUTHORIZED
74	79	SECURITY CONFLICT IN TRANSLATED DEVICE

Monitoring memory usage on a file module

Use this procedure to monitor memory usage on a file module.

1. Login to the file module and issue command `lsperfdata -g memory_free_usage -t hour -n <node> | tail`.
2. If the file module shows diminishing memory and is reaching full capacity, initiate a file module reboot. See “Shut down or reboot a file module or clustered system” in the *IBM Storwize V7000 Unified Information Center*.

Errors and messages

A variety of system errors and messages can indicate conditions that range from simple typing errors to problems with system devices or programs.

Refer to the following topics for information on errors and messages.

Note: For reference or repair information on non-Storwize V7000 Unified components, refer to the user documentation provided with those components.

Understanding error codes

The Storwize V7000 Unified error codes convey specific information in their alphanumeric sequence.

Tip: Search for most error code or event IDs by using just the ID. For an ID of 66012FC, for example, just search on 66012FC. If you get an error code similar to “01E0”, use wildcards and search on *01E0*. With 66012FC, you could use wildcards and search on 66012* or, if you seek a much broader range of results, an ID shortened to 66*. For IDs such as EFSSP1002C, do not search on the entire string, but remove the “EFS” and search on “SP1002C” or, again, use wildcards and search on a value such as *1002*.

Error code information

The following tables show the error code elements: ACDDDDx and provide information on what the various elements represent.

Table 23. Error code information

Code element	Information
A	Originating role information
C	Originating hardware or software code
DDDD	Specific error code
x	Severity of the error code

Originating device information

The following table presents the alphanumeric symbol in the A position that indicates the originating device.

Table 24. Originating role information

A = Originating role information in sequence AC-DDDD	
Code	Device
0/1	Management node error codes
2/3	File Module role error codes
4/5	Storage node role error codes

Table 24. Originating role information (continued)

A = Originating role information in sequence AC-DDDD	
Code	Device
6	Storage node role error codes
8	Ethernet switch error codes.

Table 25. Ethernet role and port reference

File Module function	Ports
Interface role	<ul style="list-style-type: none"> • 0/1 attach to the switch ports • 2/3 attach to the your IP network • 4/5 go to the 10GB (not currently supported) • 4/5/6/7 attach to the 4-port card
Management role	2/3 attach to the your management interface
Storage role	2/3 attach to the storage controller

Table 26. Ethernet switch error code categories

• 0x000-0x00F: Common errors
• 0x010-0x01F: EthSwFw errors
• 0x020-0x07F: EthSwConfig errors
• 0x080-0x0FF: EthSwHw errors
• 0x100-0x7FF: Reserved
• 0x800-0xFFF: EthSwLink errors

Originating specific hardware and software codes

The alphanumeric symbol in the C position represents the originating specific hardware and software code.

- For the originating file module and file module specific hardware code (code 0, 2, 4), go to Table 27.
- For the originating file module specific software code (code 1, 3, 5), go to Table 28 on page 74.
- For the storage enclosure hardware code (code 6), go to Table 29 on page 74.
- For the Ethernet switches (code 8): The Ethernet switches are a single field replaceable unit (FRU) and have no unique failing hardware code. The Ethernet switches use 0 for the originating specific hardware or software code.

Table 27. Originating file module and file module specific hardware code – Code 0, 2, 4

C = Originating specific hardware code in sequence ABBC-DDDD	
Code	Device
0	System x hardware (CPU, memory, powers supplies, etc.)
1	Built-in Ethernet port 0
2	Built-in Ethernet port 1
3	Built-in Ethernet port 2
4	Built-in Ethernet port 3
5	Optional Ethernet port 4 (For Quad port 1G card or Dual Port 10G card)
6	Optional Ethernet port 5 (For Quad port 1G card or Dual Port 10G card)
7	Optional Ethernet port 6 (For Quad port 1G card or Dual Port 10G card)
8	Optional Ethernet port 7 (For Quad port 1G card or Dual Port 10G card)
B	Fibre channel adapter 1 (both ports) – Storage node only

Table 27. Originating file module and file module specific hardware code – Code 0, 2, 4 (continued)

C = Originating specific hardware code in sequence ABBC-DDDD	
Code	Device
C	Fibre channel adapter 2 (both ports) – Storage node only
D	Bonded device (data0 mgmt0)
E	System x internal hard disk drives

Table 28. Originating file module specific software code – Code 1, 3, 5

C = Originating specific software code in sequence ABBC-DDDD	
Code	Device
0	Red Hat Linux
1	GPFS
2	CIFS server
3	CTDB
4	SoFS
5	winbind
6	multipathd
7	nscd
8	sshd
9	httpd
A	vsftpd
B	nmbd
C	nfsd
D	cpu
E	multipath/disk

Table 29. Storage enclosure hardware code – Code 6

C = Originating specific software code in sequence ABBC-DDDD	
Code	Device
0	Generic value for storage enclosure hardware
1	Disk drive in controller drawer
2	RAID controller card 0
3	RAID controller card 1
4	Power supply in controller drawer
5	RAID array/LUN issue in controller drawer
6	Disk drive in expansion drawer
7	Expansion fibre channel card 0
8	Expansion fibre channel card 1
9	Power supply in expansion drawer
A	RAID array/LUN issue in expansion drawer

Ethernet switches – Code 8

Severity of the error

The element *x* indicates the severity of the error. The value *x* can be:

- **A for Action:** GUI error messages. The user must perform a specific action.
- **C for Critical:** A critical error occurred which must be corrected by the user or system administrator.
- **D for Debug:** Used only for debug purposes.
- **I for Informational:** No operation action required.
- **W for Warning:** An error occurred that should be investigated and fixed.

Error code examples

These two error code examples illustrate how to interpret the alphanumeric elements based on the information provided above.

Example 1

Source: Network problems between the third file module and the management node.

Error code and message:

210000*x* – The Ethernet port0 has failed and is unresponsive.

210001*x* – A network failure was detected between Ethernet port 0 (mgmt0sl0) and the management node. Link down.

210002*x* – A network degradation was detected between Ethernet port 0 (mgmt0sl0) and the management node. There are high packet losses occurring.

210003*x* – A network degradation was detected between Ethernet port 0 (mgmt0sl0) and the management node. High collisions detected.

The following table shows the break down of the error code's alphanumeric elements:

Table 30. Error code break down

ACDXXXx	
210nnnx	
2	File Module
1	Built in Ethernet port 0
0	Originated with Denali checking
nnn	Unique error code
x	Severity of the error

Example 2

Source: A disk drive problem in the fourth storage pod, second expansion drawer.

Error code and message:

662000x – The disk drive located in position 23 has failed.

The following table shows the break down of the error code's alphanumeric elements:

Table 31. Error code break down

ACDXXXx 662000x	
6	Storage enclosure
6	Indicates a failure in the storage expansion drawer
2	Originated with system checkout
000	Unique error code
x	Severity of the error

Understanding event IDs

The Storwize V7000 Unified messages follow a specific format, which is detailed here.

Tip: Search for most error code or event IDs by using just the ID. For an ID of 66012FC, for example, just search on 66012FC. If you get an error code similar to "01E0", use wildcards and search on *01E0*. With 66012FC, you could use wildcards and search on 66012* or, if you seek a much broader range of results, an ID shortened to 66*. For IDs such as EFSSP1002C, do not search on the entire string, but remove the "EFS" and search on "SP1002C" or, again, use wildcards and search on a value such as *1002*.

The format of system messages is *cnmmnx*. The elements—*cnmmnx*—represent the following information:

- The element *c* is an alphabetic identifier assigned to a component. The message component identifiers are assigned as follows:
 - A** for Common or Access Layer
 - B** for Space
 - C** for GPFS
 - D** for Wizards
 - F** for Statistics
 - G** for CLI
 - H** for Health Center
 - I** for Asynchronous Replication
 - J** for SCM
 - L** for HSM
 - AK** for NDMP
- The element *mmmm* is a 4 digit message number
- The element *x* indicates the severity of the error. The value *x* can be:
 - A for Action:** GUI error messages. The user must perform a specific action.
 - C for Critical:** A critical error occurred which must be corrected by the user or system administrator.
 - D for Debug:** Used only for debug purposes.
 - I for Informational:** No operation action required.

W for Warning: An error occurred that can cause problems in the future. The problem should be investigated and fixed.

File module hardware problems

This section helps you to identify and resolve file module hardware problems.

Removing and replacing parts

Illustrations in this section might differ slightly from the actual hardware.

Table 32. Components identified as customer replaceable units (CRUs) and field replaceable units (FRUs)

Types of replaceable parts	Explanation of each type of replaceable part	Procedures categorized under each type of replaceable part
Tier 1 Customer replaceable units (CRUs)	Tier 1 CRUs are your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these.	"Removing the cover" on page 79 "Installing the cover" on page 80 "Removing the battery" on page 81 "Installing the battery" on page 85 "Removing the microprocessor 2 air baffle" on page 86 "Installing the microprocessor 2 air baffle" on page 87 "Removing the DIMM air baffle" on page 89 "Installing the DIMM air baffle" on page 90 "Removing the fan bracket" on page 91 "Installing the fan bracket" on page 92 "Removing the IBM virtual media key" on page 93 "Installing the IBM virtual media key" on page 94 "Removing a PCI riser-card assembly" on page 95 "Installing a PCI riser-card assembly" on page 96

Table 32. Components identified as customer replaceable units (CRUs) and field replaceable units (FRUs) (continued)

Types of replaceable parts	Explanation of each type of replaceable part	Procedures categorized under each type of replaceable part
Tier 1 Customer replaceable units (CRUs) (continued)	Tier 1 CRUs are your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these.	<p>“Removing a PCI adapter from a PCI riser-card assembly” on page 98</p> <p>“Installing a PCI adapter in a PCI riser-card assembly” on page 99</p> <p>“Removing the two-port Ethernet adapter” on page 102</p> <p>“Removing a Fibre Channel PCI adapter” on page 100</p> <p>“Installing a Fibre Channel PCI adapter” on page 101</p> <p>“Removing a 10-Gbps Ethernet PCI adapter” on page 101</p> <p>“Installing a 10-Gbps Ethernet PCI adapter” on page 102</p> <p>“Installing the two-port Ethernet adapter” on page 103</p> <p>“Storing the full-length-adapter bracket” on page 106</p> <p>“Removing the SAS riser-card and controller assembly” on page 107</p> <p>“Installing the SAS riser card and controller assembly” on page 109</p> <p>“Removing the ServeRAID SAS controller from the SAS riser-card” on page 113</p> <p>“Installing a ServeRAID SAS controller in the SAS riser-card” on page 114</p> <p>“Removing a hot-swap hard disk drive” on page 115</p> <p>“Installing a hot-swap hard disk drive” on page 116</p> <p>“Removing an optional ServeRAID adapter advanced feature key” on page 117</p> <p>“Installing an optional ServeRAID adapter advanced feature key” on page 118</p> <p>“Removing the serveRAID SAS controller battery from the remote battery tray” on page 120</p> <p>“Installing the serveRAID SAS controller battery on the remote battery tray” on page 122</p>
Tier 1 Customer replaceable units (CRUs) (continued)	Tier 1 CRUs are your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these.	<p>“Removing a CD-RW/DVD drive” on page 123</p> <p>“Installing the CD-RW/DVD drive” on page 125</p> <p>“Removing a memory module” on page 126</p> <p>“Installing a memory module” on page 126</p> <p>“Removing a hot-swap fan” on page 129</p> <p>“Installing a hot-swap fan” on page 130</p> <p>“Removing a hot-swap ac power supply” on page 131</p> <p>“Installing a hot-swap ac power supply” on page 132</p> <p>“Removing the operator information panel assembly” on page 135</p> <p>“Installing the operator information panel assembly” on page 136</p>

Table 32. Components identified as customer replaceable units (CRUs) and field replaceable units (FRUs) (continued)

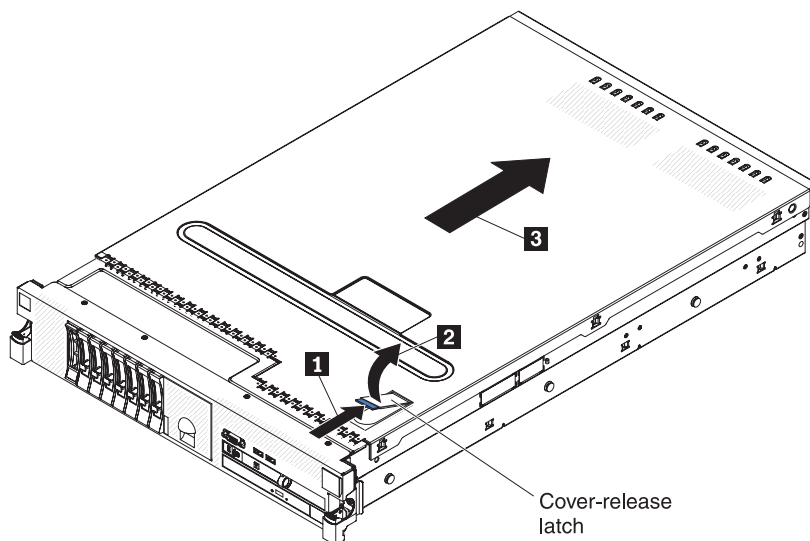
Types of replaceable parts	Explanation of each type of replaceable part	Procedures categorized under each type of replaceable part
Field replaceable units (FRUs)	FRUs must be installed only by trained service technicians.	<ul style="list-style-type: none"> “Removing a microprocessor and heat sink” on page 136 “Installing a microprocessor and heat sink” on page 138 “Thermal grease” on page 143 “Removing a heat-sink retention module” on page 143 “Installing a heat-sink retention module” on page 144 “Removing the system board” on page 145 “Installing the system board” on page 147 “Removing the 240 VA safety cover” on page 149 “Installing the 240 VA safety cover” on page 150 “Setting the machine type, model, and serial number” on page 151

Removing the cover

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove the cover, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.

2. If you are planning to view the error LEDs that are on the system board and components, leave the file module connected to power and go directly to step 4.
3. If you are planning to install or remove a microprocessor, memory module, PCI adapter, battery, or other non-hot-swap optional device, turn off the file module and all attached devices and disconnect all external cables and power cords.
4. Press down on the left and right side latches and pull the file module out of the rack enclosure until both slide rails lock.

Note: You can reach the cables on the back of the file module when the file module is in the locked position.

5. Push the cover-release latch back **1**, then lift it up **2**.
6. Slide the cover back **3**, then lift the cover off the file module and set it aside.

Attention: For proper cooling and airflow, replace the cover before turning on the file module. Operating the file module for extended periods of time (over 30 minutes) with the cover removed might damage file module components.

7. If you are instructed to return the cover, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

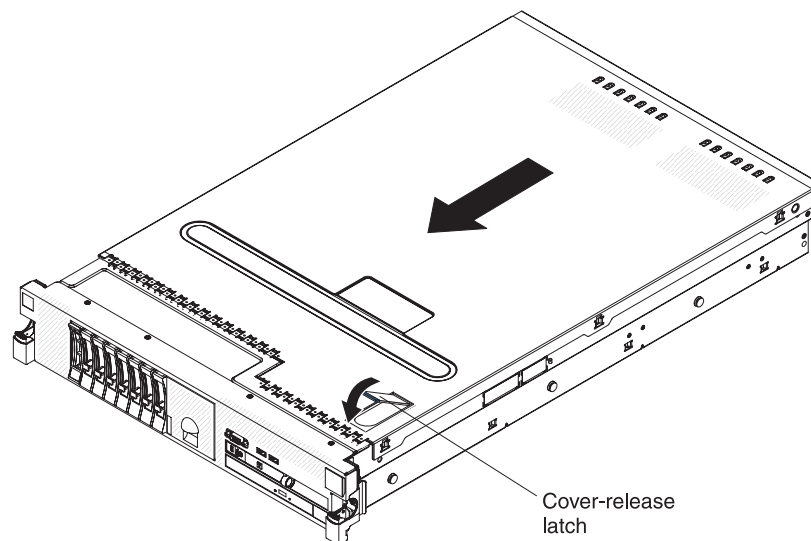
Installing the cover

The following procedure is for a Tier 1 customer replaceable unit (CRU).

Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the cover, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Make sure that all internal cables are correctly routed.
3. Place the cover-release latch in the open (up) position.

4. Insert the bottom tabs of the top cover into the matching slots in the file module chassis.
5. Press down on the cover-release latch to lock the cover in place.
6. Slide the file module into the rack.

Removing the battery

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

The following notes describe information that you must consider when replacing the battery:

- IBM has designed this product with your safety in mind. The lithium battery must be handled correctly to avoid possible danger. If you replace the battery, you must adhere to the following instructions.

Note: In the U. S., call 1-800-IBM-4333 for information about battery disposal.

- If you replace the original lithium battery with a heavy-metal battery or a battery with heavy-metal components, be aware of the following environmental consideration. Batteries and accumulators that contain heavy metals must not be disposed of with normal domestic waste. They will be taken back free of charge by the manufacturer, distributor, or representative, to be recycled or disposed of in a proper manner.
- To order replacement batteries, call 1-800-IBM-SERV within the United States, and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

Note: After you replace the battery, you must reconfigure the file module and reset the system date and time.

Statement 2



CAUTION:

When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

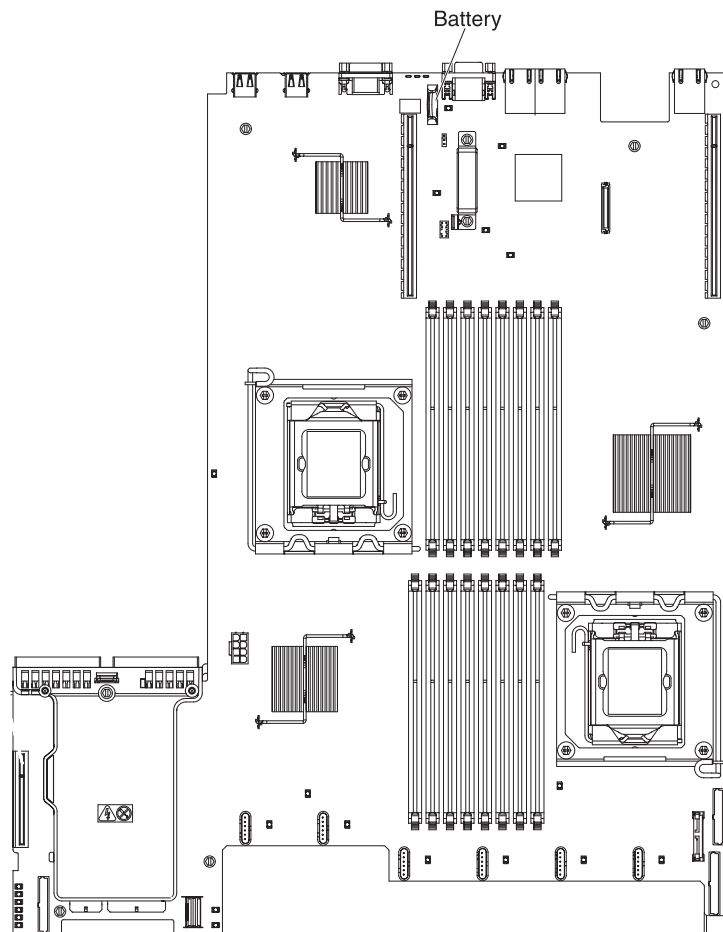
Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

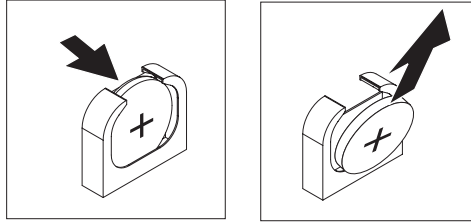
Dispose of the battery as required by local ordinances or regulations.

To remove the battery, complete the following procedure.

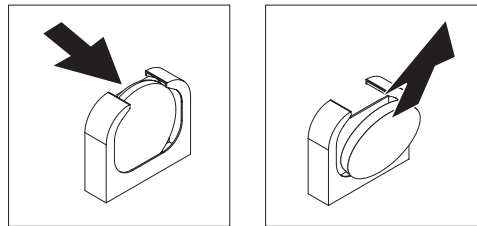
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Follow any special handling and installation instructions that come with the battery.
3. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
4. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
5. Remove the cover, as described in “Removing the cover” on page 79.
6. Disconnect any internal cables, as necessary, making note of the cable routing for later reinstallation.
7. Remove any adapters as necessary.
8. Locate the battery on the system board.



9. Remove the battery:
 - a. If there is a rubber cover on the battery holder, use your fingers to lift the battery cover from the battery connector.
 - b. Use one finger to push the battery horizontally away from the PCI riser card in slot 2 and out of its housing.



c. Lift the battery from the socket.

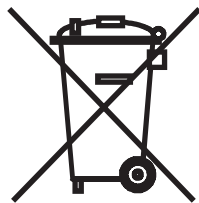


10. Dispose of the battery as required by local ordinances or regulations, as described in "Battery return program."

Battery return program: This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to www.ibm.com/ibm/environment/products/index.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

The following applies for countries within the European Union:



For Taiwan:



Please recycle batteries.

廢電池請回收

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

Spain

This notice is provided in accordance with Royal Decree 106/2008 of Spain: The retail price of batteries, accumulators and power cells includes the cost of the environmental management of their waste.

Perchlorate Material - California

Special handling may apply. See <http://www.dtsc.ca.gov/hazardouswaste/perchlorate> for more information.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product, part or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Installing the battery

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

The following notes describe information to consider when replacing the battery in the file module.

- You must replace the battery with a lithium battery of the same type from the same manufacturer.
- After you replace the battery, you must reconfigure the file module and reset the system date and time.
- To avoid possible danger, read and follow the following safety statement.
- To order replacement batteries, call 1-800-IBM-SERV within the United States, and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your support center or business partner.

Statement 2



CAUTION:

When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

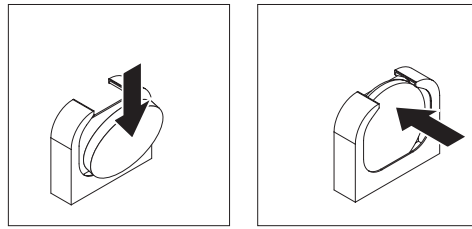
- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

See “Battery return program” on page 83 for more information. Dispose of the battery as required by local ordinances or regulations.

To install the replacement battery, complete the following steps:

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Follow any special handling and installation instructions that come with the replacement battery.
3. Insert the new battery:
 - a. Tilt the battery so that you can insert it into the socket on the side opposite the battery clip.



- b. Press the battery down into the socket until it clicks into place. Make sure that the battery clip holds the battery securely.
 - c. If you removed a rubber cover from the battery holder, use your fingers to install the battery cover on top of the battery connector.
4. Reinstall any adapters you removed in other procedures.
 5. Reconnect any internal cables that you disconnected.

Attention:

- When you route cables, do not block any connectors or the ventilated space around any of the fans.
 - Make sure that cables are not routed on top of components under the PCI riser-card assemblies.
 - Make sure that cables are not pinched by server components.
6. Install the cover, as described in “Installing the cover” on page 80.
 7. Slide the file module into the rack.
 8. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

9. Start the Setup utility and reset the configuration.
 - Set the system date and time.
 - Set the power-on password.
 - Reconfigure the file module.

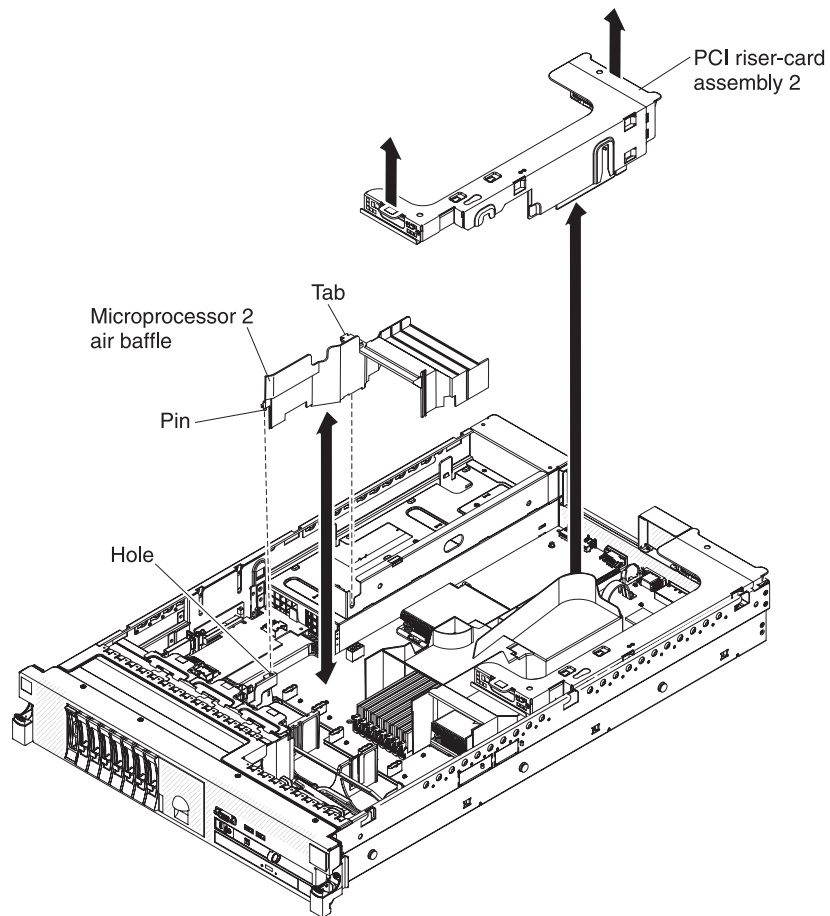
Removing the microprocessor 2 air baffle

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

When you work with some optional devices, you must first remove the microprocessor 2 air baffle to access certain components on the system board.

To remove the microprocessor 2 air baffle, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Remove PCI riser-card assembly 2, as described in “Removing a PCI riser-card assembly” on page 95.
6. Grasp the top of the air baffle and lift the air baffle out of the file module.

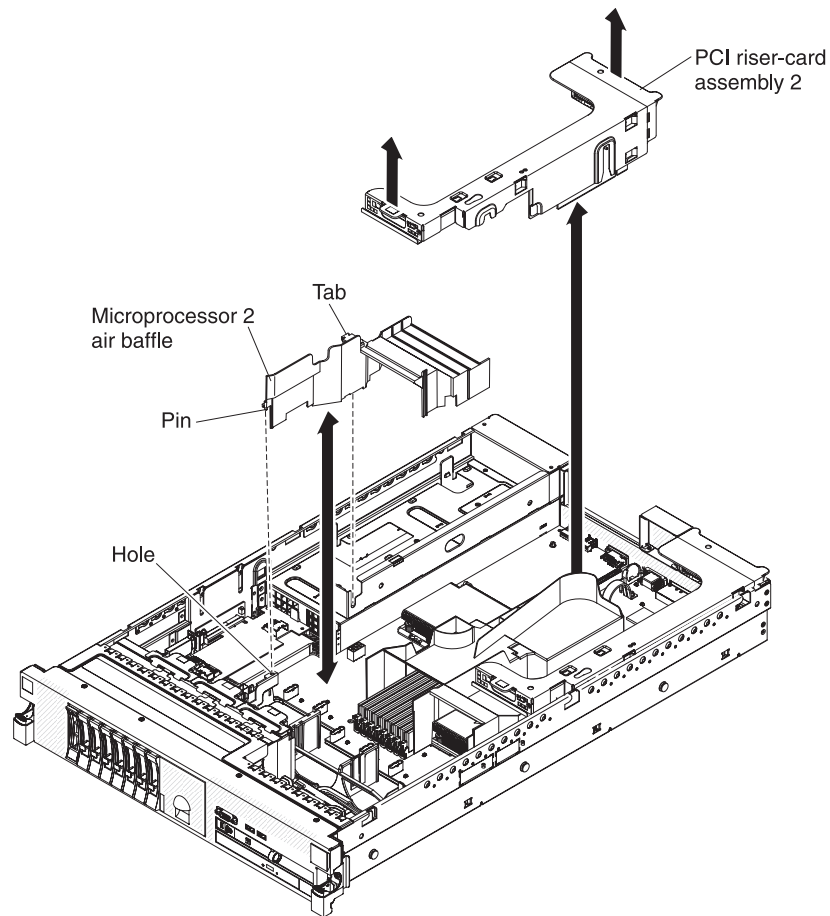
Attention: For proper cooling and airflow, replace all air baffles before you turn on the file module. Operating the file module with any air baffle removed might damage file module components.
7. If you are instructed to return the microprocessor air baffle, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the microprocessor 2 air baffle

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the microprocessor air baffle, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Align the tab on the left side of the microprocessor 2 air baffle with the slot in the right side of the power-supply cage.
3. Align the pin on the bottom of the microprocessor air baffle with the hole on the system board retention bracket.
4. Lower the microprocessor 2 air baffle into the file module.
Attention: For proper cooling and airflow, replace all air baffles before you turn on the file module. Operating the file module with any air baffle removed might damage file module components.
5. Install PCI riser-card assembly 2, if necessary.
6. Install the cover, as described in “Installing the cover” on page 80.
7. Slide the file module into the rack.
8. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

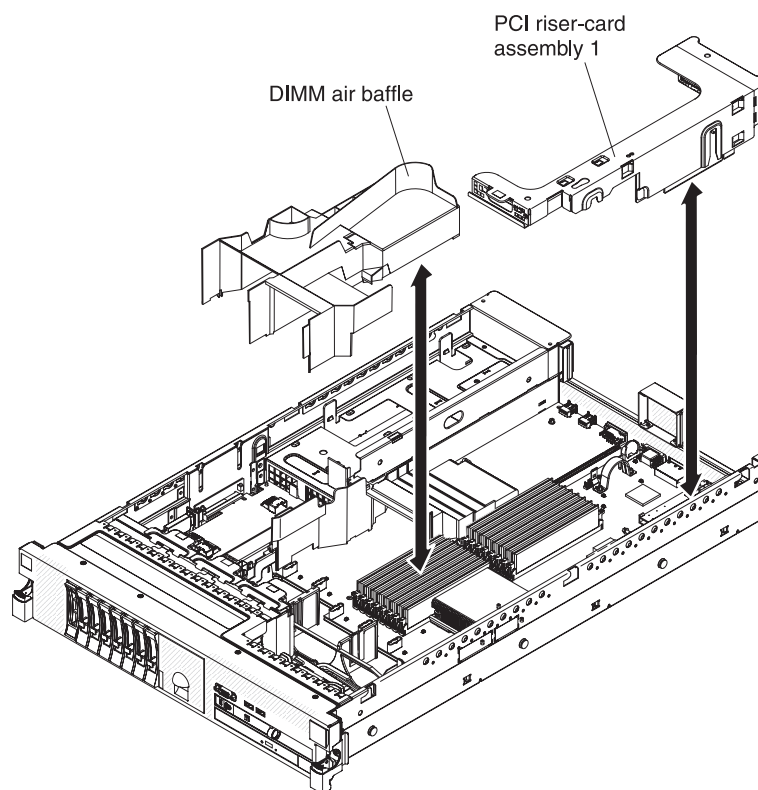
Removing the DIMM air baffle

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

When you work with some optional devices, you must first remove the DIMM air baffle to access certain components or connectors on the system board.

To remove the DIMM air baffle, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Remove riser-card assembly 1, as described in “Removing a PCI riser-card assembly” on page 95.

6. Place your fingers under the front and back of the top of the air baffle; then, lift the air baffle out of the server.

Note: If two microprocessors are installed, you must remove PCI riser card assembly 2 and microprocessor 2 air baffle first, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the microprocessor 2 air baffle” on page 86.

Attention: For proper cooling and airflow, replace all the air baffles before you turn on the server. Operating the server with any air baffle removed might damage server components.

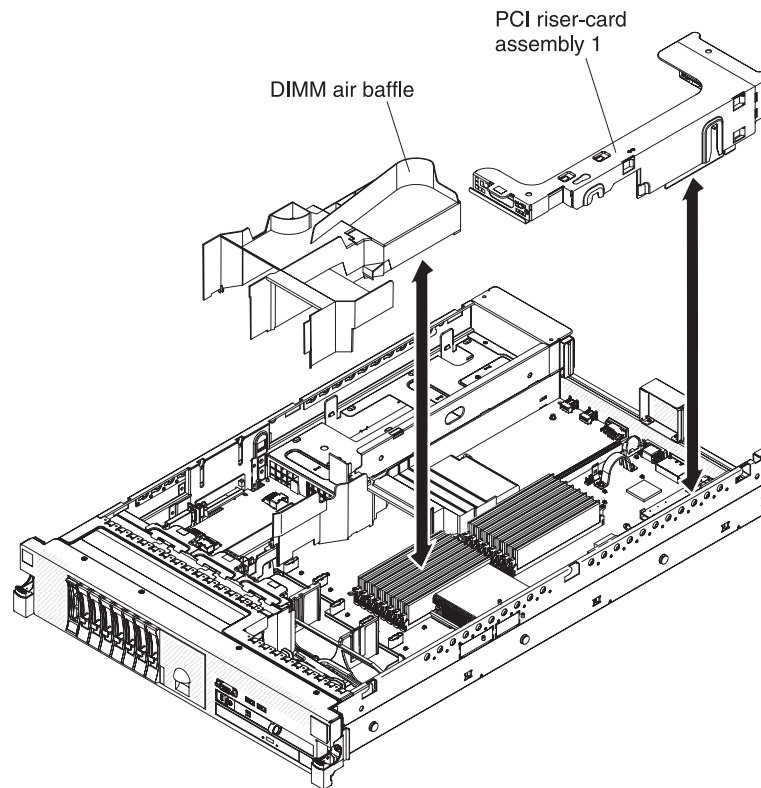
7. If you are instructed to return the DIMM air baffle, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the DIMM air baffle

The following procedure is for a Tier 1 customer replaceable unit (CRU).

Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

To install the DIMM air baffle, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Align the DIMM air baffle with the DIMMs and the back of the fans.
3. Lower the air baffle into place.
4. If necessary, replace PCI riser-card assembly 1, as described in “Installing a PCI riser-card assembly” on page 96.

5. Install the cover, as described in “Installing the cover” on page 80.
6. Slide the file module into the rack.
7. Reconnect the external cables; then, reconnect the power cords and turn on the file module.

Note: You must wait approximately 20 seconds after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Attention: For proper cooling and airflow, replace all air baffles before you turn on the server. Operating the server with any air baffle removed might damage server components.

Removing the fan bracket

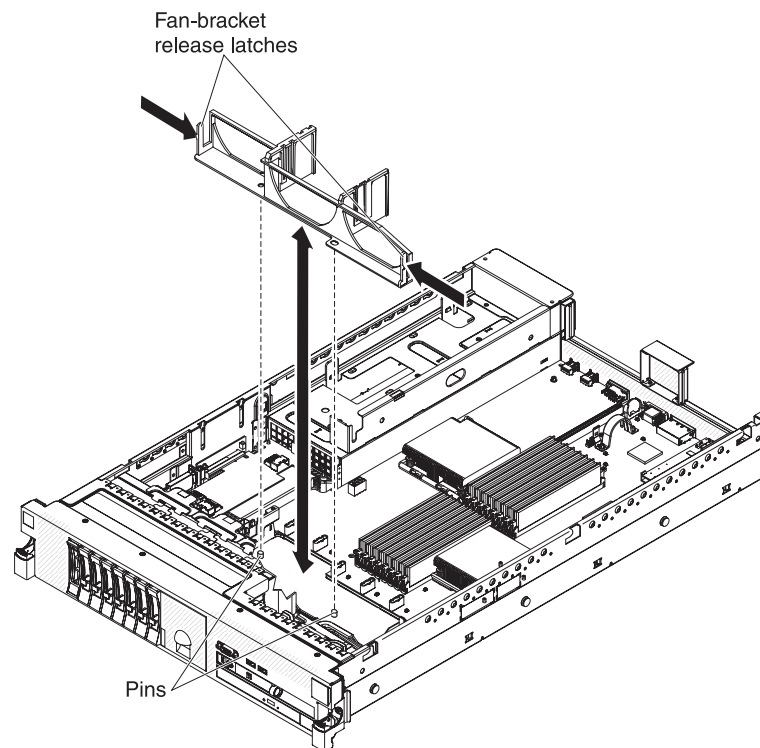
The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To replace some components or to create working room, you might have to remove the fan-bracket assembly.

Note: To remove or install a fan, it is not necessary to remove the fan bracket. See “Removing a hot-swap fan” on page 129 and “Installing a hot-swap fan” on page 130.

To remove the fan bracket, complete the following steps.



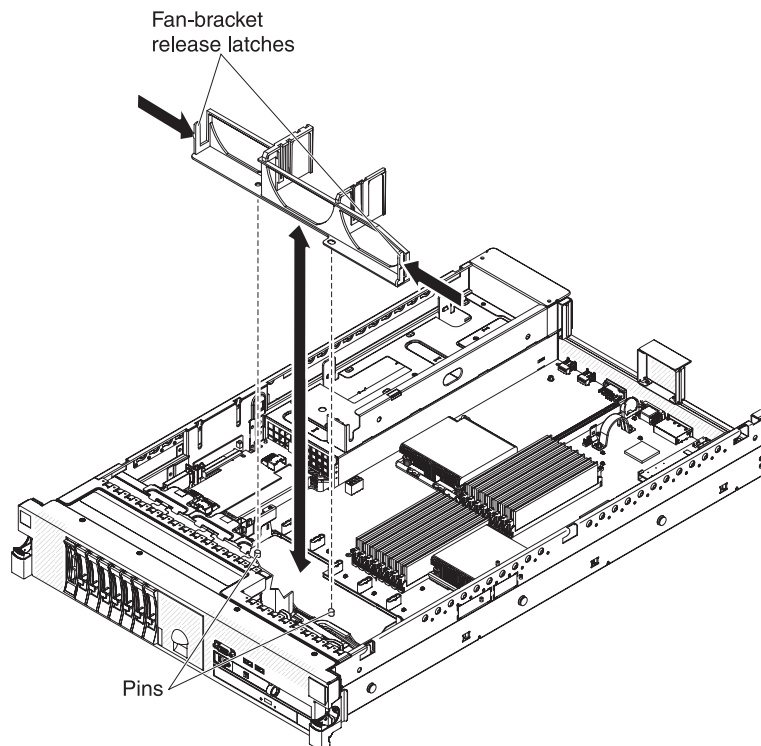
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Remove the fans, as described in “Removing a hot-swap fan” on page 129.
6. Remove the PCI riser card assemblies, as described in “Removing a PCI riser-card assembly” on page 95.
7. Remove the DIMM air baffle, as described in “Removing the DIMM air baffle” on page 89.
8. Press the fan-bracket release latches toward each other and lift the fan bracket out of the server.

Installing the fan bracket

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the fan bracket, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.

2. Lower the fan bracket into the chassis.
3. Align the holes in the bottom of the bracket with the pins in the bottom of the chassis.
4. Press the bracket into position until the fan-bracket release levers click into place.
5. Replace the fans, as described in “Installing a hot-swap fan” on page 130.
6. Replace the PCI riser card assemblies, as described in “Installing a PCI riser-card assembly” on page 96.
7. Replace the DIMM air baffle, as described in “Installing the DIMM air baffle” on page 90.
8. Install the cover, as described in “Installing the cover” on page 80.
9. Slide the file module into the rack.
10. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

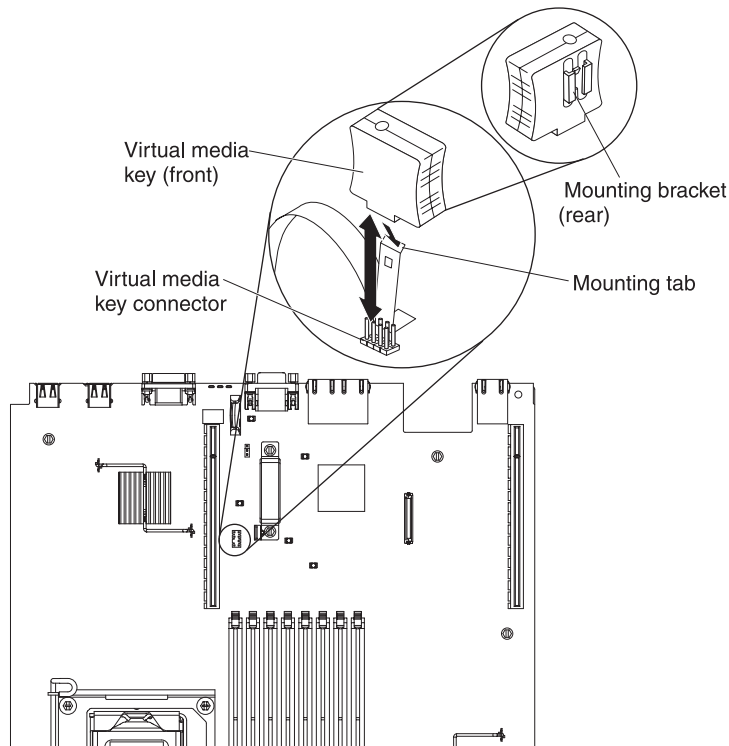
Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Removing the IBM virtual media key

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove a virtual media key, complete the following procedure.



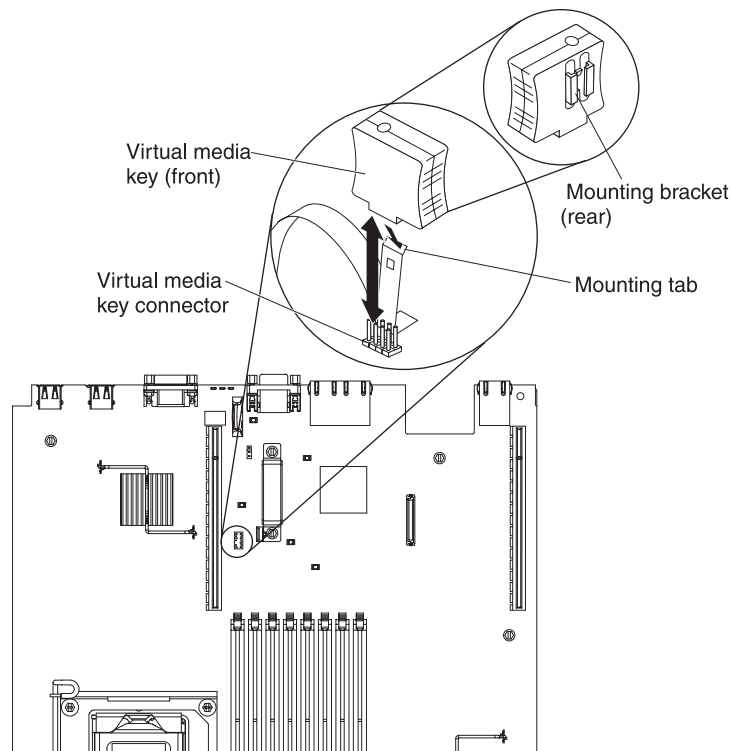
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Locate the virtual media key on the system board. Grasp it and carefully pull it off the virtual media connector pins.

Installing the IBM virtual media key

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install a virtual media key, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Align the virtual media key with the virtual media pins on the system board as shown in the illustration.
3. Insert the virtual media key onto the pins until it clicks into place.
4. Install the cover, as described in “Installing the cover” on page 80.
5. Slide the file module into the rack.

6. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

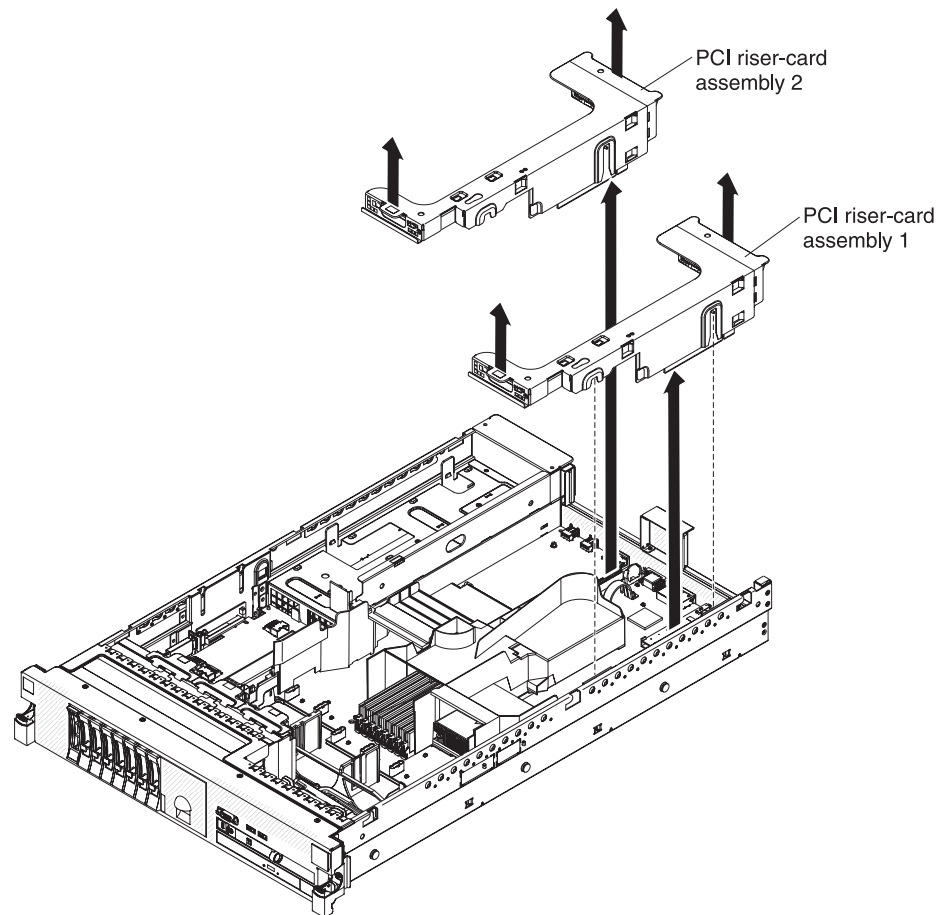
Removing a PCI riser-card assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

Each file module uses PCI riser cards differently.

To remove a riser-card assembly, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.

3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Grasp the riser-card assembly at the front tab and rear edge and lift it to remove it from the file module. Place the riser-card assembly on a flat, static-protective surface.

Installing a PCI riser-card assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU).

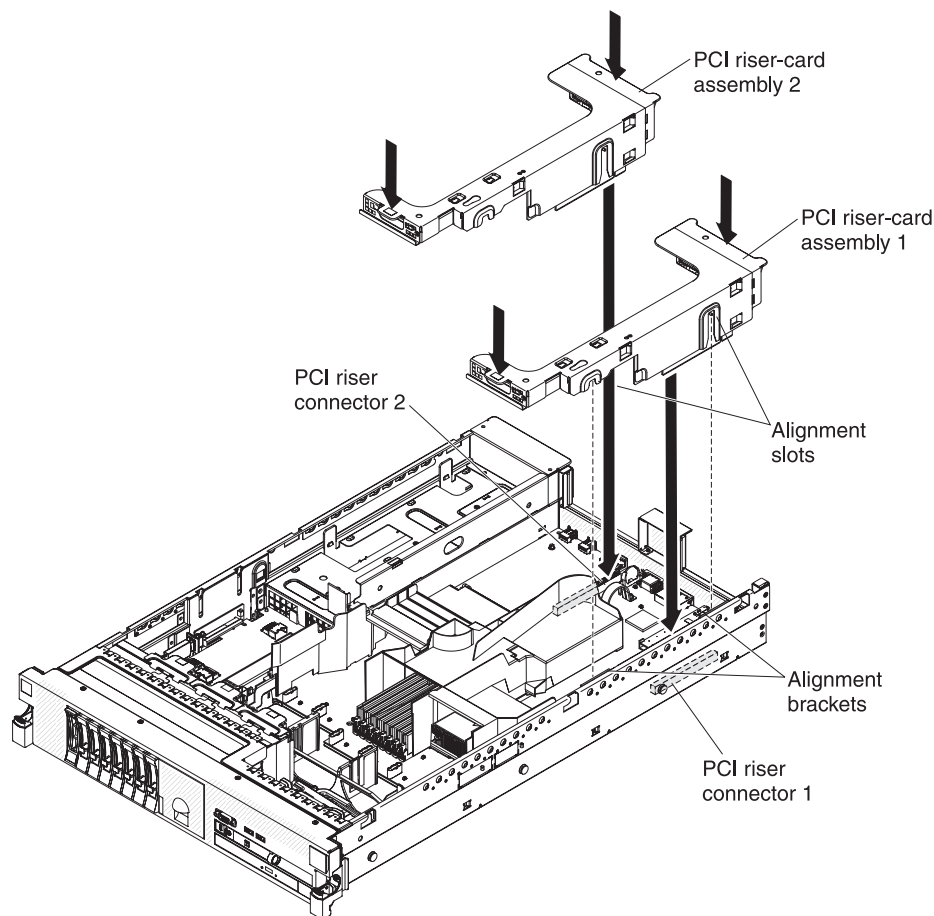
Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Ensure that you read and understand the following information:

- Standard models of the Storwize V7000 Unified come with one PCI riser-card assembly installed. If you want to replace them with PCI-X riser-card assemblies, you must order the PCI-X riser-card assembly option, which includes the bracket.
- A PCI riser-card assembly has a black connector and supports PCI adapters, and a PCI-X riser-card assembly has a white (light in color) connector and supports PCI-X adapters.
- PCI riser slot 1 is the farthest slot from the power supplies. This slot supports only low-profile adapters.
- PCI riser slot 2 is the closest slot to the power supplies. You must install a PCI riser-card assembly in slot 2 even if you do not install an adapter.
- Microprocessor 2, aux power, and PCI riser-card assembly 2 share the same power channel that is limited to 230 W.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install a riser-card assembly, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Reinstall any adapters you removed in other procedures.
3. Reconnect any internal cables that you disconnected.

Attention:

- When you route cables, do not block any connectors or the ventilated space around any of the fans.
 - Make sure that cables are not routed on top of components under the PCI riser-card assemblies.
 - Make sure that cables are not pinched by server components.
4. Align the PCI riser-card assembly with the selected PCI connector on the system board:

Note: The chassis might sag after removing the riser assembly. In this case, lift up the bottom of the chassis to line up the slots on the side of the assembly to the alignment brackets in the side of the chassis.

- **PCI connector 1:** Carefully fit the two alignment slots on the side of the assembly onto the two alignment brackets in the side of the chassis.
 - **PCI connector 2:** Carefully align the bottom edge (the contact edge) of the riser-card assembly with the riser-card connector on the system board.
5. Install the cover, as described in “Installing the cover” on page 80.
 6. Slide the file module into the rack.

7. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

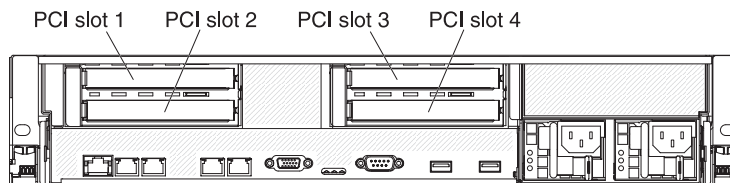
Removing a PCI adapter from a PCI riser-card assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

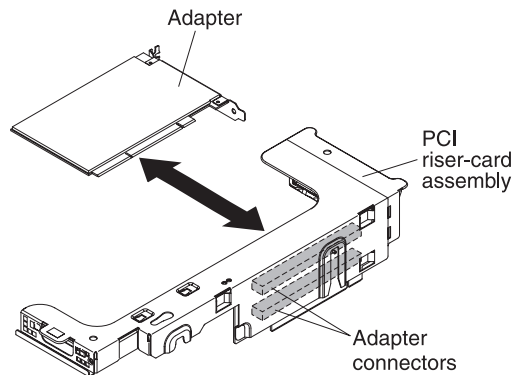
Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

Use this procedure to remove an adapter from a PCI expansion slot in a PCI riser-card assembly. To remove the ServeRAID SAS controller from the SAS riser-card, see “Removing the ServeRAID SAS controller from the SAS riser-card” on page 113.

The following illustration shows the locations of the adapter expansion slots from the rear of the file module.



To remove an adapter from a PCI expansion slot, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.

5. Remove the PCI riser-card assembly that contains the adapter, as described in “Removing a PCI riser-card assembly” on page 95.
 - If you are removing an adapter from PCI expansion slot 1 or 2, remove PCI riser-card assembly 1.
 - If you are removing an adapter from PCI expansion slot 3 or 4, remove PCI riser-card assembly 2.
6. Disconnect any internal cables, as necessary, making note of the cable routing for later reinstallation.
7. Carefully grasp the adapter by its top edge or upper corners, and pull the adapter from the PCI expansion slot.
8. If the adapter is a full-length adapter in the upper expansion slot of the PCI riser-card assembly and you do not intend to replace it with another full-length adapter, remove the full-length-adapter bracket and store it on the underside of the top of the PCI riser-card assembly.
9. If you are instructed to return the adapter, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

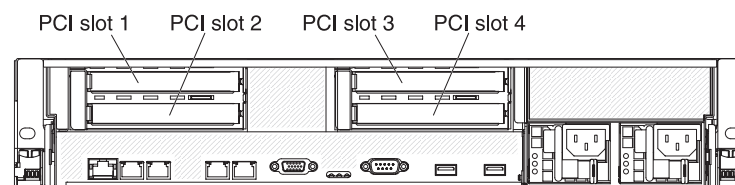
Installing a PCI adapter in a PCI riser-card assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

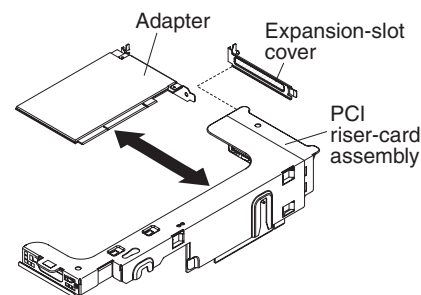
Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

Use this procedure to install an adapter in a PCI expansion slot in a PCI riser-card assembly. To install a ServeRAID SAS controller, go to “Installing a ServeRAID SAS controller in the SAS riser-card” on page 114.

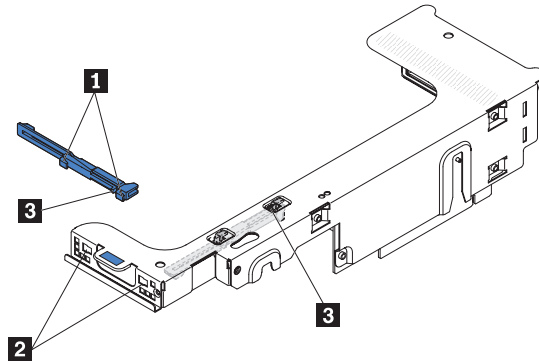
The following illustration shows the locations of the adapter expansion slots from the rear of the server.



To install an adapter, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Install the adapter in the expansion slot.
3. If the adapter is a full-length adapter for the upper expansion slot (1 or 3) in the riser card, remove the full-length-adapter bracket **1** from beneath the top of the riser-card assembly **3** and insert it in the end of the upper expansion slot **2** of the riser-card assembly.



- a. Align the adapter with the PCI connector on the riser-card, and the guide on the external end of the riser-card assembly.
 - b. Press the adapter firmly into the PCI connector on the riser card.
4. Reconnect any internal cables that you disconnected.

Attention:

- When you route cables, do not block any connectors or the ventilated space around any of the fans.
 - Make sure that cables are not routed on top of components under the PCI riser-card assemblies.
 - Make sure that cables are not pinched by server components.
5. Align the PCI riser-card assembly with the selected PCI connector on the system board.
 - **PCI-riser connector 1:** Carefully fit the two alignment slots on the side of the assembly onto the two alignment brackets on the side of the chassis; align the rear of the assembly with the guides on the rear of the server.
 - **PCI-riser connector 2:** Carefully align the bottom edge (the contact edge) of the riser-card assembly with the riser-card connector on the system board; align the rear of the assembly with the guides on the rear of the server.
 6. Perform any configuration tasks that are required for the adapter.
 7. Install the cover, as described in “Installing the cover” on page 80.
 8. Slide the file module into the rack.
 9. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

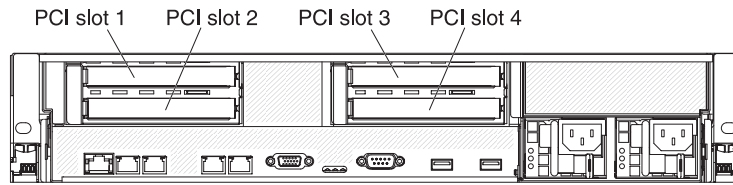
Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Removing a Fibre Channel PCI adapter

These removal instructions show the slot location for the Fibre Channel PCI adapter.

The Fibre Channel adapter is in PCI slot 2.

The following illustration shows the locations of the adapter expansion slots from the rear of the file module.



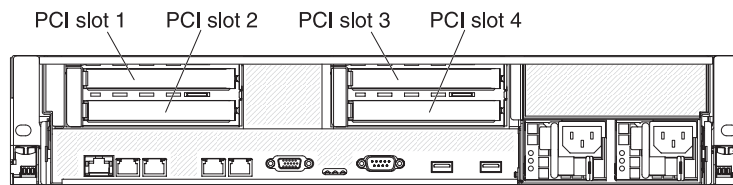
Refer to “Removing a PCI adapter from a PCI riser-card assembly” on page 98 for instructions.

Installing a Fibre Channel PCI adapter

These installation instructions show the slot location for the Fibre Channel PCI adapter.

The Fibre Channel adapter must go in PCI slot 2.

The following illustration shows the locations of the adapter expansion slots from the rear of the file module.



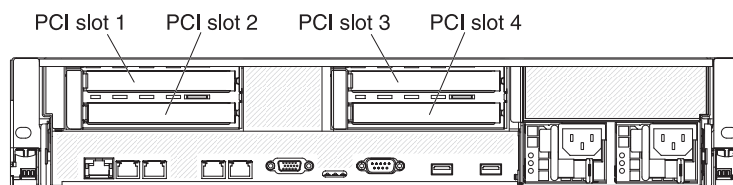
Refer to “Installing a PCI adapter in a PCI riser-card assembly” on page 99 for instructions.

Removing a 10-Gbps Ethernet PCI adapter

These instructions show the slot location for the 10-Gbps Ethernet PCI adapter.

The 10-Gbps Ethernet adapter is in PCI slot 4.

The following illustration shows the locations of the adapter expansion slots from the rear of the file module.



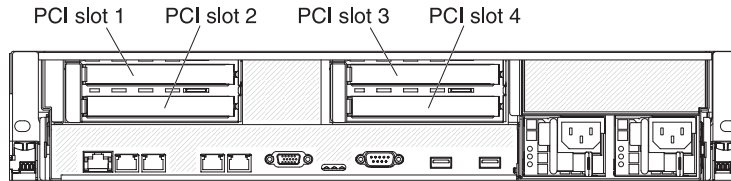
Refer to “Removing a PCI adapter from a PCI riser-card assembly” on page 98 for instructions.

Installing a 10-Gbps Ethernet PCI adapter

These installation instructions show the slot location for the 10-Gbps Ethernet PCI adapter.

The 10-Gbps Ethernet adapter must go in PCI slot 4.

The following illustration shows the locations of the adapter expansion slots from the rear of the file module.



Refer to “Installing a PCI adapter in a PCI riser-card assembly” on page 99 for instructions.

Removing the two-port Ethernet adapter

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove the two-port Ethernet adapter, complete the following procedure.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Remove the PCI riser-card assembly as described in “Removing a PCI riser-card assembly” on page 95.
6. Grasp the Ethernet adapter and disengage it from the standoffs and the connector on the system board; then, slide the Ethernet adapter out of the port openings on the rear of the chassis and remove it from the server. See Figure 13 on page 103.

Note: You may need to squeeze the springs on the head of the stand off with a pair of pliers, for example, at the same time as lifting up on the adapter from a point near the same stand-off.

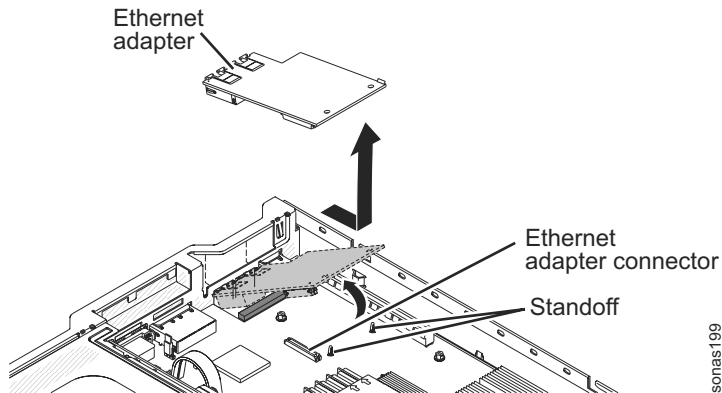


Figure 13. Removing the Ethernet adapter

7. If you are instructed to return the Ethernet adapter, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the two-port Ethernet adapter

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the two-port Ethernet adapter, complete the following procedure.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Remove the cover. See “Removing the cover” on page 79.
4. Attach the rubber stopper on the chassis, along the edge of the system board, as shown in the following illustration.

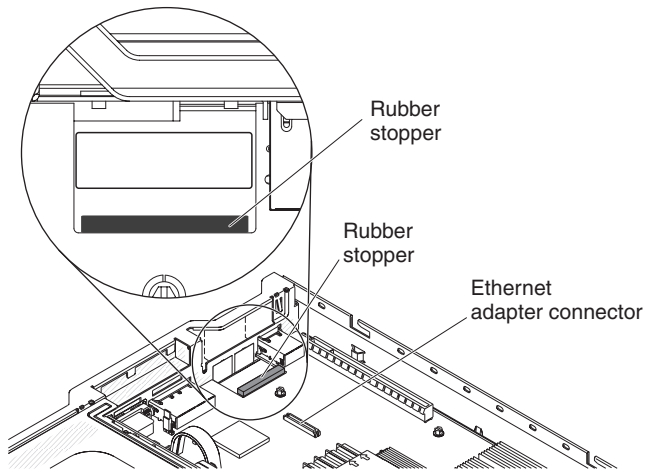


Figure 14. Location of the rubber stopper on the chassis

5. Remove the Ethernet adapter filler panel on the rear of the chassis (if it has not been removed already). See Figure 15.

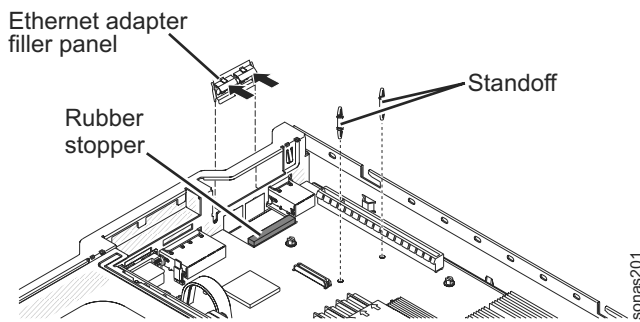


Figure 15. Location of the Ethernet adapter filler panel on the chassis

6. Install the two standoffs on the system board.
7. Insert the bottom tabs of the metal clip into the port openings from outside the chassis. See Figure 16 on page 105.

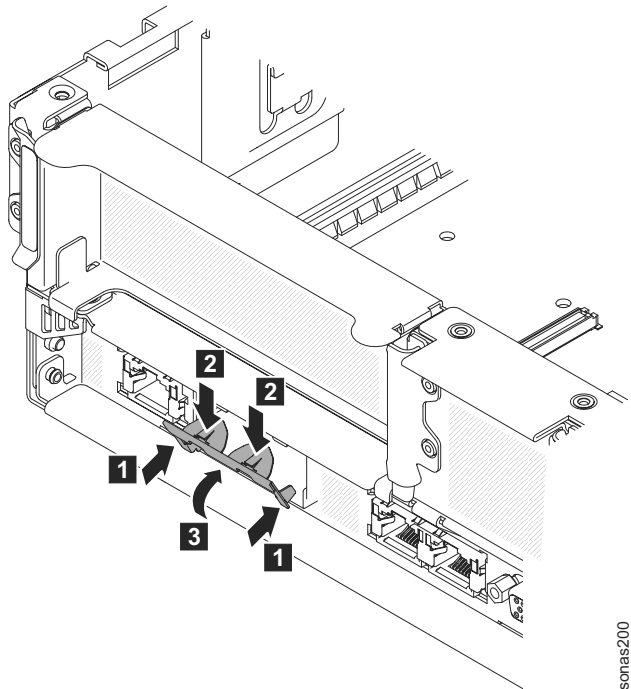


Figure 16. Location of the port openings on the chassis

8. While you slightly press the top of the metal clip, rotate the metal clip toward the front of the server until the metal clip clicks into place. Make sure the metal clip is securely engaged on the chassis.

Attention: Pressing the top of the metal clip with excessive force may cause damage to the metal clip.

9. Touch the static-protective package that contains the new Ethernet adapter to any unpainted metal surface on the server. Then, remove the Ethernet adapter from the package.
10. Align the adapter with the adapter connector on the system board; then, tilt the adapter so that the port connectors on the adapter line up with the port openings on the chassis. See Figure 17.

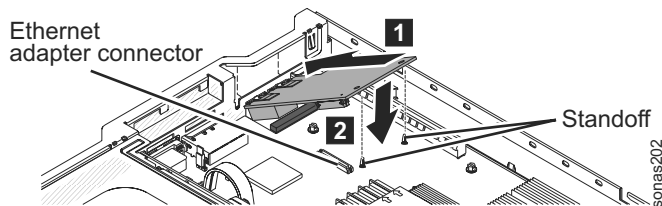


Figure 17. Aligning the Ethernet adapter port connectors with the port openings

11. Slide the port connectors on the adapter into the port openings on the chassis; then, press the adapter firmly until the two standoffs engage the adapter. Make sure the adapter is securely seated on the connector on the system board.

Make sure the port connectors on the adapter do not set on the rubber stopper. The following illustration shows the side view of the adapter in the

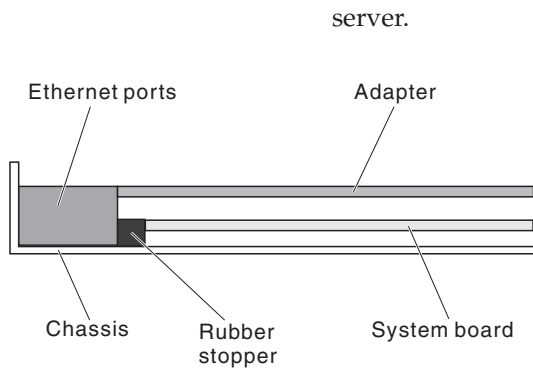


Figure 18. Side view of adapter in the server

Attention: Make sure the port connectors on the adapter are aligned properly with the chassis on the rear of the server. An incorrectly seated adapter might cause damage to the system board or the adapter.

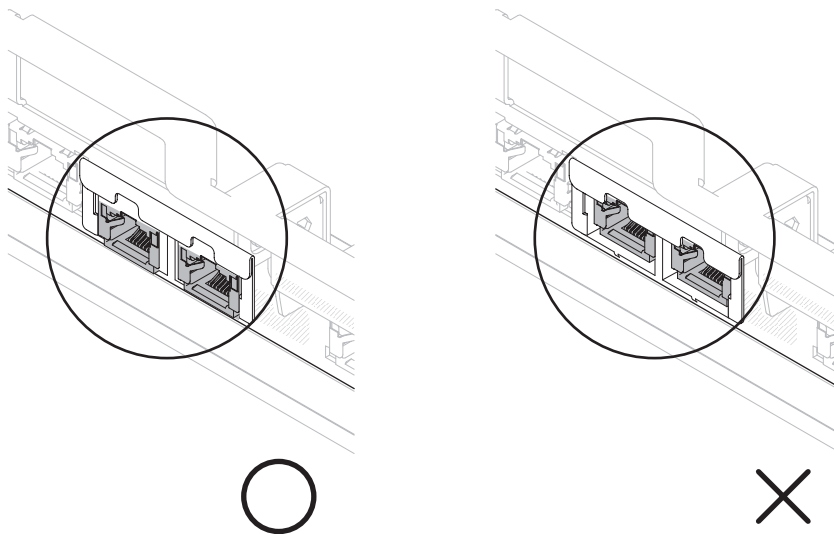


Figure 19. Port connector alignment

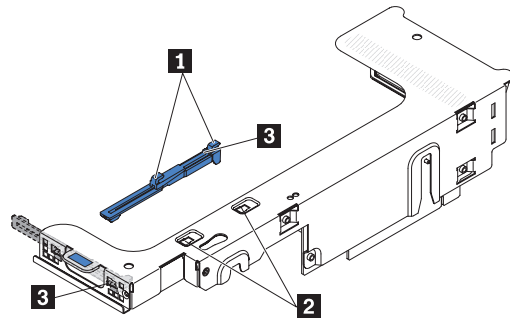
12. Install PCI riser **1**. See Installing a PCI riser-card assembly.
13. Install the cover. See Installing the cover.
14. Slide the server into the rack.
15. Reconnect the power cord and any cables that you removed.
16. Turn on the peripheral devices and the server.

Storing the full-length-adapter bracket

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

If you are removing a full-length adapter in the upper riser-card PCI slot and will replace it with a shorter adapter or no adapter, you must remove the full-length-adapter bracket from the end of the riser-card assembly and return the bracket to its storage location.

To remove and store the full-length-adaptor bracket, complete the following procedure.



1. Press the bracket tab **3** and slide the bracket to the left until the bracket falls free of the riser-card assembly.
2. Align the bracket with the storage location on the riser-card assembly as shown.
3. Place the two hooks **1** in the two openings **2** in the storage location on the riser-card assembly.
4. Press the bracket tab **3** and slide the bracket toward the expansion-lot-opening end of the assembly until the bracket clicks into place.

Removing the SAS riser-card and controller assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove the SAS riser-card and controller assembly from the server, complete the following procedure.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. To remove the SAS riser-card and controller assembly for a 16-drive-capable server model, complete the following steps.

Figure 20 on page 108 shows the SAS riser card in the 16-drive-capable server model.

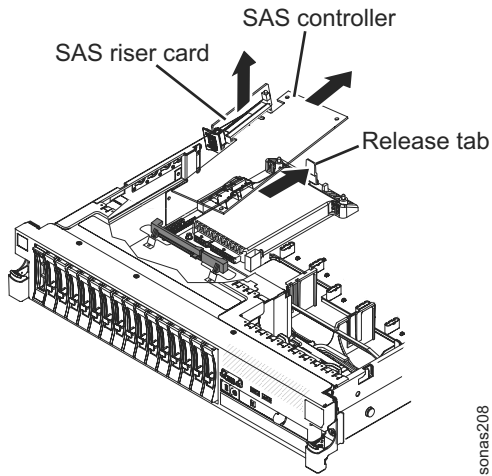


Figure 20. 16-drive-capable server model

- a. Press the release tab toward the rear of the server and lift the back end of the SAS controller card slightly.
 - b. Place your fingers underneath the upper portion of the SAS riser card and lift the assembly from the system board.
 - c. Slide the front end of the SAS controller card out of the retention bracket and lift the assembly out of the server.
3. To remove the SAS riser-card and controller assembly for a tape-enabled server model, complete the following steps.

Figure 21 shows the SAS riser card in the tape-enabled server model.

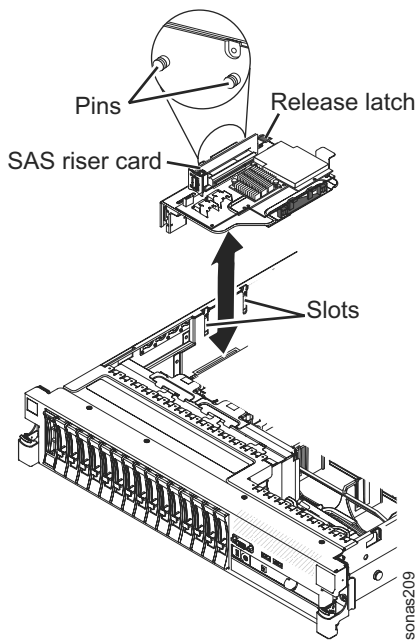


Figure 21. Tape-enabled server model

- a. Press down on the assembly release latch and lift up on the tab to release the SAS controller assembly, which includes the SAS riser card, from the system board.

- b. Lift the front and back edges of the assembly to remove the assembly from the server.

Installing the SAS riser card and controller assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the SAS riser-card and controller assembly in the file module, complete the following procedure.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. To install the SAS riser-card and controller assembly for a 16-drive-capable server model, complete the following steps.

Figure 22 shows the SAS riser-card and controller assembly in the 16-drive-capable server model.

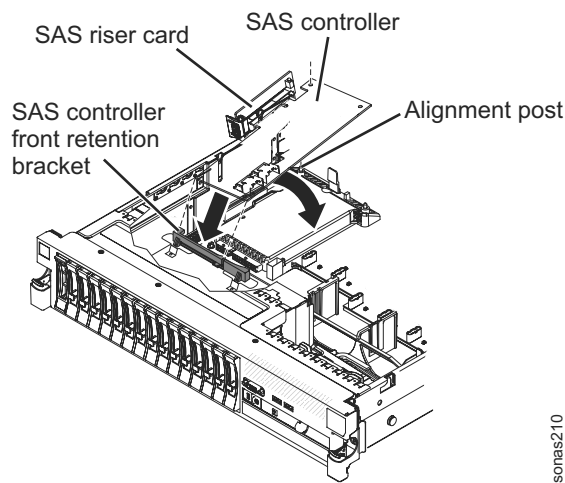


Figure 22. SAS riser-card and controller assembly on the 16-drive-capable server model

- a. If you are replacing a ServeRAID-BR10il v2 SAS/SATA controller with a ServeRAID-M5015/M5014 SAS/SATA controller, you must swap the controller retention brackets to fit the new SAS controller. See Figure 23 on page 110.

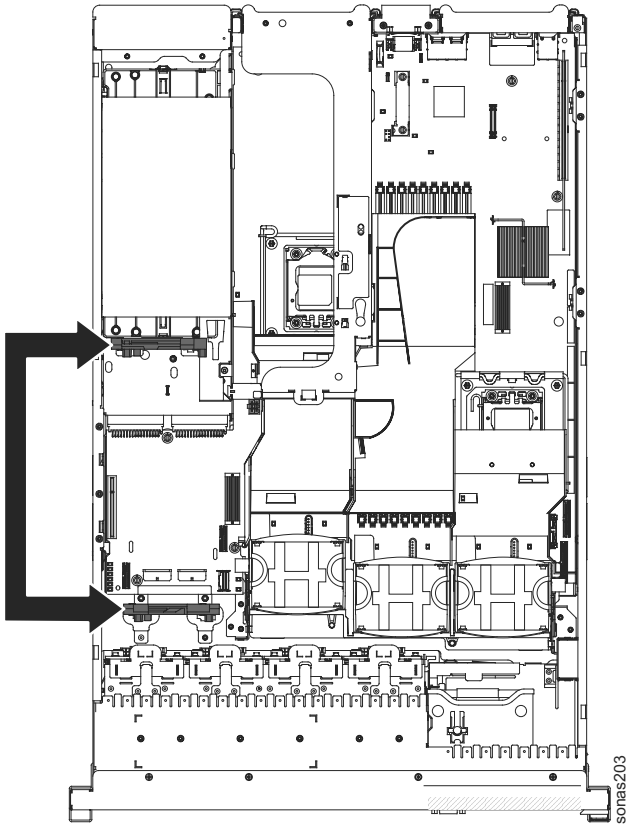


Figure 23. Controller retention brackets on 16-drive-capable server model

- 1) Remove the SAS controller front retention bracket from the server. See Figure 24.

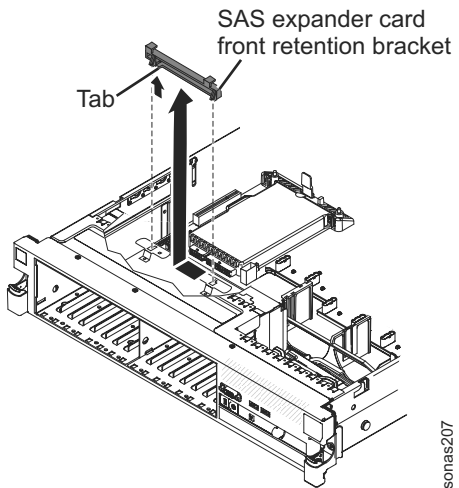
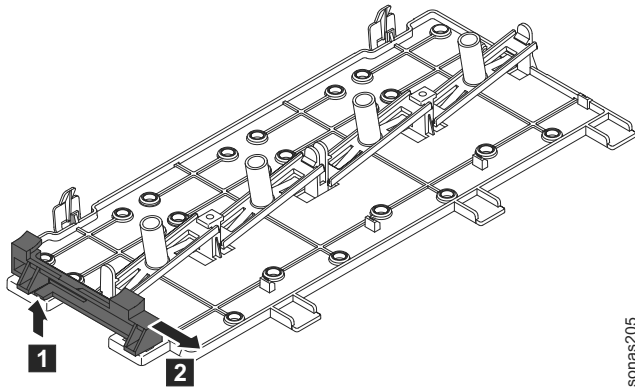


Figure 24. SAS controller front retention brackets

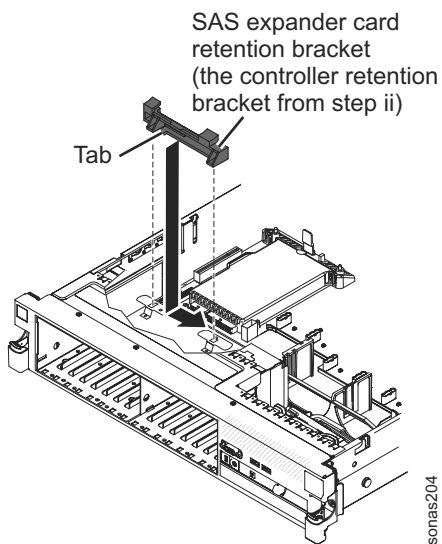
- 2) Remove the rear controller retention bracket located in the battery bay above the power supplies by pulling up the release tab **1** and sliding the bracket outward **2**. See Figure 25 on page 111.



sonas205

Figure 25. Removing the rear controller retention bracket

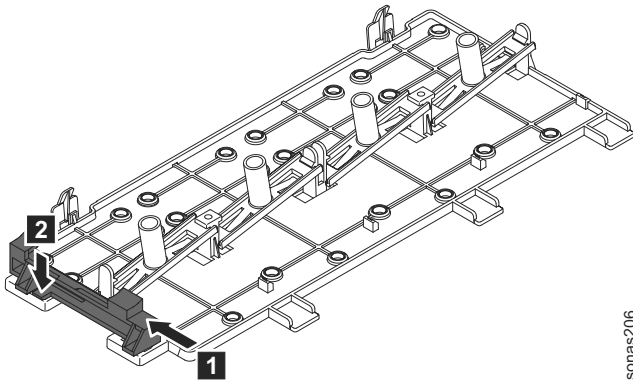
- 3) Install the controller retention bracket from step ii by aligning the retention bracket controller slot and then placing the bracket tabs in the holes on the chassis, and slide the bracket to the left until it clicks into place. See Figure 26.



sonas204

Figure 26. Installing the controller retention bracket

- 4) Install the controller retention bracket from step i by sliding the bracket inward **1** and pressing down the release tab into place **2**. See Figure 27 on page 112.



sonas206

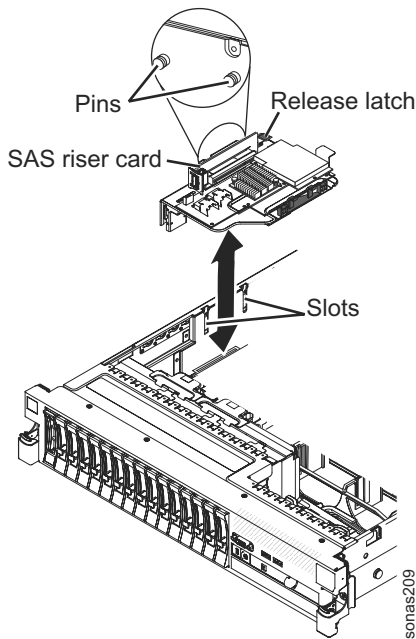
Figure 27. Sliding the controller retention bracket inward and pressing the release tab

- b. Place the front end of the SAS controller in the retention bracket and align the SAS riser card with the SAS riser-card connector on the system board.
- c. Press down on the SAS riser card and the rear edge of the SAS controller until the SAS riser card is firmly seated and the SAS controller card retention latch clicks into place.

One or two pins (depending on the size of the card) clicks into the corner holes of the SAS controller card when the controller card is correctly seated.

- 3. To install the SAS riser-card and controller assembly for a tape-enabled server model, complete the following steps.

Figure 28 shows the SAS riser card in the tape-enabled server model.



sonas209

Figure 28. SAS riser-card assembly on tape-enabled server model

- a. Align the pins on the backside of the riser with the slots on the side of the chassis.
- b. Align the SAS riser card of the SAS controller assembly with the SAS riser-card connector on the system board.

- c. Press the SAS controller assembly into place; make sure that the SAS riser card is firmly seated and that the release latch and retention latch holds the assembly securely.

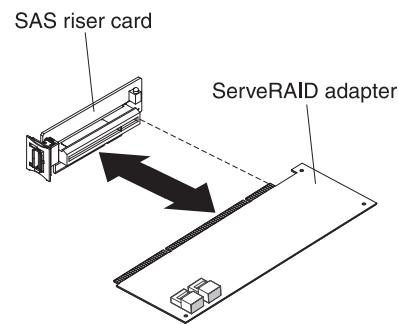
Removing the ServeRAID SAS controller from the SAS riser-card

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

A ServeRAID SAS controller is installed in a dedicated slot on the SAS riser card.

Note: For brevity, in this documentation the ServeRAID SAS controller is often referred to simply as *SAS controller*.



Important: If an 8-disk-drive optional expansion device in a 16-disk drive is installed in a 12-drive-capable server, the SAS controller is installed in a PCI riser-card assembly. Install and remove the SAS controller the same way as any other PCI adapter. Do not use the instructions in this topic. Use the instructions in “Installing a PCI adapter in a PCI riser-card assembly” on page 99.

To remove a ServeRAID SAS controller from a SAS riser card, complete the following procedure.

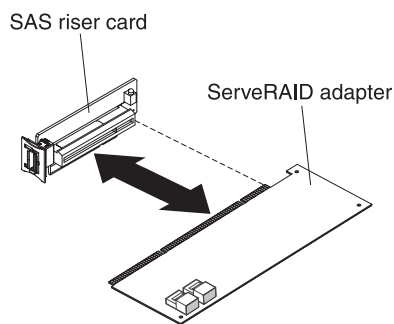
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Locate the SAS riser-card and controller assembly near the left front corner of the server.
6. Disconnect the SAS signal cables from the connectors on the SAS controller.
7. Remove the SAS controller assembly, which includes the SAS riser card, from the server, as described in “Removing the SAS riser-card and controller assembly” on page 107.
8. Pull the SAS controller horizontally out of the connector on the SAS riser card.

9. If you are replacing the SAS controller card, remove the battery, but keep the cables connected.
10. If you are instructed to return the ServeRAID SAS controller, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

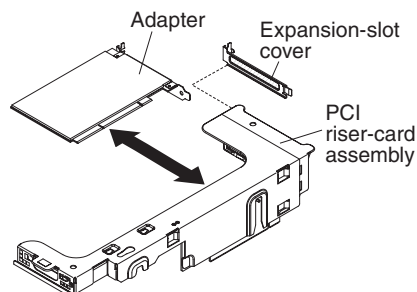
Installing a ServeRAID SAS controller in the SAS riser-card

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.



To install a SAS controller on the SAS riser card, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Touch the static-protective package that contains the new ServeRAID SAS controller to any unpainted metal surface on the file module. Then, remove the ServeRAID SAS controller from the package.
3. If you are replacing a SAS controller that uses a battery, continue to use that battery with the new SAS controller.
4. Turn the SAS controller so that the keys on the bottom edge align correctly with the connector on the SAS riser card in the SAS controller assembly.
5. Firmly press the SAS controller horizontally into the connector on the SAS riser card.
6. Install the SAS riser card and controller assembly, as described in “Installing the SAS riser card and controller assembly” on page 109.
7. Install the cover, as described in “Installing the cover” on page 80.

8. Slide the file module into the rack.
9. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

10. Allow the initialization process to complete. If you do not, the battery pack does not work, and the file module might not start.

When you restart the file module for the first time after you install a SAS controller with a battery, the monitor screen remains blank while the controller initializes the battery. This might take a few minutes, after which the startup process continues. This is a one-time occurrence.

11. Run the file module for 4 to 6 hours to fully charge the controller battery.

The battery comes partially charged, at 30% or less of capacity. The LED just above the battery on the controller remains lit until the battery is fully charged.

Until the battery is fully charged, the controller firmware sets the controller cache to write-through mode; after the battery is fully charged, the controller firmware re-enables write-back mode.

12. When you restart the file module, import the existing RAID configuration to the new ServeRAID SAS controller at the prompt.

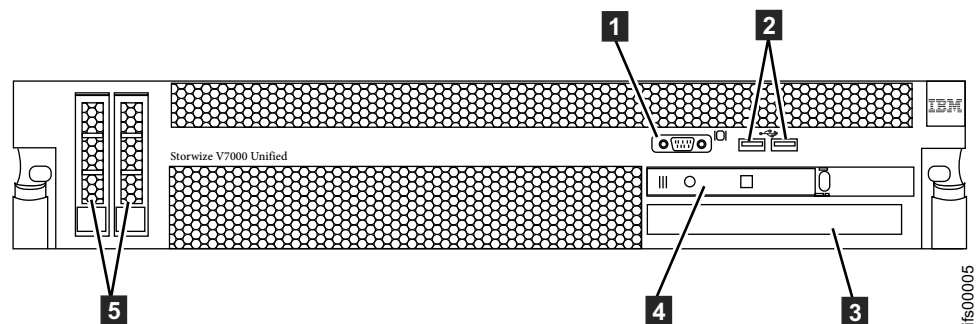
Removing a hot-swap hard disk drive

The following procedure is for a Tier 1 customer replaceable unit (CRU).

Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove a hard disk drive from a hot-swap bay, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Press up on the release latch at the top of the drive front.
3. Rotate the handle on the drive downward to the open position.
4. Pull the hot-swap drive assembly from the bay.

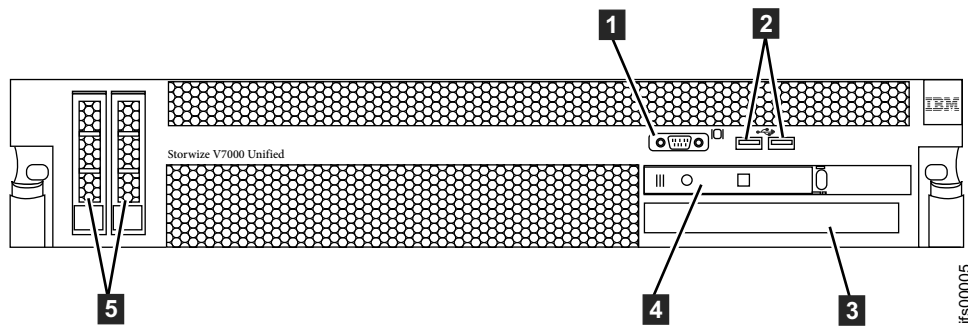
5. If you are instructed to return the hot-swap drive, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a hot-swap hard disk drive

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

Locate the documentation that comes with the hard disk drive and follow those instructions in addition to the instructions in this topic.



Attention: To maintain proper system cooling, do not operate the file module for more than 10 minutes without either a drive or a filler panel installed in each bay.

To install a drive in a hot-swap bay, complete the following procedure.

1. Orient the drive as shown in the illustration.
2. Make sure that the tray handle is open.
3. Align the drive assembly with the guide rails in the bay.
4. Gently push the drive assembly into the bay until the drive stops.
5. Push the tray handle to the closed (locked) position.
6. Since both hard disk drives are part of a mirrored array, the array will start to rebuild on the newly installed disk.

While the array rebuilds, the green hard-disk-drive status LED blinks fast, and the amber hard-disk-drive status LED blinks slowly.

Note: If the file module is configured for mirrored array (RAID 1) operation using a ServeRAID adapter, you might have to reconfigure your disk arrays after you install hard disk drives. See the ServeRAID adapter documentation for additional information about RAID operation and complete instructions for using the ServeRAID adapter.

7. Monitor the rebuild and initialization.
 - a. Open the management GUI.
 - b. Click **Monitoring > Events**.
 - c. Note the Eventtime of the rebuild message so that you can locate the rebuild status.
8. When the rebuild and initialization are complete, check the hard-disk-drive status LED to verify that the hard-disk drive is operating correctly.

If the amber hard-disk-drive status LED for a drive is lit continuously, the drive is faulty and you must replace it. If the green hard-disk-drive activity LED is flashing, the drive is being accessed.

Removing an optional ServeRAID adapter advanced feature key

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the server and peripheral devices and disconnect the power cords.
3. Remove the cover, as described in “Removing the cover” on page 79.
4. Grasp the feature key and lift to remove it from the connector on the ServeRAID adapter. See Figure 29 and Figure 30 on page 118.

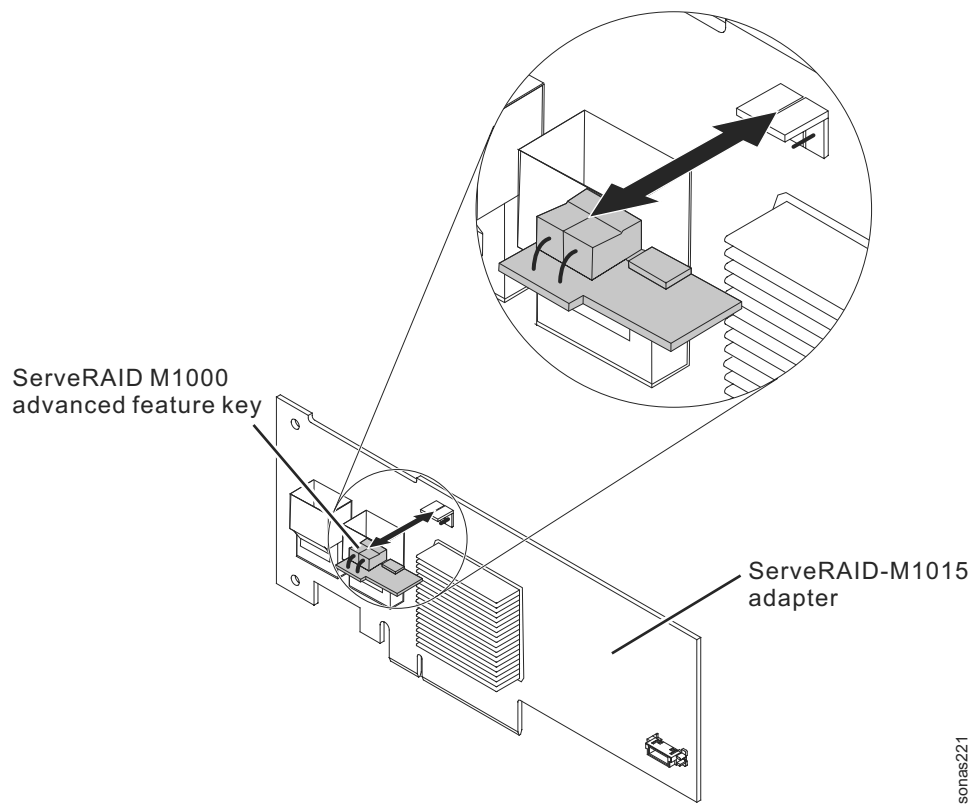


Figure 29. ServeRAID M1000 advanced feature key and M1015 adapter

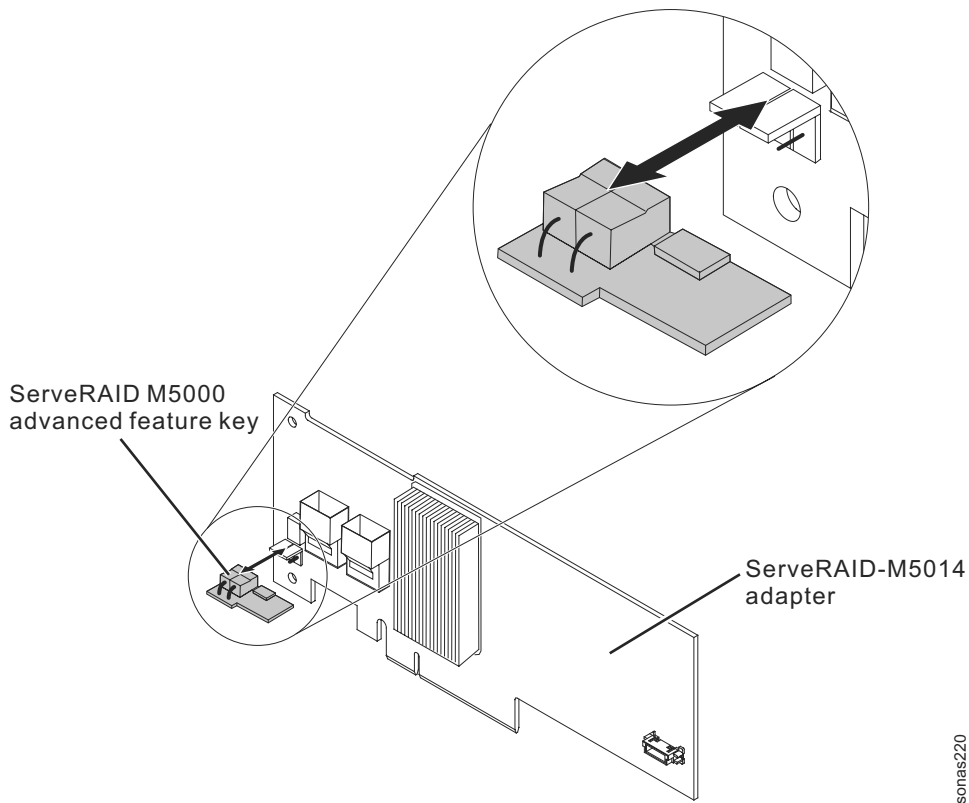


Figure 30. ServeRAID M5000 advanced feature key and M5014 adapter

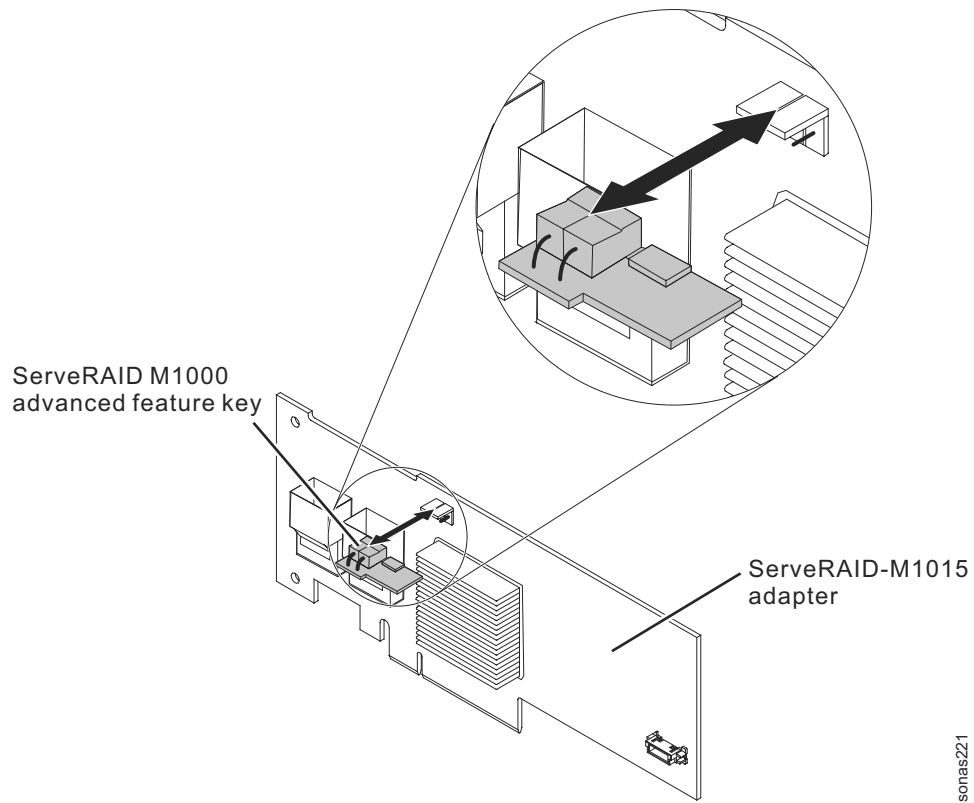
5. If you are instructed to return the feature key, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing an optional ServeRAID adapter advanced feature key

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the server and peripheral devices and disconnect the power cords.
3. Remove the cover, as described in “Removing the cover” on page 79.
4. Align the feature key with the connector on the ServeRAID adapter and push it into the connector until it is firmly seated. See Figure 31 on page 119 and Figure 32 on page 120.



sonas221

Figure 31. ServeRAID M1000 advanced feature key and M1015 adapter

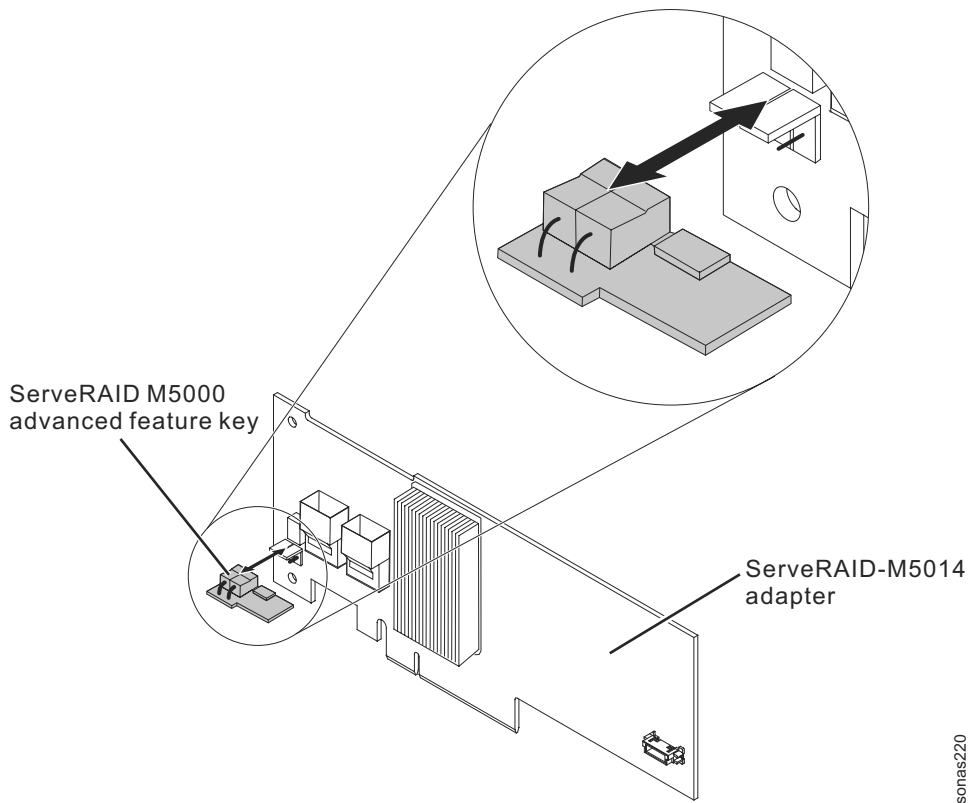


Figure 32. ServeRAID M5000 advanced feature key and M5014 adapter

5. Reconnect the power cord and any cables that you removed.
6. Install the cover, as described in Installing the cover.
7. Slide the server into the rack.
8. Turn on the peripheral devices and the server.

Removing the serveRAID SAS controller battery from the remote battery tray

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove a serveRAID SAS controller battery from the remote battery tray, complete the following procedure.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.

5. Locate the remote battery tray in the server and remove the battery that you want to replace.
 - a. Remove the battery retention clip from the tabs that secure the battery to the remote battery tray. See Figure 33.

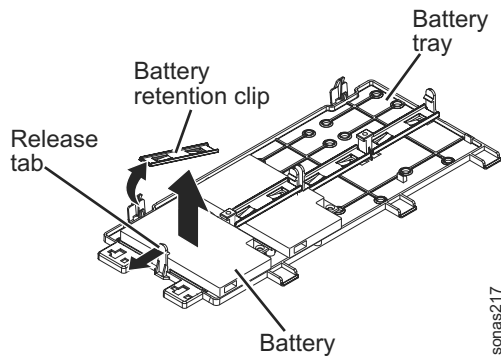


Figure 33. Releasing the battery retention clip

- b. Lift the battery and battery carrier from the tray and carefully disconnect the remote battery cable from the interposer card on the ServeRAID controller. See Figure 34.

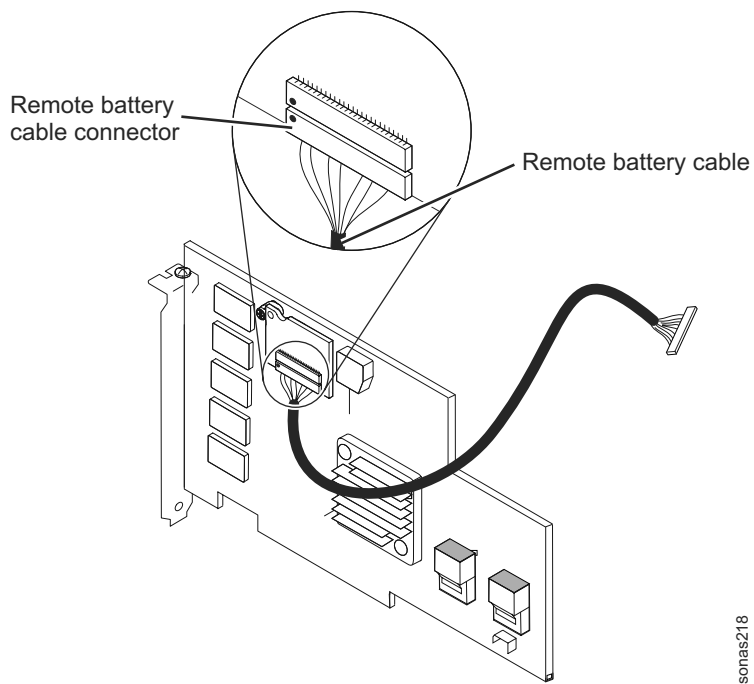


Figure 34. Disconnecting the remote battery cable

- c. Disconnect the battery carrier cable from the battery.
 - d. Squeeze the clip on the side of the battery and battery carrier to remove the battery from the battery carrier.

Note: If your battery and battery carrier are attached with screws instead of a locking-clip mechanism, remove the three screws to remove the battery from the battery carrier. See Figure 35 on page 122.

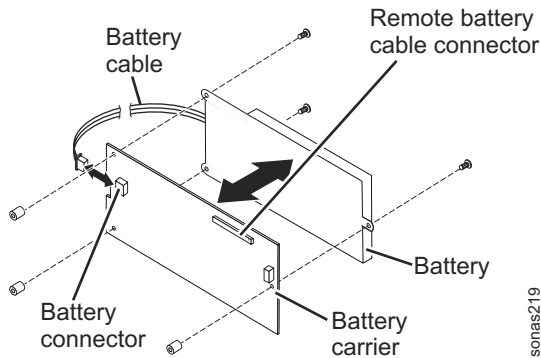


Figure 35. Removing the battery from the battery carrier

- e. If you are instructed to return the ServeRAID SAS controller battery, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the serveRAID SAS controller battery on the remote battery tray

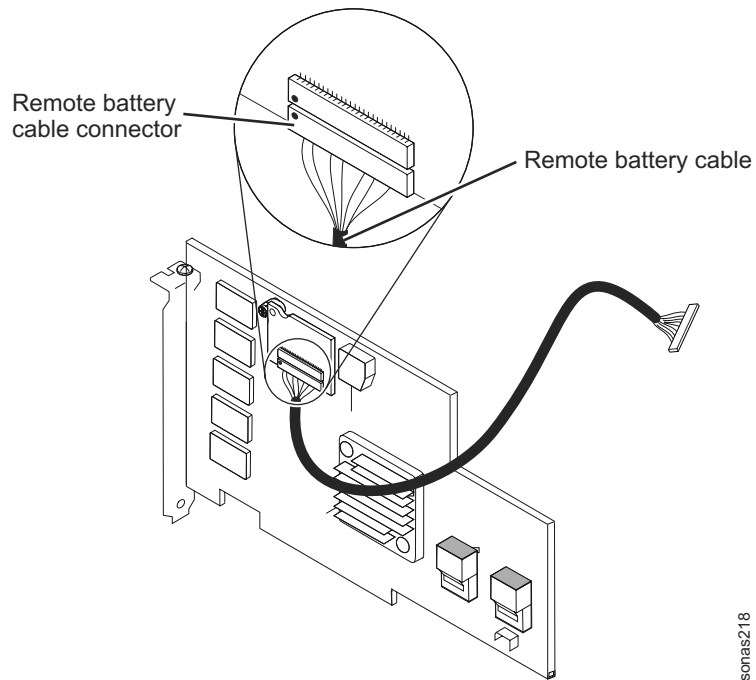
The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the serveRAID SAS controller battery on the remote battery tray, complete the following procedure.

1. Place the replacement battery on the battery carrier from which the former battery had been removed, and connect the battery carrier cable to the replacement battery.
2. Connect the remote battery cable to the interposer card.

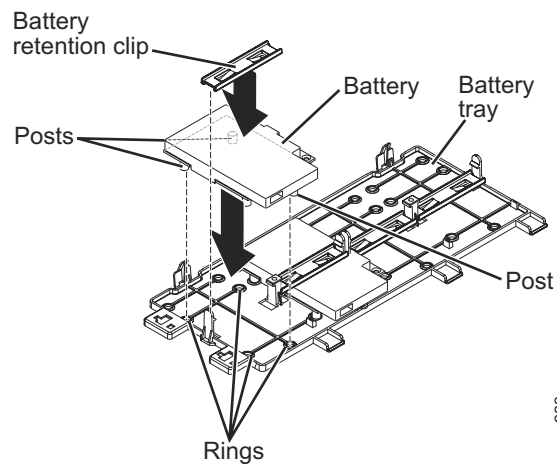
Attention: To avoid damage to the hardware, make sure that you align the black dot on the cable connector with the black dot on the connector on the interposer card. Do not force the remote battery cable into the connector. See Figure 36 on page 123



sonas218

Figure 36. Connecting the remote battery cable

3. On the remote battery tray, find the pattern of recessed rings that matches the posts on the battery and battery carrier. See Figure 37.



sonas222

Figure 37. Locating the posts on the battery and battery carrier

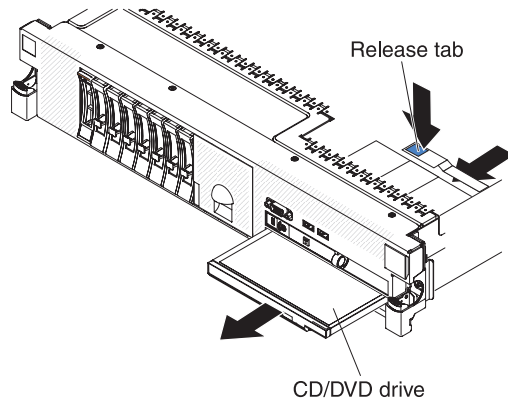
4. Press the posts into the rings and underneath the tabs on the remote battery tray.
5. Secure the battery to the tray with the battery retention clip.
6. Install the cover, as described in Installing the cover.

Removing a CD-RW/DVD drive

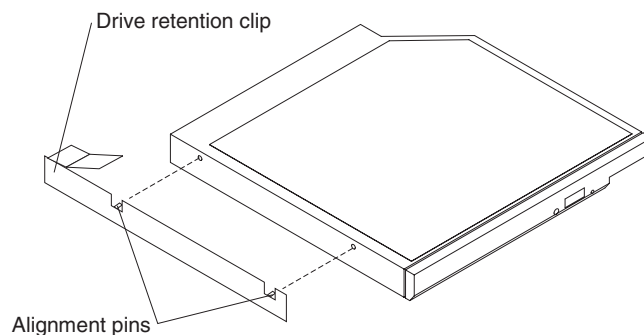
The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove the CD-RW/DVD drive, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Find the CD-RW/DVD drive, and the blue release tab on the top left hand corner of the CD-RW/DVD drive. Press the release tab down to release the drive; then, while pressing the tab, pull the drive toward the front of the server.
6. From the front of the server, carefully pull the drive out of the bay.



Note: The cables to the CD-RW/DVD drive do not need to be disconnected from the CD-RW/DVD drive in order to remove the drive.

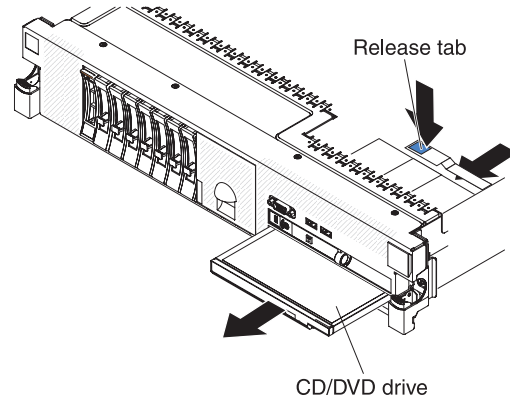
7. Remove the drive retention clip from the drive. The retention bracket is not secured by any fasteners; carefully unclip the retention bracket from the CD-RW/DVD drive, noting the point of attachment as indicated in the figure.
8. Carefully attach the retention bracket to the replacement CD-RW/DVD drive, noting the point of attachment as indicated in the figure.
9. If you are instructed to return the CD-RW/DVD drive, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the CD-RW/DVD drive

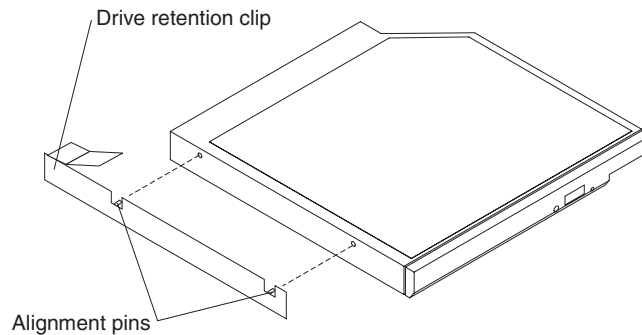
The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To install the replacement CD-RW/DVD drive, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Follow the instructions that come with the drive to set any jumpers or switches.
3. If a drive filler panel is in place, remove it.
4. Attach the drive-retention clip to the side of the drive. The retention bracket is not secured by any fasteners; carefully attach the retention bracket to the CD-RW/DVD drive, noting the point of attachment as indicated in the figure.



5. Slide the drive into the CD/DVD drive bay until the drive clicks into place.
6. Install the cover, as described in “Installing the cover” on page 80.
7. Slide the file module into the rack.
8. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

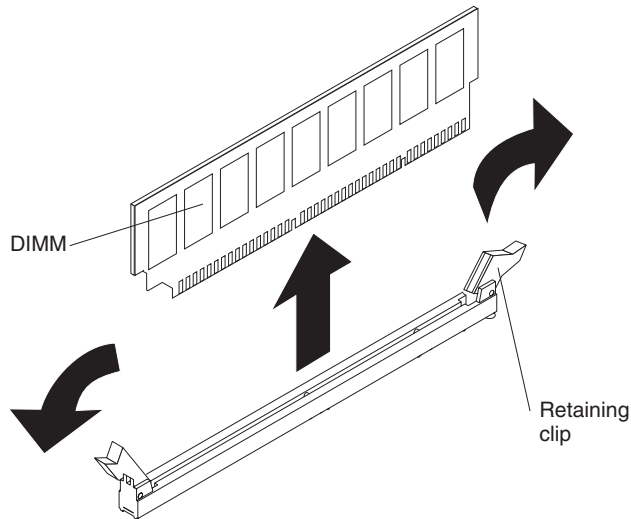
Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Removing a memory module

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Note: Before running a procedure, refer to “Removing a file module to perform a maintenance action” on page 47.

To remove a DIMM, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. If riser-card assembly 1 contains one or more adapters, remove it (see “Removing a PCI riser-card assembly” on page 95).
6. Remove the DIMM air baffle, as described in “Removing the DIMM air baffle” on page 89.
7. Open the retaining clip on each end of the DIMM connector and lift the DIMM from the connector.
Attention: To avoid breaking the retaining clips or damaging the DIMM connectors, open and close the clips gently.
8. If you are instructed to return the DIMM, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a memory module

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

See Figure 38 for DIMM locations for the Storwize V7000 Unified System x3650 M2 server and Figure 39 on page 128 for DIMM locations for the Storwize V7000 Unified System x3650 M3 server.

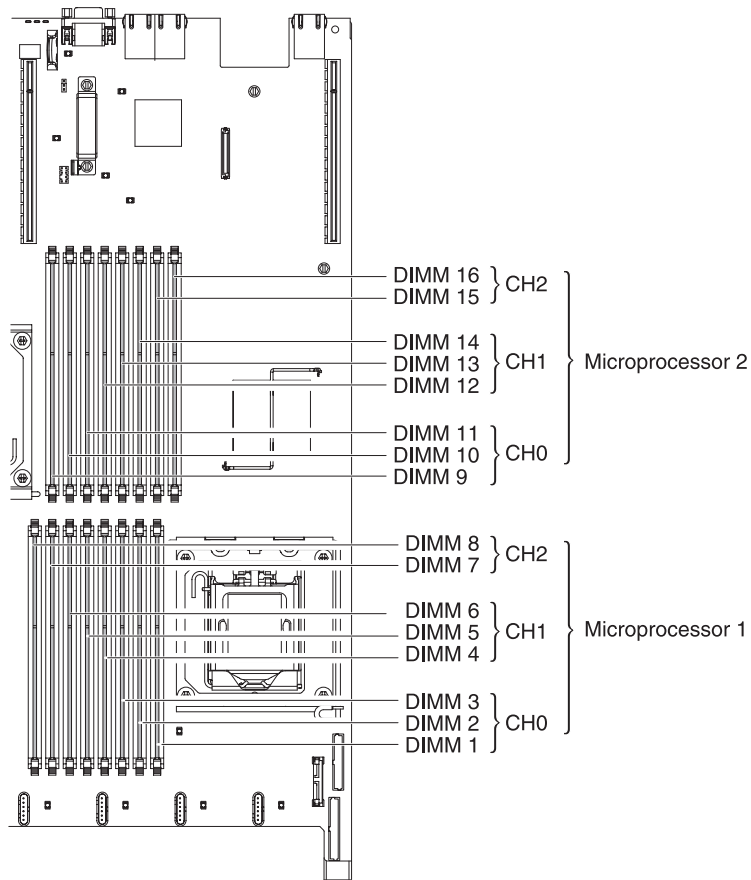


Figure 38. DIMM locations for the Storwize V7000 Unified System x3650 M2 server

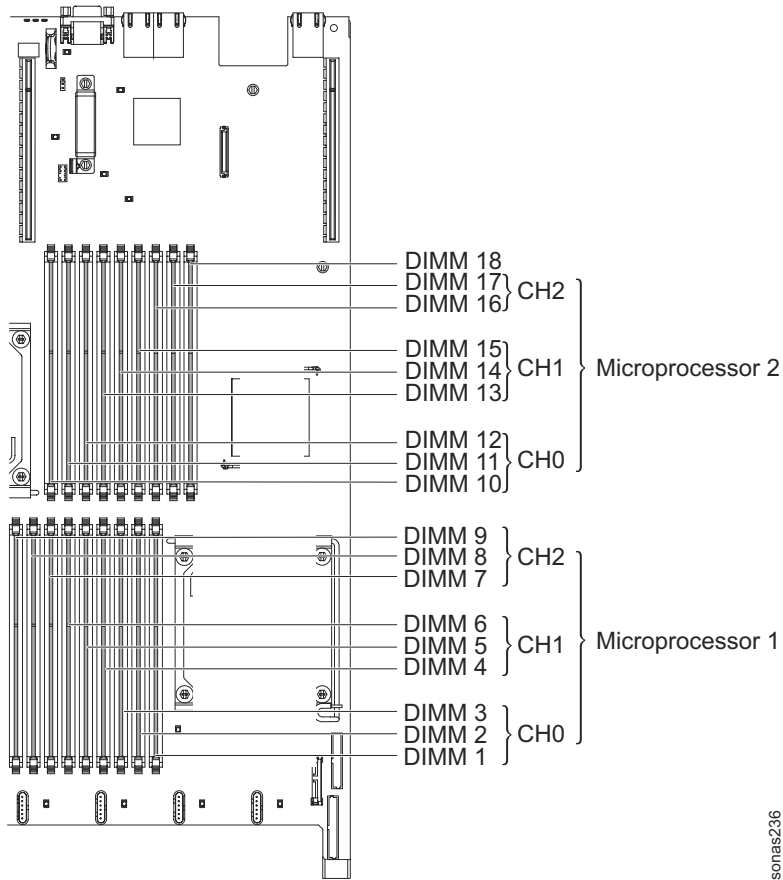
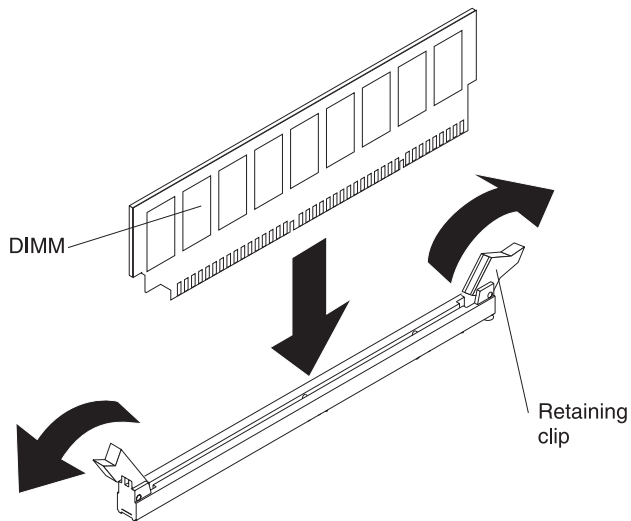


Figure 39. DIMM locations for the Storwize V7000 Unified System x3650 M3 server

To install a DIMM, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in "Safety" on page xi, "Safety statements" on page xiii, and "Installation guidelines" on page 50.
2. Remove riser-card assembly 1, as described in "Removing a PCI riser-card assembly" on page 95.

3. Remove the DIMM air baffle, as described in “Removing the DIMM air baffle” on page 89.
4. Open the retaining clip on each end of the DIMM connector.
Attention: To avoid breaking the retaining clips or damaging the DIMM connectors, open and close the clips gently.
5. Touch the static-protective package that contains the DIMM to any unpainted metal surface on the file module. Then, remove the DIMM from the package.
6. Turn the DIMM so that the DIMM keys align correctly with the connector.
7. Insert the DIMM into the connector by aligning the edges of the DIMM with the slots at the ends of the DIMM connector.
Attention: If there is a gap between the DIMM and the retaining clips, the DIMM has not been correctly inserted; open the retaining clips, remove the DIMM, and then reinsert it.
8. Firmly press the DIMM straight down into the connector by applying pressure on both ends of the DIMM simultaneously.
The retaining clips snap into the locked position when the DIMM is firmly seated in the connector.
9. Repeat step 2 on page 128 through step 7 until all the new or replacement DIMMs are installed.
10. Replace the DIMM air baffle, as described in “Installing the DIMM air baffle” on page 90.
11. Replace the PCI riser card assemblies, as described in “Installing a PCI riser-card assembly” on page 96.
12. Install the cover, as described in “Installing the cover” on page 80.
13. Slide the file module into the rack.
14. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

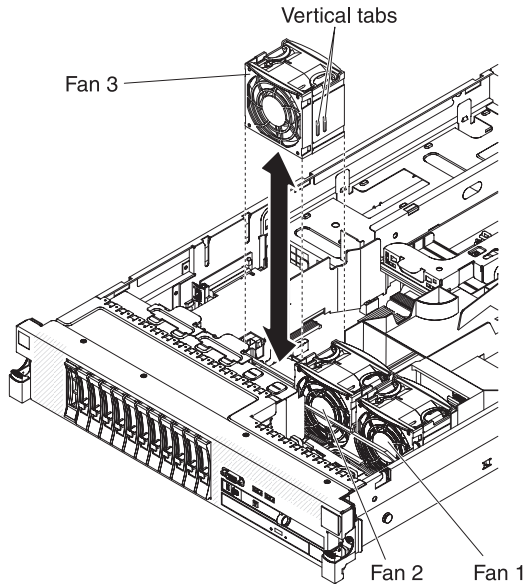
Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.
15. Go to the **Setup** utility and make sure that all the installed DIMMs are present and enabled.

Removing a hot-swap fan

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Attention: To ensure proper server operation and cooling, if you remove a fan you must install a replacement fan as soon as possible.

To remove any of the 3 replaceable fans, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Leave the server connected to power.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. To ensure proper system cooling, do not remove the top cover for more than 30 minutes during this procedure.
The LED on the system board near the connector for the failing fan is lit.
6. Grasp the fan by the finger grips on the sides of the fan.
7. Lift the fan out of the server.
8. Replace the fan within 30 seconds.
9. If you are instructed to return the fan, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a hot-swap fan

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

For proper cooling, the server requires that all three fans be installed at all times.

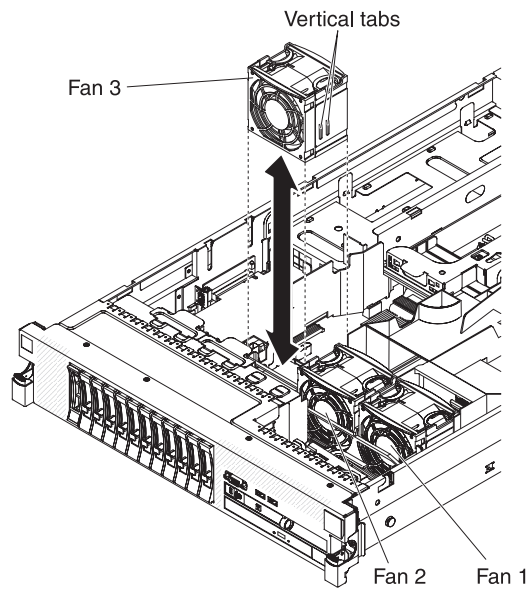
Attention: To ensure proper server operation, if a fan fails, replace it immediately. Have a replacement fan ready to install as soon as you remove the failed fan.

The fans use system-board fan connectors 2, 4, and 6 only. The following table lists the fan connector on the system board for each double-fan. See “System-board internal connectors” in the *IBM Storwize V7000 Unified Information Center* for the locations of the fan connectors.

Table 33. System board fan locations

Fan number	System board fan connector
1	2
2	4
3	6

To install any of the three replaceable fans, complete the following steps.



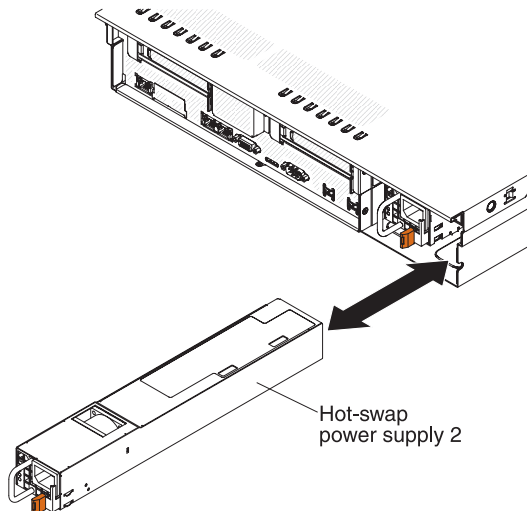
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Orient the new fan over its position in the fan bracket so that the connector on the bottom aligns with the fan connector on the system board.
3. Align the vertical tabs on the fan with the slots on the fan cage bracket.
4. Push the new fan into the fan connector on the system board. Press down on the top surface of the fan to seat the fan fully.
5. Repeat until all the new or replacement fans are installed.
6. Install the cover, as described in “Installing the cover” on page 80.
7. Slide the file module into the rack.

Removing a hot-swap ac power supply

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

Important: The file module has two power supplies for redundancy. Do not replace a power supply while the file module is powered on. Both power supplies are required to provide redundancy to the file module. Follow the procedures in “Procedure: Powering off your system” on page 202 to power off the file module before replacing a power supply.

To remove a power supply, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices.
3. Disconnect the power cord from the power supply that you are removing.
4. Grasp the power-supply handle.
5. Press the orange release latch to the left and hold it pressed.
6. Pull the power supply part of the way out of the bay.
7. Release the release latch; then, support the power supply and pull it the rest of the way out of the bay.
8. If you are instructed to return the power supply, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a hot-swap ac power supply

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

The file module supports a maximum of two hot-swap ac power supplies.

The following notes describe the type of power supply that the server supports and other information that you must consider when you install a power supply:

- Make sure that the devices that you are installing are supported. For a list of supported devices for the server, see “Parts listing for Storwize V7000 Unified System x3650 M3 file modules” in the *IBM Storwize V7000 Unified Information Center*.
- Before you install an additional power supply or replace a power supply with one of a different wattage, you may use the IBM Power Configurator utility to determine current system power consumption. For more information and to download the utility, go to <http://www-03.ibm.com/systems/bladecenter/resources/powerconfig.html>.
- The server comes with one hot-swap 12-volt output power supply that connects to power supply bay 1. The input voltage is 110 V ac or 220 V ac auto-sensing.

- You cannot mix 460-watt and 675-watt power supplies, high-efficiency and non-high-efficiency power supplies, or ac and dc power supplies in the server.
- The following information applies when you install 460-watt power supplies in the server:
 - A warning message is generated if the total power consumption exceeds 400 watts and the server only has one operational 460-watt power supply. In this case, the server can still operate under normal condition. Before you install additional components in the server, you must install an additional power supply
 - The server automatically shuts down if the total power consumption exceeds the total power supply output capacity
 - You can enable the power capping feature in the Setup utility to control and monitor power consumption in the server (see the “Setup utility” information available in “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center*.)

The following table shows the system status when you install 460-watt power supplies in the server:

Table 34. System status with 460-watt power supplies installed

Total system power consumption (in watts)	Number of 460-watt power supplies installed		
	One	Two	Two with one failure
< 400	Normal	Normal, redundant power	Normal
400 ~ 460	Normal, status warning	Normal, redundant power	Normal, status warning
> 460	System shutdown	Normal	System shutdown

- Power supply 1 is the default/primary power supply. If power supply 1 fails, you must replace the power supply immediately.
- You can order an optional power supply for redundancy.
- These power supplies are designed for parallel operation. In the event of a power-supply failure, the redundant power supply continues to power the system. The server supports a maximum of two power supplies.
- For instructions on how to install a hot-swap dc power supply, refer to the documentation that comes with the dc power supply.

Statement 8

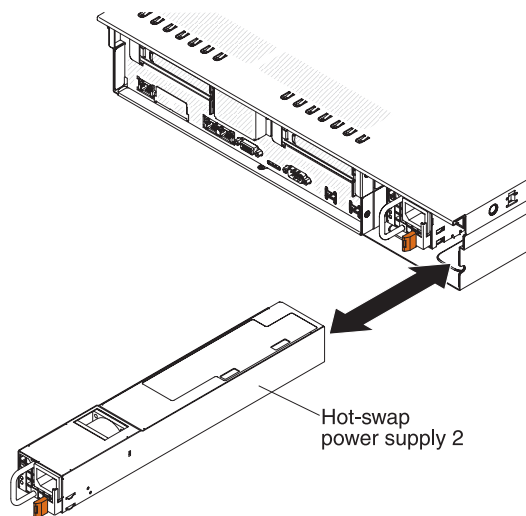


CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

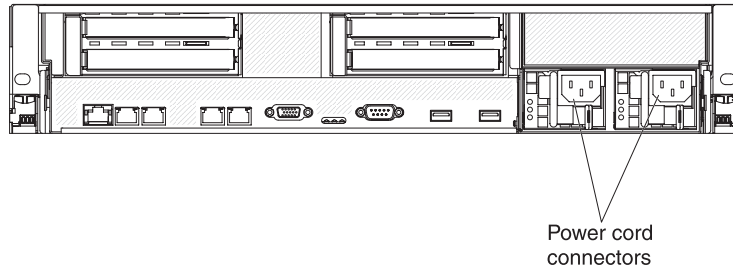


Attention: During normal operation, each power-supply bay must have either a power supply or power-supply filler installed for proper cooling.

To install an ac power supply, complete the following steps:

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Slide the ac power supply into the bay until the retention latch clicks into place.
3. Connect the power cord for the new ac power supply to the power-cord connector on the power supply.

The following illustration shows the power-supply connectors on the back of the file module.

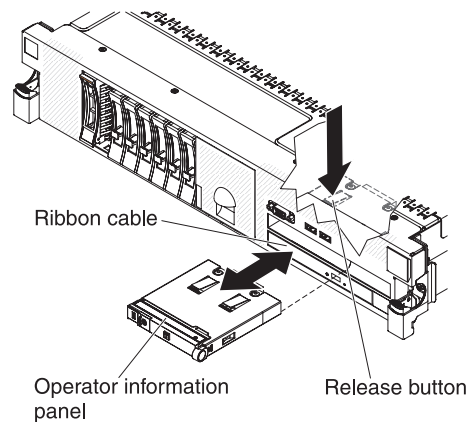


4. Route the power cord through the cable management arm on the rear of the file module, to prevent the power cord from being accidentally pulled out when you slide the file module in and out of the rack.
5. Connect the power cord to a properly grounded electrical outlet.
6. Make sure that the error LED on the power supply is not lit, and that the dc power LED and ac power LED on the power supply are lit, indicating that the power supply is operating correctly.

Removing the operator information panel assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

To remove the operator information panel assembly, complete the following procedure.



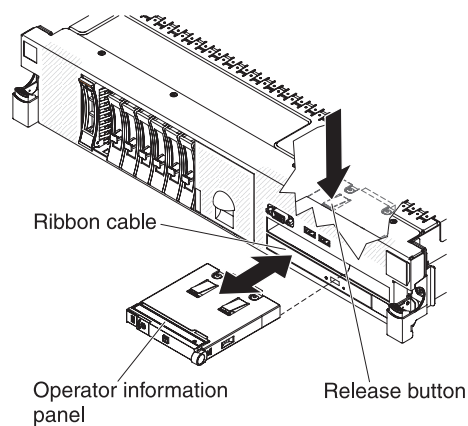
1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Disconnect the cable from the back of the operator-information panel assembly.
6. Reach inside the file module and press the release tab; then, while holding the release tab down, push the assembly toward the front of the file module.
7. From the front of the file module, carefully pull the operator information panel assembly out of the file module.

8. If you are instructed to return the operator information panel assembly, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the operator information panel assembly

The following procedure is for a Tier 1 customer replaceable unit (CRU). Replacement of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation. Service agreements can be purchased so that you can ask IBM to replace these units.

To install the replacement operator information panel assembly, complete the following procedure.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Slide the operator information panel assembly into the server until it clicks into place.
3. Inside the server, connect the cable to the rear of the operator information panel assembly.
4. Install the cover, as described in “Installing the cover” on page 80.
5. Slide the file module into the rack.
6. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Removing a microprocessor and heat sink

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

Attention:

- Do not allow the thermal grease on the microprocessor and heat sink to come in contact with anything. Contact with any surface can compromise the thermal grease and the microprocessor socket.
- Dropping the microprocessor during installation or removal can damage the contacts.
- Do not touch the microprocessor contacts; handle the microprocessor by the edges only. Contaminants on the microprocessor contacts, such as oil from your skin, can cause connection failures between the contacts and the socket.

To remove a microprocessor and heat sink, complete the following steps:

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the server and peripheral devices, then label and disconnect both power cords and all external cables
3. Remove the cover, as described in “Removing the cover” on page 79.
4. Depending on which microprocessor you are removing, remove the following components, if needed:
 - **Microprocessor 1:** PCI riser card assembly 1 and DIMM air baffle, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the DIMM air baffle” on page 89.

Note: If there are two microprocessors, you must remove PCI riser card assembly 2 and microprocessor 2 air baffle first, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the microprocessor 2 air baffle” on page 86.

- **Microprocessor 2:** PCI riser card assembly 2 and microprocessor 2 air baffle, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the microprocessor 2 air baffle” on page 86.
5. Open the heat-sink release lever to the fully open position. See Figure 40.

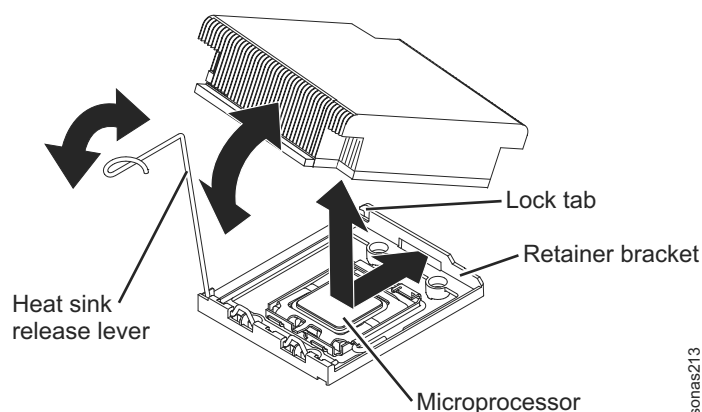


Figure 40. Heat-sink release lever

6. Lift the heat sink out of the server. If the heat sink sticks to the microprocessor, slightly twist the heat sink back and forth to break the seal. After removal, place the heat sink on its side on a clean, flat surface.
7. Release the microprocessor retention latch by pressing down on the end, moving it to the side, and releasing it to the open (up) position. See Figure 41 on page 138

on page 138.

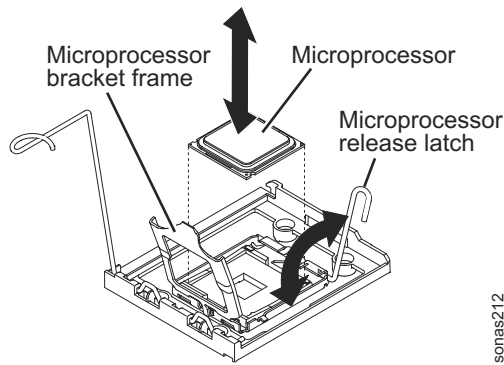


Figure 41. Microprocessor release latch

Note: The retention latch is under tension and care should be taken when unlatching and latching the retention latch.

8. Open the microprocessor bracket frame by lifting up the tab on the top edge. Keep the bracket frame in the open position.
9. Carefully lift the microprocessor straight up and out of the socket, and place it on a static-protective surface.
10. If you are instructed to return the microprocessor, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a microprocessor and heat sink

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

Read the documentation that comes with the microprocessor to determine whether you must update the IBM System x Server Firmware. To download the most current level of server firmware, complete the following steps:

1. Go to <http://www.ibm.com/systems/support/>.
2. Under **Product support**, click **System x**.
3. Under **Popular links**, click **Software and device drivers**.
4. Click **System x3650 M2** to display the matrix of downloadable files for the server.

Attention:

- A startup (boot) microprocessor must always be installed in microprocessor connector 1 on the system board.
- To ensure correct server operation, make sure that you use microprocessors that are compatible and you have installed an additional DIMM for microprocessor 2.
- Microprocessors with different stepping levels are supported in this server. If you install microprocessors with different stepping levels, it does not matter which microprocessor is installed in microprocessor connector 1 or connector 2.
- If you are installing a microprocessor that has been removed, make sure that it is paired with its original heat sink or a new replacement heat sink. Do not reuse a heat sink from another microprocessor; the thermal grease distribution might be different and might affect conductivity.
- If you are installing a new heat sink, remove the protective backing from the thermal material that is on the underside of the new heat sink.
- If you are installing a new heat sink assembly that did not come with thermal grease, see “Thermal grease” on page 143 for instructions for applying thermal grease; then, continue with step 2 of this procedure.
- If you are installing a heat sink that has contaminated thermal grease, see “Thermal grease” on page 143 for instructions for replacing the thermal grease; then, continue with step 2 of this procedure.

To install a new or replacement microprocessor, complete the following steps. The following illustration shows how to install a microprocessor on the system board.

Note: For simplicity, certain components are not shown in this illustration.

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Touch the static-protective package containing the microprocessor to any unpainted metal surface on the server. Then, remove the microprocessor from the package.
3. Rotate the microprocessor release lever on the socket from its closed and locked position until it stops in the fully open position.

Attention:

- Do not touch the microprocessor contact; handle the microprocessor by the edges only. Contaminants on the microprocessor contacts, such as oil from your skin, can cause connection failures between the contacts and the socket.
- Handle the microprocessor carefully. Dropping the microprocessor during installation or removal can damage the contacts.
- Do not use excessive force when you press the microprocessor into the socket.
- Make sure that the microprocessor is oriented and aligned and positioned in the socket before you try to close the lever. See Figure 42 on page 140.

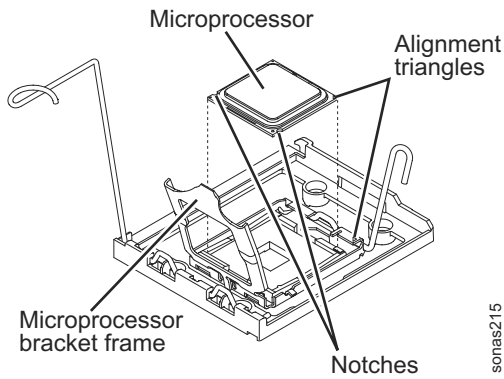
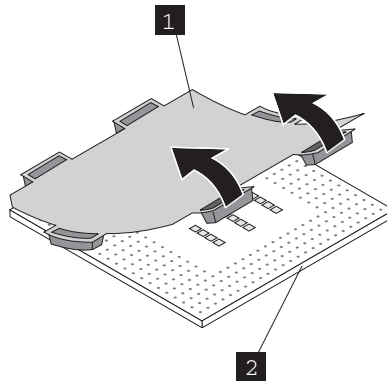


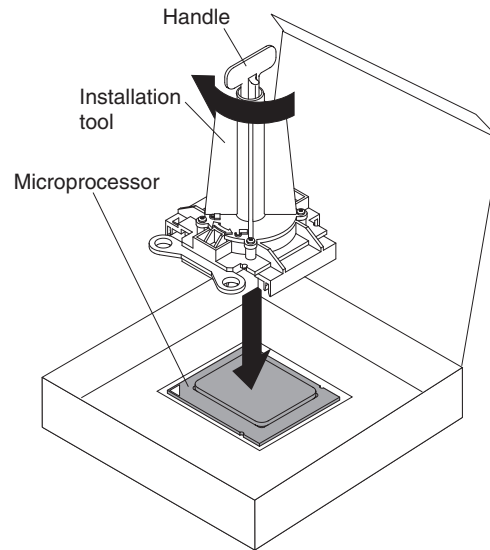
Figure 42. Aligning the microprocessor

4. If there is a plastic protective cover on the bottom of the microprocessor, carefully remove it.



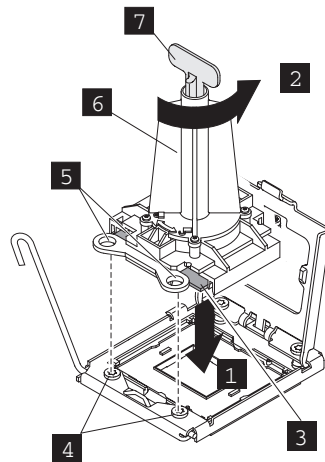
5. Locate the microprocessor installation tool that comes with the new microprocessor.
6. Twist the handle of the installation tool counterclockwise so that it is in the open position.
7. Align the triangle alignment mark on the microprocessor installation tool with the triangle alignment mark on the microprocessor, and then place the microprocessor on the underside of the tool so that the tool can grasp the microprocessor correctly.
8. Twist the handle of the installation tool clockwise to secure the microprocessor in the tool.

Note: You can pick up or release the microprocessor by twisting the microprocessor installation tool handle.



9. Carefully align the microprocessor installation tool over the microprocessor socket. Twist the handle of the microprocessor tool counterclockwise to insert the microprocessor into the socket.

Attention: The microprocessor fits only one way on the socket. You must place a microprocessor straight down on the socket to avoid damaging the pins on the socket. The pins on the socket are fragile. Any damage to the pins may require replacing the system board.



10. Close the microprocessor bracket frame.
11. Carefully close the microprocessor release lever to the closed position to secure the microprocessor in the socket.
12. Install a heat sink on the microprocessor.

Attention: Do not touch the thermal grease on the bottom of the heat sink or set down the heat sink after you remove the plastic cover. Touching the thermal grease will contaminate it.

Figure 43 on page 142 shows the bottom surface of the heat sink.

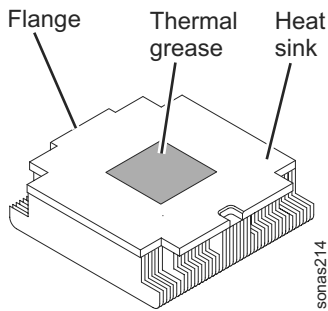


Figure 43. Bottom surface of the heat sink

13. Make sure that the heat-sink release lever is in the open position.
14. Remove the plastic protective cover from the bottom of the heat sink.
15. If the new heat sink did not come with thermal grease, you must apply thermal grease on the microprocessor before you install the heat sink, as described in “Thermal grease” on page 143.
16. Align the heat sink above the microprocessor with the thermal grease side down. See Figure 44.

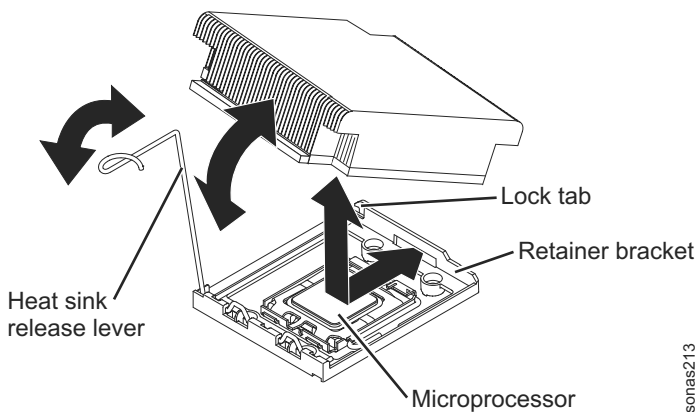


Figure 44. Aligning the heat sink above the microprocessor

17. Slide the flange of the heat sink into the opening in the retainer bracket.
18. Press down firmly on the heat sink until it is seated securely.
19. Rotate the heat-sink release lever to the closed position and hook it underneath the lock tab.
20. Replace the components that you removed in Removing a microprocessor and heat sink.
 - **Microprocessor 1:** DIMM air baffle and PCI riser card assembly 1, as described in “Installing the DIMM air baffle” on page 90 and “Installing a PCI riser-card assembly” on page 96.
 - **Microprocessor 2:** Microprocessor 2 air baffle and PCI riser card assembly 2, as described in “Installing the microprocessor 2 air baffle” on page 87 and “Installing a PCI riser-card assembly” on page 96.
21. Install the cover, as described in “Installing the cover” on page 80.
22. Slide the server into the rack.
23. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Thermal grease

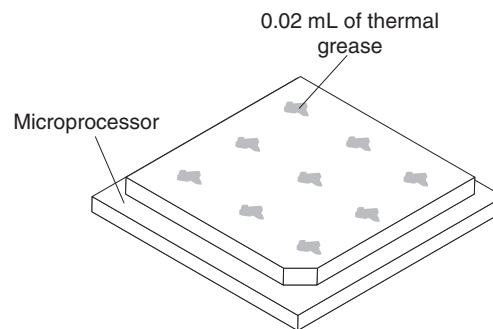
The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

To replace damaged or contaminated thermal grease on the microprocessor and heat exchanger, complete the following procedure.

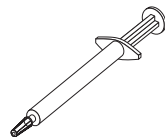
1. Place the heat sink assembly on a clean work surface.
2. Remove the cleaning pad from its package and unfold it completely.
3. Use the cleaning pad to wipe the thermal grease from the bottom of the heat exchanger.

Note: Make sure that all of the thermal grease is removed.

4. Use a clean area of the cleaning pad to wipe the thermal grease from the microprocessor; then, dispose of the cleaning pad after all of the thermal grease is removed.



5. Use the thermal-grease syringe to place nine uniformly spaced dots of 0.02 mL each on the top of the microprocessor.



Note: 0.01mL is one tick mark on the syringe. If the grease is properly applied, approximately half (0.22 mL) of the grease remains in the syringe.

6. Continue with step 9. of the "Installing a microprocessor and heat sink" on page 138 procedure.

Removing a heat-sink retention module

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

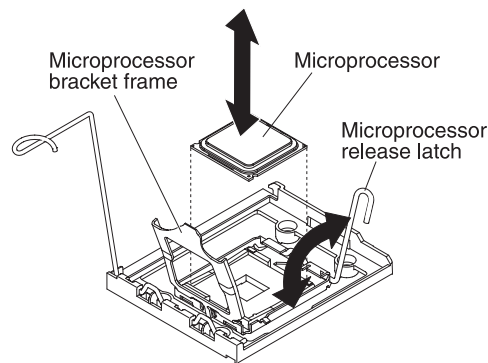
To remove a heat-sink retention module, complete the following steps:

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in "Safety" on page xi, "Safety statements" on page xiii, and "Installation guidelines" on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.

3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Depending on which microprocessor you are removing, remove the following components, if needed:
 - **Microprocessor 1:** PCI riser card assembly 1 and DIMM air baffle, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the DIMM air baffle” on page 89.

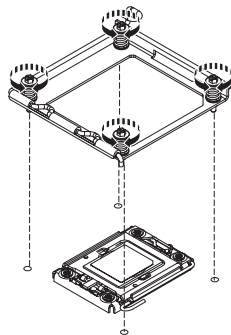
Note: If there are two microprocessors, you must remove PCI riser card assembly 2 and microprocessor 2 air baffle first, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the microprocessor 2 air baffle” on page 86.

- **Microprocessor 2:** PCI riser card assembly 2 and microprocessor 2 air baffle, as described in “Removing a PCI riser-card assembly” on page 95 and “Removing the microprocessor 2 air baffle” on page 86.



In the following step, keep each heat sink paired with its microprocessor for reinstallation.

6. Remove the heat sink and microprocessor, as described in “Removing a microprocessor and heat sink” on page 136.
7. Remove the four screws that secure the heat-sink retention module to the system board; then, lift the heat-sink retention module from the system board.



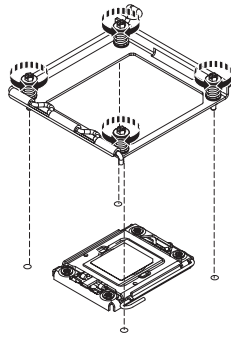
8. If you are instructed to return the heat-sink retention module, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing a heat-sink retention module

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

To install a heat-sink retention module, complete the following procedure.

1. Place the heat-sink retention module in the microprocessor location on the system board.



2. Install the four screws that secure the module to the system board.
Attention: Make sure that you install each heat sink with its paired microprocessor.
3. Install the microprocessor, heat sink, and applicable air baffle, as described in *Installing a microprocessor and heat sink*.
4. Install the cover, as described in *“Installing the cover”* on page 80.
5. Slide the file module into the rack.
6. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

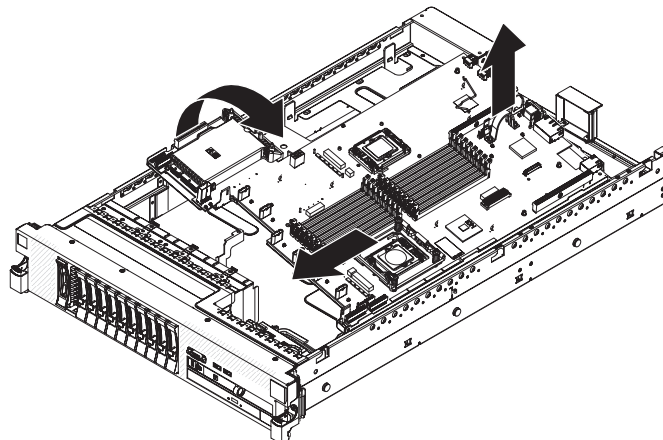
Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

Removing the system board

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

Note: When you replace the system board, you must either update the server with the latest firmware or restore the pre-existing firmware that the customer provides on a diskette or CD image. Make sure that you have the latest firmware or a copy of the pre-existing firmware before you proceed.

To remove the system board, complete the following steps.



1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. To query and record the PCI slot settings prior to removing the system board so that you can reapply the settings after the replacement, use the following Advanced Settings Utility (ASU) command:

```
# asu show all --kcs | grep uEFI.PCIeGenSelection
uEFI.PCIeGenSelection.1=Gen2
uEFI.PCIeGenSelection.10=Gen2
uEFI.PCIeGenSelection.11=Gen2
uEFI.PCIeGenSelection.12=Gen2
uEFI.PCIeGenSelection.13=Gen2
uEFI.PCIeGenSelection.14=Gen2
uEFI.PCIeGenSelection.15=Gen2
uEFI.PCIeGenSelection.16=Gen2
uEFI.PCIeGenSelection.2=Gen1
uEFI.PCIeGenSelection.3=Gen2
uEFI.PCIeGenSelection.4=Gen2
uEFI.PCIeGenSelection.5=Gen2
uEFI.PCIeGenSelection.6=Gen2
uEFI.PCIeGenSelection.7=Gen2
uEFI.PCIeGenSelection.8=Gen2
uEFI.PCIeGenSelection.9=Gen2
```

Some of the PCI slots might be set to the *Gen1* value instead of the default *Gen2* value. To reuse the same card in that slot, you must change the setting of the new system board in the replacement procedure.

3. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
4. Pull the power supplies out of the rear of the server; just enough to disengage them from the server.
5. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
6. Remove the cover, as described in “Removing the cover” on page 79.
7. Remove the PCI riser-card assembly that contains the adapter, as described in “Removing a PCI riser-card assembly” on page 95.
 - If you are removing an adapter from PCI expansion slot 1 or 2, remove PCI riser-card assembly 1.
 - If you are removing an adapter from PCI expansion slot 3 or 4, remove PCI riser-card assembly 2.
8. Remove the SAS controller assembly, which includes the SAS riser card, from the server, as described in “Removing the SAS riser-card and controller assembly” on page 107.
9. If an Ethernet daughter card is installed in the server, remove it.
10. If a virtual media key is installed in the server, remove it, as described in “Removing the IBM virtual media key” on page 93.
11. Remove the DIMM air baffle, as described in “Removing the DIMM air baffle” on page 89.
12. Remove the microprocessor 2 air baffle, as described in “Removing the microprocessor 2 air baffle” on page 86.
13. Remove all DIMMs, and place them on a static-protective surface for reinstallation, as described in “Removing a memory module” on page 126.

Important: Note which DIMMs are in which connectors, before you remove the DIMMs. You must install them in the same configuration on the replacement system board.

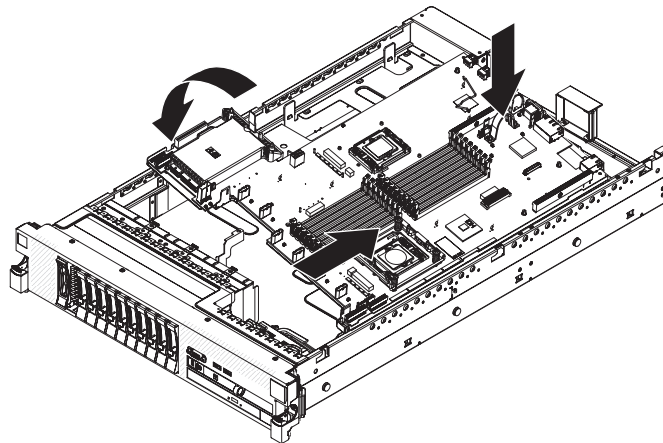
14. Remove the fans, as described in “Removing a hot-swap fan” on page 129.
15. Remove the fan bracket, as described in “Removing the fan bracket” on page 91.
16. Disconnect all cables from the system board.
Attention: In the following step, do not allow the thermal grease to come in contact with anything, and keep each heat sink paired with its microprocessor for reinstallation. Contact with any surface can compromise the thermal grease and the microprocessor socket; a mismatch between the microprocessor and its original heat sink can require the installation of a new heat sink instead.
17. Remove each microprocessor heat sink and microprocessor; then, place them on a static-protective surface for reinstallation, as described in “Removing a microprocessor and heat sink” on page 136.
18. Push in and lift up the two system board release latches on either side of the fan cage.
19. Slide the system board forward and tilt it away from the power supplies. Using the lift handle, pull the system board out of the server.
20. If you are instructed to return the system board, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the system board

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

You must remove and replace the microprocessors when you replace the system board. Ensure that you have alcohol wipes (part number 59P4739) and thermal grease (part number 41Y9292) available to correctly perform this task. If you do not already have the parts, order them separately.

To reinstall the system board, complete the following steps.



1. Install the Ethernet daughter card.
2. Align the system board as tilted shown, then rotate and lower it flat and slide it back toward the rear of the server.
3. Reconnect to the system board the cables that you disconnected in step 16 of “Removing the system board” on page 145.

When you reassemble the components in the server, route all cables carefully so that they are not exposed to excessive pressure.

4. Rotate the system board release latch toward the rear of the server until the latch clicks into place.
5. Replace the fans, as described in “Installing a hot-swap fan” on page 130.
6. Install each microprocessor with its matching heat sink, as described in “Installing a microprocessor and heat sink” on page 138.
This procedure describes how to remove the old thermal grease and apply a new coat of grease.
7. Install the DIMMs, as described in “Installing a memory module” on page 126.
8. Install the air baffles, as described in “Installing the DIMM air baffle” on page 90 and “Removing the microprocessor 2 air baffle” on page 86.
9. Install the SAS riser-card and controller assembly, as described in “Installing the SAS riser card and controller assembly” on page 109.
10. Install the PCI riser-card assemblies and all adapters, as described in “Installing a PCI riser-card assembly” on page 96.
11. Install the cover, as described in “Installing the cover” on page 80.
12. Push the power supplies back into the server.
13. Slide the file module into the rack.
14. Reconnect the external cables; then, reconnect the power cords and turn on the peripheral devices and the file module.

Note: You must wait approximately 2.5 minutes after you connect the power cord of the file module to an electrical outlet before the power-control button becomes active.

15. When you replace the system board, update the server firmware, as described in “Restoring System x firmware (BIOS) settings” on page 254.
16. From the active management file module terminal application, issue the following Advanced Settings Utility (ASU) commands to reset the serial number and the product name of the new system board:

```
asu set SYSTEM_PROD_DATA.SysInfoSerialNum KQ3497D --host int002st001
asu set SYSTEM_PROD_DATA.SysInfoProdName 7947PCV --host int002st001
```

Replace *KQ3497D* with the serial number of the file module.

Replace *int002st001* with the host name or IP address of the file module with the new motherboard.

Replace *7947PCV* with the system type of the file module.

17. From the active management file module terminal application, use the Advanced Settings Utility (ASU) to verify the settings for the PCI slots in the interface file module.

For example, when replacing the system board on the *int002st001* interface file module, query the PCI slot settings:

```
# asu show all --kcs | grep uEFI.PCIeGenSelection
uEFI.PCIeGenSelection.1=Gen2
uEFI.PCIeGenSelection.10=Gen2
uEFI.PCIeGenSelection.11=Gen2
uEFI.PCIeGenSelection.12=Gen2
uEFI.PCIeGenSelection.13=Gen2
uEFI.PCIeGenSelection.14=Gen2
uEFI.PCIeGenSelection.15=Gen2
uEFI.PCIeGenSelection.16=Gen2
uEFI.PCIeGenSelection.2=Gen2
uEFI.PCIeGenSelection.3=Gen2
uEFI.PCIeGenSelection.4=Gen2
uEFI.PCIeGenSelection.5=Gen2
```

```
uEFI.PCIeGenSelection.6=Gen2
uEFI.PCIeGenSelection.7=Gen2
uEFI.PCIeGenSelection.8=Gen2
uEFI.PCIeGenSelection.9=Gen2
```

By default, all PCI slots on the system board are set to *Gen2* in the replacement system board.

A problem might arise when an older adapter is not recognized at the power-on self test (POST) because the adapter requires a *Gen1* setting.

To set the slots on the new system board just as the slots were set on the original system board and avoid such a problem, use the settings information that you recorded before removing the system board.

To change the appropriate settings from *Gen2* to *Gen1*, use the ASU. For example, if slot 2 must be *Gen1* on the *int002st001imm* file module, issue the following command from the active management file module terminal application:

```
asu set uEFI.PCIeGenSelection.2 Gen1 --host int002st001imm
```

Tip: To query and set such options while the file module is powered off, use the host name for the Integrated Management Module (IMM), which in this example is *int002st001imm* instead of the IP host name of *int002st001*.

If the file module requires modification of the uEFI.PCIeGenSelection settings, you must reboot the file module for the new settings to take effect.

18. Once the system has finished booting, complete the following two steps:

- a. Discover the IMM IP setting by running the following command:

```
gethostip (#NODENAME)imm
```

For example, if file module 4 had its system board replaced, the command would be **gethostip int004st001imm**.

- b. Reconfigure the IMM network setting by running the following command:

```
sonas_ipcfg --setip --adapter=sm --dhcp=no --ip=#IP_NUM
--netmask=255.255.128.0
```

where *IP_NUM* is the IP number obtained in the previous step.

Removing the 240 VA safety cover

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

To remove the 240 VA safety cover, perform the following steps:

1. To help you work safely with Storwize V7000 Unified file modules, read the safety information in “Safety” on page xi, “Safety statements” on page xiii, and “Installation guidelines” on page 50.
2. Turn off the file module and peripheral devices, then label and disconnect both power cords and all external cables.
3. Press down on the left and right side latches and pull the server out of the rack enclosure until both slide rails lock.
4. Remove the cover, as described in “Removing the cover” on page 79.
5. Remove the SAS riser-card assembly. See Removing the SAS riser-card and controller assembly.
6. Remove the screw from the safety cover. See Figure 45 on page 150.

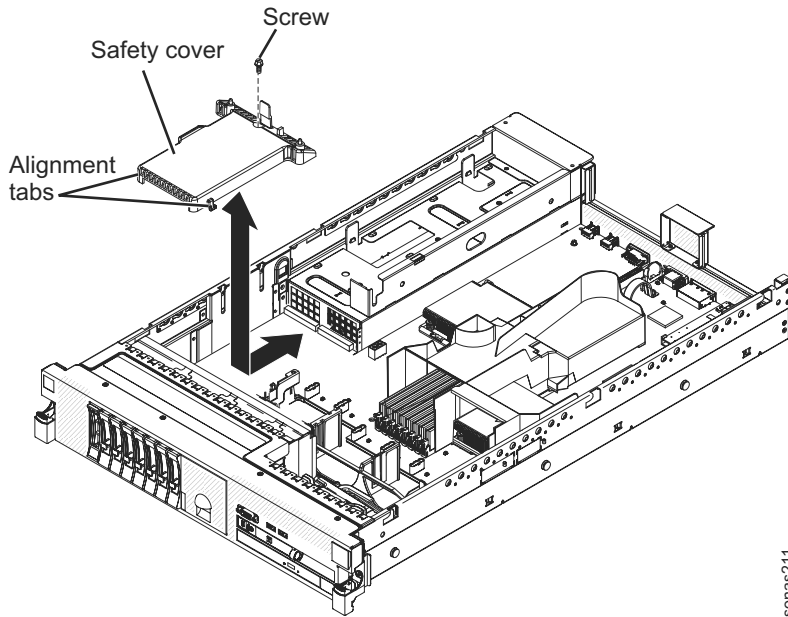


Figure 45. 240 VA safety cover

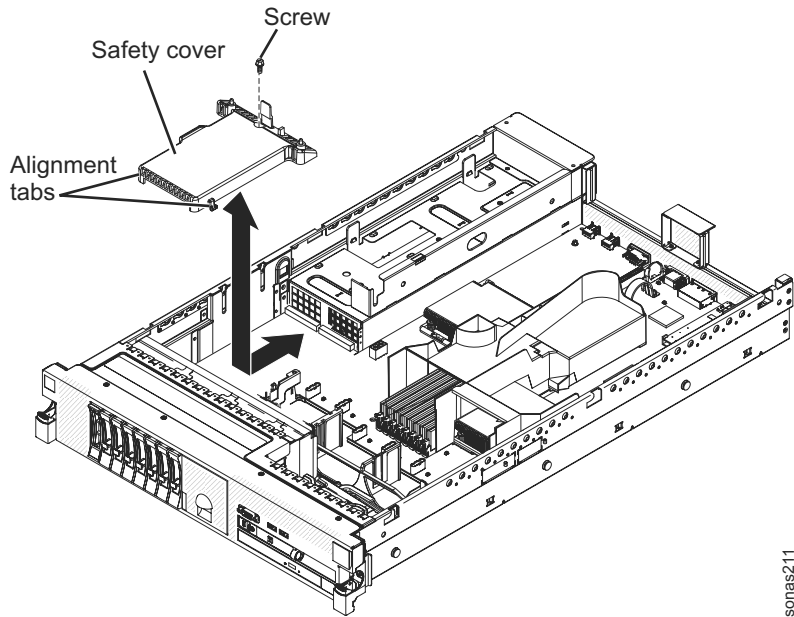
7. Disconnect the hard disk drive backplane power cables from the connector in front of the safety cover.
8. Slide the cover forward to disengage it from the system board, and then lift it out of the server.
9. If you are instructed to return the 240 VA safety cover, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Installing the 240 VA safety cover

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

To install the 240 VA safety cover, perform the following steps:

1. Line up and insert the tabs on the bottom of the safety cover into the slots on the system board. See Figure 46 on page 151.



sonas211

Figure 46. 240 VA safety cover

2. Slide the safety cover toward the back of the server until it is secure.
3. Connect the hard disk drive backplane power cables to the connector in front of the safety cover.
4. Install the screw into the safety cover.
5. Install the SAS riser-card assembly.
6. Install the server cover.
7. Slide the server into the rack.
8. Reconnect the external cables, then reconnect the power cords and turn on the peripheral devices and the server.

Setting the machine type, model, and serial number

The following procedure is for a field replaceable unit (FRU). FRUs must be installed only by trained service technicians.

The ASU package is part of the Storwize V7000 Unified code. ASU is available to authorized service personnel from the command-line interface (CLI) on the file module. Use ASU to modify selected settings in the integrated-management-module (IMM)-based Storwize V7000 Unified file modules.

You can use the ASU remotely from your laptop (if allowed) or from a file module that has Storwize V7000 Unified installed.

1. Access and log in to the Storwize V7000 Unified system from the CLI.
2. Issue the following command to view the current settings for the machine type and model:

```
asu show SYSTEM_PROD_DATA.SysInfoProdName
```

3. Issue the ASU command on the Storwize V7000 Unified file module to set the machine type and model:

```
asu set SYSTEM_PROD_DATA.SysInfoProdName 2073-700
```

4. Issue the following command to verify that you set the machine type and model number correctly:

```
asu show SYSTEM_PROD_DATA.SysInfoProdName
```

5. Issue the following command to view the current setting of the serial number:

```
asu show SYSTEM_PROD_DATA.SysInfoSerialNum
```
6. Issue the following ASU command on the Storwize V7000 Unified node to set the serial number:

```
asu set SYSTEM_PROD_DATA.SysInfoSerialNum xxxxx
```

The variable *xxxxx* in the command stands for the serial number.
7. Issue the following command to verify that you set the serial number correctly:

```
asu show SYSTEM_PROD_DATA.SysInfoSerialNum
```

File module software problems

This section helps you to identify and resolve file module software problems.

Logical devices and physical port locations

Use this table to help identify logical devices, file module roles used, and physical locations.

Table 35. Storwize V7000 Unified logical devices and physical port locations

Logical Ethernet device name	Device description	Physical location information
mgmtsl0_0	Internal connection between the file modules	Port 1 - Built-In xSeries Ethernet Port
mgmtsl0_1	Internal connection between the file modules	Port 2 - Built-In xSeries Ethernet Port
ethXsl0_0	1 Gbps Customer Network	Port 3 - Built-In xSeries Ethernet Port
ethXsl0_1	1 Gbps Customer Network	Port 4 - Built-In xSeries Ethernet Port
ethXsl1_0	10 Gbps customer network	Port 1 / 10GbE Converged Network Adapter
ethXsl1_1	10 Gbps customer network	Port 2 / 10GbE Converged Network Adapter

Management node role failover procedures

The following procedures either restart the management service or initiate a management service failover from the file module hosting the active management node role to the file module hosting the passive management node role.

Once complete, the file module that previously hosted the active management node role now hosts the passive management node role. The file module that previously hosted the passive management node role now hosts the active management node role.

Note: All of these tasks require a user that is configured as a CLI admin. Other users cannot perform these tasks.

Determining the service IP for the management node roles

Use this procedure to identify the service IP addresses for the file modules that host the management node roles.

You need the service IP address of a file module that hosts a management node role to perform a management failover from the file module that hosts the active management node role to the file module that hosts the passive management node role, when the active management node fails and the current management IP does not respond.

1. Attempt to open an SSH connection to the root IP of one of the file modules hosting a management node role.

Note: Run the CLI command **lsnode**.

- If you get output from **lsnode** that shows the system configuration (as in Example 1), proceed to step 2.
- If you get a message that the management service is stopped or is not running (as in Example 2), attempt to log out and log in to the other file module hosting a management node role. If the other file module is not responding, refer to “Management node role failover procedures for failure conditions” on page 154.

Example 1: System configuration output from **lsnode** displays similar to the following example:

```
[root@kq186wx.mgmt001st001 ~]# lsnode
Hostname IP Description Role
mgmt001st001 172.31.8.2 active management node management,interface,storage
mgmt002st001 172.31.8.3 passive management node management,interface,storage

Product version Connection status GPFS status CTDB status Last updated
1.3.0.0-50a OK active active 8/30/11 8:36 PM
1.3.0.0-50a OK active active 8/30/11 8:36 PM

EFSSG1000I The command completed successfully.
[root@kq186wx.mgmt001st001 ~]#
```

Example 2: Output for **lsnode** for a management service that is not running is similar to the following example:

```
[root@kq186wx.mgmt002st001 ~]# lsnode
EFSSG0026I Cannot execute commands because Management Service is stopped.
Use startmgtsrv to restart the service.
```

2. Determine the service IP addresses for the file modules hosting a management node role by running the CLI command **lsnwmgt**. Output that is similar to the following example is displayed:

```
[root@kq186wx.mgmt001st001 ~]# lsnwmgt
Interface Service IP Node1 Service IP Node2
ethX0 9.11.137.128 9.11.137.129

Management IP Network Gateway VLAN ID
9.11.137.127 255.255.254.0 9.11.136.1
EFSSG1000I The command completed successfully.
```

The following table describes the nodes that are identified by the command:

Table 36. Hostname and service IP reference

Host name	Corresponding Service IP reference
mgmt001st001	Service IP Node1
mgmt002st001	Service IP Node2

Performing management node role failover on a “good” system

Use this procedure to complete a failover process when both file modules appear to be operating correctly.

If both file modules are operating correctly with regard to management services, perform the following procedure to failover the active management node to the passive management node.

1. Open an SSH connection to the service IP of the file module hosting the passive management node role.
Refer to “Determining the service IP for the management node roles” on page 152, if necessary.
2. To initiate the management services on the passive node and perform the switchover from the active management node, run the **startmgtsrv** command.

Note: If you run the **startmgtsrv** command from the node that is becoming active, you first need to run the **setcluster** command to set the cluster environment variable. If you see the following error message when running the command, wait until the initialization has completed before running **setcluster** again:

```
IBM SONAS management service is starting up
EFSSG0654I The Management Service is starting up.
```

After you run the **startmgtsrv** command, the system displays information that is similar to the following example:

```
[yourlogon@yourmachine.mgmt002st001 ~]# startmgtsrv
Other node is reachable and its management state is active.
Are you sure? (Y/N)Y
EFSSG0717I Takeover initiated by root - this may take a few minutes
EFSSG0544I Takeover of the management functions from the active
node was successful
```

Once complete, the file module that previously hosted the active management node role now hosts the passive management node role. The file module that previously hosted the passive management node role now hosts the active management node role.

Management node role failover procedures for failure conditions

Use this topic to isolate and perform file module failover for failed conditions.

“Failed conditions” exist when the active management node has failed and is not responding. This failure is exposed by the inability to access the file module, run CLI commands, and/or access the GUI.

Note: If the management IP is accessible and you can establish an SSH connection and run CLI tasks, do not perform a management failover. Refer to .

Complete the following procedure to address this issue.

Important: Performing this procedure does not repair a problem that caused the current system condition. This procedure provides for system access and troubleshooting to restart the management services or to failover the management service from a failed file module to the passive management node on the other file module. Once you complete this procedure, follow the appropriate troubleshooting documentation to isolate and repair the core problem that caused this condition.

1. Attempt to open an SSH connection to the service IP of the file module with the active management node role. Refer to . Was the connection successful?
 - **Yes** - proceed to step 2
 - **No** - proceed to step 5 on page 155
2. If the connection is successful, verify that the management service is not running by executing the CLI command **lsnode** and then reviewing the output.
 - If the system responds with output for the **lsnode** command, then the management services are already running. If you still cannot access the GUI, refer to . If the GUI is accessible, then the management services are properly running on the active management node and no failover is needed. If you want to initiate a failover, refer to “Performing management node role failover on a “good” system” on page 153.
 - If the system responds that the management service is not running, proceed to the next step.

Note: For a management service that is not running, the system displays information similar to the following example:

```
[yourlogon@yourmachine.mgmt002st001 ~]# lsnode
EFSSG0026I Cannot execute commands because Management Service is stopped.
Use startmgtsrv to restart the service.
```

3. Attempt to stop and restart the management services. Wait for the commands to complete.
 - a. Run the CLI command **stopmgtsrv**.
 - b. Run the CLI command **startmgtsrv**. This restarts the management services.
4. Once command execution is complete:
 - a. Verify that the management service is running by again executing the CLI command **lsnode**. If the system responds that the management service is not running, proceed to step 5.
 - b. If the **lsnode** output provides system configuration information, verify that you can access and log in to the GUI. If you still have trouble with accessing the GUI, refer to .
 - c. If the problem appears to be resolved, DO NOT perform steps 5-9. Instead, using the GUI event log, follow the troubleshooting documentation to isolate the software or hardware problem that might have caused this issue.

Attention: Perform the following steps only if the active management node is not responding properly. These steps initiate a startup and failover of the management services on the file module hosting the passive management node role.

5. Open an SSH connection to the service IP and port of the file module with the passive management node role. Refer to “Determining the service IP for the management node roles” on page 152.
6. Verify the management service status by running the CLI command **lsnode**. If the file module responds that the management service is not running, proceed to the next step.
7. Run the CLI command **startmgtsrv**. This starts the management services on the passive node.
8. Once command execution is complete:
 - a. Verify that the management service is running by again executing the CLI command **lsnode**.
 - b. If the **lsnode** output provides system configuration information, verify that you can access and log in to the GUI. If you still have trouble with accessing the GUI, refer to .
 - c. If the **lsnode** output reports that the management service is still not running, contact IBM support.
9. Using the GUI event log, follow the troubleshooting documentation against the file module with the failed management node role to isolate the software or hardware problem that might have caused this issue.

Checking CTDB health

Use this information for checking system health with the clustered trivial database (CTDB).

CTDB checks the health status of the Storwize V7000 Unified file modules, scanning elements such as storage access, General Parallel File System (GPFS), networking, Common Internet File System (CIFS), and Network File System (NFS).

An unhealthy file module cannot serve public Internet Protocol (IP) addresses and must be fixed. However, the high availability features of the Storwize V7000 Unified system can mask the unhealthy status from its clients by failing over IP addresses from an unhealthy file module to a healthy file module.

If your file modules are in an unhealthy state, your clients lose IP access. In the management graphical user interface (GUI), select **Monitoring > System** and check the health status for errors and degraded events.

To check the status using either the GUI or the command-line interface (CLI), complete this procedure:

1. To check the CTDB status:
 - With the Storwize V7000 Unified GUI, use the following method:
 - Select **Monitoring > System Details > Interface Nodes > mgmt001st001 > NAS Services**. In the **CTDB state** row, a healthy status is displayed as “Active” and an unhealthy status is displayed as “unhealthy”.
 - Review the status of both file modules, **1** mgmt001st001 and **2** mgmt002st001, as shown in Figure 47.

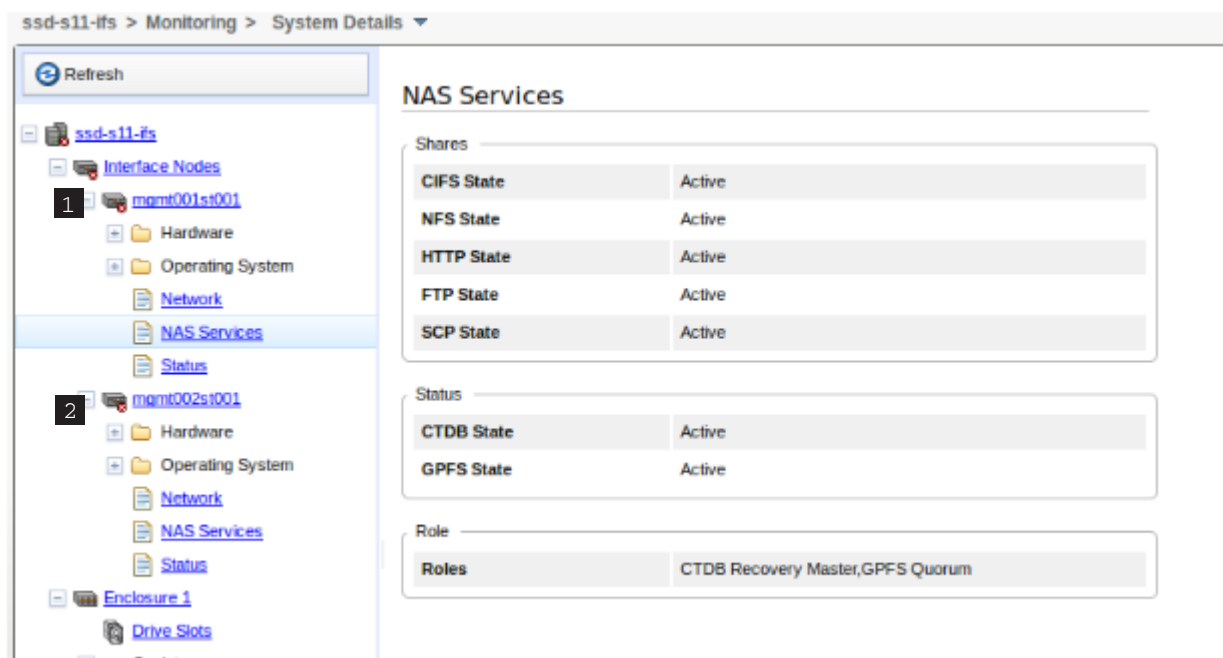


Figure 47. Management GUI showing CTDB status for both file modules

- With the CLI, log in as an admin user, then open the CLI and issue the **lnode -r** command to determine whether CTDB is active on all nodes.

The system displays information similar to the following:

```
[yourlagon@yourmachine]$ lnode -r
EFSSG0015I Refreshing data.
Hostname      IP      Description      Role
mgmt001st001 10.254.8.2 active management node management,interface,storage
mgmt002st001 10.254.8.3 passive management node management,interface,storage

Product version Connection status GPFS status CTDB status Last updated
1.3.0.0-55c      OK      active active
1.3.0.0-55c      OK      active unhealthy
EFSSG1000I The command completed successfully.
```

In the CTDB Status column, “active” indicates a healthy status and “unhealthy” indicates an error status.

2. If the CTDB status for a file module is “unhealthy”, perform one or more of the following procedures:
 - Review the health status for any potential network problems. A network failure between a file module and the customer can result in an “UNHEALTHY” CTDB status. Follow the appropriate error code action plans to resolve the network problems. Refer to “Checking network interface availability” on page 161.
 - If the network has been isolated without any problems being identified, perform the procedures in “Checking the GPFS file system mount on each file module.”
 - Refer to the information in “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center* to determine if any additional hardware problems might be causing the “unhealthy” CTDB status.
 - Perform a reboot of the unhealthy file module. Refer to “Resuming services on a suspended file module” in the *IBM Storwize V7000 Unified Information Center*.
 - If none of the above actions resolves the problem, contact your next level of support.

Checking the GPFS file system mount on each file module

Use this information to identify and resolve problems with General Parallel File System (GPFS) file system mounts on IBM Storwize V7000 Unified file modules.

One of the reasons that clustered trivial database (CTDB) status can be reported as “UNHEALTHY” is from having a GPFS file system that is not mounted on a Storwize V7000 Unified file module. The GPFS file system must be mounted on file modules in the Storwize V7000 Unified product to support dual redundancy and to allow file input/output through all public IP addresses.

To identify the CTDB status, see “Checking CTDB health” on page 155.

- To identify all of the currently created file systems on the Storwize V7000 Unified system, or on each file module, perform the procedure in “Identifying created and mounted file system mounts.”
- To resolve problems with mounted file systems that are missing, perform the procedure in “Resolving problems with missing mounted file systems” on page 158.
- To resolve problems with stale NFS file systems, perform the procedure in “Resolving stale NFS file systems” on page 159.
- To resolve problems that are not covered by the information presented in the previous topics, perform the procedure in “Recovering a GPFS file system” on page 162.

Identifying created and mounted file system mounts

You can identify and resolve problems in GPFS file system mounts on the Storwize V7000 Unified system and file modules.

To identify and resolve problems in file system mounts, perform this procedure:

1. To identify all the currently created file systems on the Storwize V7000 Unified system, log in as the admin user, then enter the **lsfs -r** command from the command-line interface (CLI), as shown in the following example:

```
# lsfs -r
EFSSG0015I Refreshing data.
Cluster   Device name Quota           Def. quota Block size Inodes
kd18pz5.ibm gpfs1       user;group;fileset 256 kB     11373

Replication Dmapi Block allocation type Last update
none        yes  scatter                10/3/11 2:08 PM

EFSSG1000I The command completed successfully.
```

- To identify the currently created file systems on each Storwize V7000 Unified file module, log in as the root user on the active management node, then enter the **onnode -n mgmt001st001 df | grep ibm** command from the CLI, as shown in the following example:

```
# onnode -n mgmt001st001 df | grep ibm

/dev/gpfs1      3221225472 4590080 3216635392 1% /ibm/gpfs1
```

Repeat the command for another file module by running the **onnode -n mgmt002st001 df | grep ibm** command, for example:

```
# onnode -n mgmt002st001 df | grep ibm

/dev/gpfs1      3221225472 4590080 3216635392 1% /ibm/gpfs1
```

Resolving problems with missing mounted file systems

You can resolve problems with mounted file systems that are missing on Storwize V7000 Unified file modules.

Display the file system by using the **lsfs -r** command. The **lsmount -r -v** command shows which file modules mount the file system. The Mounted status means that both file modules mount the file system. All other states, Partially, Internally, or Not mounted mean that a file system is not properly mounted.

To resolve the problem with the missing mounted file system, perform the following procedure:

- Log in to the Storwize V7000 Unified CLI as admin.
- Identify on which file module the file system is missing, for example, mgmt001st001.
- Attempt to mount the missing file system on the file module by using the **mountfs** command.


```
mountfs gpfs0
```
- Rerun the **lsmount** command to verify that all file systems are now mounted on file modules 0 and 1.
- If the mounted file systems are not consistent across the file modules, reboot the file module on which a file system is missing, and then rerun the **lsmount** command.

Reboot the file module by using the **initnode** command:

```
initnode -r -n mgmt001st001
```

If they are not mounted on either file module, then reboot each file module.

- Use the **lsnode** command to determine when the file modules are back up and when GPFS and CTDB are both active.

The file systems might take several minutes to get mounted after GPFS becomes active on both file modules. More than one reboot might be required to bring the file system back up. Allow time between reboots because the file system might take some time before it comes back up after a reboot.

- Verify that the CTDB status is now shown as **active** on both file modules, as described in “Checking CTDB health” on page 155.

8. If a GPFS file system fails to mount, complete the following actions:
 - a. Check the output log of the **lslog** command and find the latest messages for mounting the file system.

If you find input/output errors and messages about a failure to read the super block, the problem is with the DMAPi clients of the TSM/HSM system.

Check for disk related problems, such as errors reading from a disk or errors showing a non-existent disk. For these errors, check that the path to the storage system is working and, if it is, that the storage system itself is in working order.
 - b. For additional information, refer to the “Diagnostics: Troubleshooting tables” information in “Troubleshooting the System x3650” in the *IBM Storwize V7000 Unified Information Center*.
 - c. If file systems remain unmounted, contact IBM support.

Resolving stale NFS file systems

You can resolve problems with stale NFS file systems on Storwize V7000 Unified file modules. A file module might have the file system mounted, but the file system remains inaccessible due to a stale NFS file handle.

To identify and resolve stale file handle problems, perform this procedure:

1. To identify stale NFS file handle problems, log in as the root user to the active management node, then enter the **onnode all df | grep NFS** command:

```
# onnode all df | grep NFS

df: `/ibm/gpfs0': Stale NFS file handle
```
2. If the command reports a stale NFS file handle on a particular file system, see “Working with file modules that report a stale NFS file handle” on page 254 for instructions on file system recovery.

Checking user and server authentication issues

Issues with logging on as a user or a lack of connection between servers might be tied to authentication problems.

With regard to user authentication issues, if you are sure that you have used the correct logon ID and password, your user account might have been deleted or corrupted.

Refer to these topics in the *IBM Storwize V7000 Unified Information Center* “Planning for user authentication”, “Verifying the authentication configuration”, “Establishing user and group mapping for client access”, and “chkauth”.

If you cannot resolve the issue, contact your authentication server administrator to validate or reestablish your account.

With regard to server configuration issues, refer to “Managing authentication server integration” and the authentication topics available there.

Error for “Missing SRV record in DNS”

If you encounter a “Missing SRV record in DNS” error similar to the following when configuring the active directory (AD) with the **cfgad** command, verify that

entries for DNS Domain Name, DNS Server, and DNS Search Domains are correct. Also, verify that the DNS server has valid SRV records for that domain.

```
$ cfgad -s 9.9.9.9 -u admin -p ****
(1/9) Fetching the list of cluster file modules.
(2/9) Check if cfgcluster has done the basic configuration successfully.
(3/9) Check whether file modules are
reachable from management file module.
(4/9) Detection of AD server and fetching domain information from AD server.
Missing SRV record in DNS : _ldap._tcp.xxxxx.COM
Missing SRV record in DNS : _ldap._tcp.dc._msdcs.xxxxx.COM
Missing SRV record in DNS : _kerberos._tcp.xxxxx.COM
Missing SRV record in DNS : _kerberos._tcp.dc._msdcs.xxxxx.COM
Necessary DNS entries are missing, the domain join step might fail.
(5/9) Check whether AD server is reachable
from file modules.
(6/9) Joining the domain of the specified ADS.
EFSSG0110C Configure AD failed on cluster. Cause: Error encountered while
executing netjoinAD.sh. Output till failure is :Join to Active Directory
domain with user Administrator
Failed to join domain: failed to find DC for domain SONAS
Error occurred due to reason : Join to Active Directory domain failed
```

If “netgroup” functionality with NIS is not working

If “netgroup” functionality with Network Information Service (NIS) is not working, ensure that you have included a “@” in front of the netgroup name, as shown in the following example:

```
$ mkexport testnetgrp5 /ibm/gpfs0/netgroup5 --nfs "@ng1(rw,no_root_squash)"
```

Do not create a netgroup with an IP address; instead, use a hostname. The hostname that is defined in a netgroup should resolve to a valid IP that points back to the same hostname when you query for it.

Possible client misconfiguration

Authentication problems might be due to a misconfiguration at the NAS client side. To verify, run the **lookupname** command as shown in the following example on all the file modules to check if they can authenticate with the authentication server.

```
$ lookupname --user SONAS\\userr
USER      GROUP
SONAS\\userr SONAS\\domain users
EFSSG1000I The command completed successfully.
```

```
$ chkauth -i -u SONAS\\userr
Command_Output_Data  UID      GID      Home_Directory      Template_Shell
FETCH USER INFO SUCCEED 12004360 12000513 /var/opt/IBM/sofs/scproot /usr/bin/rssh
EFSSG1000I The command completed successfully.
```

When the system unable to authenticate against an external authentication server, you need to make sure that it can obtain user information from the authentication server. For this user information, query commands can be run from the file modules. For example, in the case of the LDAP authentication server, you can run a command as shown in the following example:

```
$ chkauth -a -u SONAS\\userr -p *****
AUTHENTICATE USER SUCCEED
EFSSG1000I The command completed successfully.
```

Checking client access

Make sure your client is able to ping the full hostname of the cluster and all of the IP addresses associated with it.

The example here shows how to ping a cluster. When the client connects to the hostname of the cluster, the DNS server answers with IP addresses. You then ping each IP address from the client machine.

If clients cannot ping the IP addresses, they are not able to access Storwize V7000 Unified whenever the DNS returns the IP address on name resolution requests. This can lead to situations where some clients have access while others do not.

1. Ping your Storwize V7000 Unified cluster by using the **nslookup** command—this non-disruptive command requires “root” access—and your domain name. .

Information similar to the following example is displayed:

```
# nslookup yourdomainname
Server:          9.11.136.116
Address:         9.11.136.116#53
```

```
Non-authoritative answer:
Name:   yourdomainname
Address: 129.42.16.103
Name:   yourdomainname
Address: 129.42.17.103
Name:   yourdomainname
Address: 129.42.18.103
```

The system returns the public IP addresses, for example, 129.42.18.103 above, that are served by the Storwize V7000 Unified cluster.

2. Ping each IP address listed in the output by issuing **ping returned IP Address**. A successful return indicates a working connection. A response of “Request timed out” indicates a failed connection.

Note: If clients cannot ping the IP addresses, refer to “Checking network interface availability.”

3. If you have a failed connection, contact your system administrator or your next level of support.

Checking network interface availability

You have several options for checking network availability by using the Storwize V7000 Unified GUI or the CLI.

1. In the Gui, select **Monitoring > System Details > mgmt00xst001 > Operating System > Network**.
2. In the CLI, check the status of the interface “ethX0” (the interface of nodes to the customer net).
 - a. Open the CLI.
 - b. Use the **lswinterface** command to display the status for the desired IPs.

```
# lswinterface
```

The system displays information similar to the following example:

Node	Interface	MAC	Master/Subordinate	Bonding mode
mgmt001st001	ethX0	e4:1f:13:d6:ae:ac	MASTER	balance-alb (6)
mgmt001st001	ethX1	00:c0:dd:17:bc:ac	MASTER	active-backup (1)

```

mgmt002st001 ethX0    e4:1f:13:d6:ae:94 MASTER          balance-a1b (6)
mgmt002st001 ethX1    00:c0:dd:17:c5:50 MASTER          active-backup (1)

```

```

Up/Down Speed IP-Addresses      MTU
UP      1000
UP      10000 9.11.84.84,9.11.84.85 1500
UP      1000
UP      10000 9.11.84.82,9.11.84.83 1500
EFSSG1000I The command completed successfully.

```

In the **Up/Down** column, “UP” indicates a connection.

3. If you find that the network interface is not available, perform a visual inspection of the cabling to ensure that it is plugged in. For instance, if you have no machine connectivity between nodes and switches, check the external Ethernet cabling. If the cabling is all good, you then need to work upstream, checking Intranet availability, for example, or external Internet availability. If none of these checks leads to a resolution of the problem, contact your next level of support.

Recovering a GPFS file system

Use this procedure to recover a GPFS file system after a storage system failure has been fully addressed.

Prerequisites:

- You are executing this procedure on a file module.
- You are logged into the management CLI as root. See “Accessing a file module as root” on page 251.

For storage system recovery, see the procedure for recovering a storage system.

This procedure provides steps to recover a GPFS file system after a failure of the storage system. The file volumes were offline and are now back online after a repair or recovery action. The disks referred to in this procedure are the volumes that are provided by the storage system.

Note: Because no I/O can be done by GPFS, it is assumed for these procedures that the storage unit failure caused the GPFS file system to unmount. After satisfying the prerequisites above, take the following steps:

1. Verify that GPFS is running on both file modules by using the **lsnode -r** command.
The column **GPFS state** shows active.
2. With GPFS functioning normally on both file modules, ensure that all disks in the file system are available by running the **lsdisk -r** command. The **Availability** column shows Up.
3. Run the **chkfs file_system_name -v** command to capture the output to a file. Review the output file for errors.
If the file contains a TSM ERROR message, perform the following steps:
 - a. Run the **stopbackup -d file_system_name** command and the **stoprestore -d file_system_name** command to stop any backup or restore operation.
 - b. Validate that no error occurred while stopping any Tivoli Storage Manager service.

- c. Run the **chkfs** *file_system_name -v* command to recapture the output to a file.
- d. Run the **startrestore** command and the **startbackup** command to enable Tivoli Storage Manager.

Review the new output file for errors. It is expected that the file contains Lost blocks were found messages. It is normal to have some missing file system blocks. If the only errors that are reported are missing blocks, no further repair is needed. However, if the **chkfs** command reports more severe errors, contact IBM support to assist with repairing the file system.

Resolving an ANS1267E error

An ANS1267E error might indicate an incorrect setting in the Tivoli® Storage Manager server configuration.

An ANS1267E error can result from the Tivoli Storage Manager server not being set up to handle hierarchical storage management (HSM) migrated files. A return of ANS1267E means that the management class is not accepting files from HSM.

The fix for this is to set “spacemgtech” to “auto”.

Resolving issues reported for lshhealth

Use this information for resolving **lshhealth** reported issues, specifically for “MGMTNODE_REPL_STATE ERROR DATABASE_REPLICATION_FAILED” and “The mount state of the file system /ibm/Filesystem_Name changed to error level.”

These errors may be transient and may clear automatically at any time.

Error for “MGMTNODE_REPL_STATE ERROR DATABASE_REPLICATION_FAILED”

To resolve the “MGMTNODE_REPL_STATE ERROR DATABASE_REPLICATION_FAILED” error, complete the following procedure.

1. Verify that the other management node role has “Host State OK”. Repair the host state if necessary.
2. Allow fifteen minutes for the error to disappear.
3. If the error does not disappear, attempt to reboot the passive management node.
4. Following the reboot and within five minutes of the file module showing “Host State OK” again, the issue should be resolved.

This ends the procedure.

Error for “The mount state of the file system /ibm/Filesystem_Name changed to error level”

To resolve the issue when the command **lshhealth -i gpfs_fs -r** returns “The mount state of the file system /ibm/Filesystem_Name changed to error level”, complete the following procedure.

1. Verify that the other management node role has “Host State OK”. Repair the host state if necessary.
2. Run the command **mountfs fileSystem**.
3. Run the command **lsfs -r**.

4. Run the command `lshealth -i gpfs_fs -r`.
The expected output for the command should be “The mount state of the file system /ibm/gpfs1 was set back to normal level.”
5. If there are still problems, refer to the GPFS documentation to try to debug or repair the error.
This ends the procedure.

Resolving full condition for GPFS file system

Use this procedure when the management GUI reports a critical error when a file system is 100% full.

You must have root access to perform this procedure.

Note: If you use GPFS snapshots, the file system locks when it reaches 100% utilization.

To resolve the full condition for the file system, perform the following steps:

1. Review the contents of the GPFS file system.
 - If the file system has snapshots, remove the oldest snapshot after verifying that it is no longer needed. Continue to remove the snapshots from oldest to newest until the level of free space that you want is achieved.
 - If no snapshots exist, perform the following steps:
 - a. Run the `mmdf` command to determine what storage pool is out of space.
 - b. Remove files to free up storage.
 - c. If the `mmdf` command output shows that there is space in free fragments, run the `mmdefragfs` command to combine the fragments into full blocks.

Note: You can run the GPFS `defrag` command while the file systems are mounted. However, for better results, unmount the GPFS file system before performing the defragmentation operation.

2. If there is no space in fragments or if the `mmdefragfs` command does not free up space, add disks (NSDs) to the file system to create space.
 - a. Verify if there are any free NSDs by issuing the `mm|nsnd -L` command.
 - b. If there are no free NSDs, look for free storage and create an NSD.
 - c. Add the free NSD to the appropriate storage pool.
If the system pool is the one that is out of space, ensure that the new NSD is configured to hold metadata.
 - d. When sufficient free space is available, remove the newly added NSD.
 - e. If there is no storage space available, contact IBM support.

Analyzing GPFS logs

Use this procedure when reviewing GPFS log entries.

Note: Contacting IBM support is recommended for any analysis of GPFS log entries.

1. Log into the appropriate file module using root privileges.
2. Review the log file `/var/adm/ras/mmfs.log.latest`. The log file is ordered from oldest to newest, so the end of the log has the latest GPFS information.

Note: The GPFS log is a complex raw log file for GPFS. If you are unable to understand the conditions listed in the log, contact IBM support.

Synchronizing time on the file modules

Use this information to synchronize the time on all Storwize V7000 Unified file module.

Synchronizing the time on all the file module can help as you start troubleshooting because the timestamps on the logs then indicate whether you have concurrent, legitimate results.

You can ensure that the Storwize V7000 Unified, Active Directory (AD), Kerberos, and other servers are synchronized with a valid Network Time Protocol (NTP) source. This is important both for log checking and because if the cluster falls behind the correct time, Kerberos tickets, for example, can expire and then no one can access the cluster. For the Storwize V7000 Unified file module, the **ntpq -p** command shows you which server is used for synchronization and any peers and a set of data about their status. The * in the first column indicates that the local clock is used for synchronization.

```
# ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
=====
*machine.domain.i 9.19.0.220  2 u  269 1024  377   0.659  -0.115  0.164
+machine.domain.i 9.19.0.220  2 u  992 1024  377   1.380   0.337  0.564
LOCAL(0)          .LOCL.        10 l  50   64  377   0.000   0.000  0.001
```

As NTP is drift based, large time differences can prevent NTP from synchronizing, or cause synchronization to take a long time. It can be helpful to synchronize time manually once and to verify that the time is picked up correctly afterward. Use the separate commands of **service ntpd stop**, **ntpdate *your IP***, and **service ntpd start**. The following example shows the sequence:

```
[root@domain.node ~]# service ntpd stop
Shutting down ntpd: [ OK ]
[root@domain.node ~]# ntpdate 9.19.0.220
14 Jan 12:06:46 ntpdate[25360]: adjust time server 9.19.0.220 offset 0.003277 sec
[root@domain.node ~]# service ntpd start
Starting ntpd: [ OK ]
[root@domain.node ~]#
```

After the time on all of the servers is synchronized, you can verify that the logs apply to your troubleshooting situation.

Chapter 5. Control enclosure

Find out how to troubleshoot the control enclosure, which includes the use of error codes, problem scenarios, software, and removal and replacement instructions.

Storwize V7000 system interfaces

The Storwize V7000 system 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 by using the 10 Gbps Ethernet ports.

You can perform almost all of the configuration, troubleshooting, recovery, and maintenance of the storage system from within the Storwize V7000 Unified management GUI or the CLI commands that are running on the Storwize V7000 file modules.

Attention: Do not use the Storwize V7000 system interfaces directly unless you are directed to do so by a service procedure.

Use the initialization tool to do the initial setup of your system. Use the Storwize V7000 Unified management GUI or the Storwize V7000 system management GUI to monitor and maintain the configuration of storage that is associated with your systems. Perform service procedures from the service assistant. Use the command-line interface (CLI) to manage your system.

Service assistant interface

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

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

When to use the service assistant

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

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

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

Use the service assistant in the following situations:

- When you cannot access the system from the management GUI and you cannot access the storage Storwize V7000 Unified 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. You can also perform the following service-related actions:

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

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

Accessing the service assistant

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

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

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

To start the application, perform 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 187.
2. Log on to the service assistant using the superuser password.

If you are accessing a new node canister, the default password is `passwd`. 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 190.

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

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

Storage system command-line interface

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

You can also access most of the storage system CLI commands from the Storwize V7000 Unified CLI that runs in the file system on one of the file modules.

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

When to use the storage system CLI

The storage 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 by using the CLI commands to monitor for certain conditions or to automate configuration changes that you make on a regular basis.

Accessing the storage system CLI

Follow the steps that are described in the “Command-line interface” topic in the “Reference” section of the Storwize V7000 Unified 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 Unified Information Center.

When to use the service CLI

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

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

Accessing the service CLI

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

USB key and Initialization tool interface

Use a USB key 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 key to perform the most common tasks.

When a USB key 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 key 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 key.

When to use the USB key

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

Using the USB key 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 key

Use any USB key that is formatted with FAT32, EXT2, or EXT3 file systems on its first partition.

When a USB key is plugged into a node canister, the node canister software searches for a text file named `satask.txt` in the root directory. If the software 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 key. 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 key.

The USB key 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 key, the result file is still created, if necessary, and the status and configuration data is written to it.

Using the initialization tool

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

The initialization tool is available on the USB key that is shipped with the control enclosures. The name of the application file is `InitTool.exe`. If you cannot locate the USB key, you can download the application from the support website:

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

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

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

The initialization tool is used to create the `satask.txt` file on a USB key. After the `satask.txt` file is created, follow the instructions in “Using a USB key” on page 170 to run the commands on the node.

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

By using the initialization tool, you can set the USB key to run one of the following tasks:

- Create a new system.
- Reset the superuser password.
- Set or reset the service IP address on the node canister on the control enclosure.

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

satask.txt commands

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

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 key. The **satask.txt** commands always run on the node that the USB key 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

(Required) The IPv4 address for the service assistant.

-gw

(Optional) The IPv4 gateway for the service assistant.

-mask

(Optional) The IPv4 subnet for the service assistant.

-serviceip_6

(Required) The IPv6 address for the service assistant.

-gw_6

(Optional) The IPv6 gateway for the service assistant.

-prefix_6

(Optional) Resets to the default IPv4 address.

-default

(Required) 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 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.

Attention: Run this command only when instructed by IBM support. Running this command directly on a Storwize V7000 can affect your I/O operations on the file modules.

Syntax

▶▶— satask — resetpassword —————▶▶

Parameters

None.

Description

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

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

This command calls the **satask resetpassword** command.

Snap command:

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

Attention: Run this command only when instructed by IBM support. Running this command directly on a Storwize V7000 can affect your I/O operations on the file modules.

Syntax

▶▶— satask — snap — --options————▶▶

Parameters

-options

(Optional) Specifies which diagnostic information to collect.

Description

This command moves a snap file to a USB key.

This command calls the **satask snap** command.

Apply software command:

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

Attention: Run this command only when instructed by IBM support. Running this command directly on a Storwize V7000 can affect your I/O operations on the file modules.

Syntax

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

Parameters

-file

(Required) The file name of software installation package.

-ignore

(Optional) Overrides prerequisite checking and forces installation of the software.

Description

This command copies the file from the USB key to the upgrade directory on the node canister.

This command calls the **satask installsoftware** command.

Create cluster command:

Use this command to create a storage system.

Note: The reference to cluster is not the same as the file system cluster on the Storwize V7000 file modules.

Attention: Run this command only when instructed by IBM support. Running this command directly on a Storwize V7000 can affect your I/O operations on the file modules.

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

(Required) The IPv4 address for Ethernet port 1 on the system.

-gw

(Required) The IPv4 gateway for Ethernet port 1 on the system.

-mask

(Required) The IPv4 subnet for Ethernet port 1 on the system.

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).

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 (**lseventlog**). 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 37 describes some of the fields that are available to assist you in diagnosing problems.

Table 37. Description of data fields for the event log

Data field	Description
Event ID	This number precisely identifies why the event was logged.
Error code	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.
Sequence number	A number that identifies the event.
Event count	The number of events coalesced into this event log record.

Table 37. Description of data fields for the event log (continued)

Data field	Description
Object type	The object type to which the event log relates.
Object ID	A number that uniquely identifies the instance of the object.
Fixed	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.
First time	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.
Last time	The time when the last instance of this error event was recorded in the log.
Root sequence number	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.
Sense data	Additional data that gives the details of the condition that caused the event to be logged.

Event notifications

Storwize V7000 Unified can use Simple Network Management Protocol (SNMP) traps, syslog messages, and Call Home email to notify you and the IBM Support Center when significant events are detected. Any combination of these notification methods can be used simultaneously. Notifications are normally sent immediately after an event is raised. However, there are some events that might occur because of service actions that are being performed. If a recommended service action is active, these events are notified only if they are still unfixed when the service action completes.

Table 38 describes the types of event notifications.

Table 38. Notification types

Notification type	Description
Error	<p>An error notification is sent to indicate a problem that must be corrected as soon as possible.</p> <p>This notification indicates a serious problem with the Storwize V7000 Unified. 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 type. Error notifications can be configured to be sent as a Call Home email to the IBM Support Center.</p>

Table 38. Notification types (continued)

Notification type	Description
Warning	<p>A warning notification is sent to indicate a problem or unexpected condition with the Storwize V7000 Unified. Always immediately investigate this type of notification to determine the effect that it might have on your operation, and make any necessary corrections.</p> <p>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 type Error.</p>
Information	<p>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.</p>

Power-on self-test

When you turn on the system, the file modules and the control enclosure 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 file module or a node canister, go to "Procedure: Understanding the system status using the LEDs" on page 193.

When the software is loaded, additional testing takes place, which ensures that all of the required hardware and software components are installed and functioning correctly.

Understanding events

The Storwize V7000 Unified software generates events, such as informational events and configuration events. An event ID or number is associated with the event and indicates the reason for the event.

There are different types of events:

- Informational events provide information on the status of an operation. Information events are recorded in the error event log, and depending on the configuration, can be notified through email, SNMP, and syslog.
- Error events are generated when a service action is required. An error event maps to an alert with an associated error code. Depending on the configuration, error events can be notified through email, SNMP, or syslog.

Understanding the error codes

Error codes are generated by the event-log analysis and system configuration code.

Error codes help you to identify the cause of a problem, the failing field-replaceable units (FRUs), and the service actions that might be needed to solve the problem.

Viewing logs and traces

The Storwize V7000 Unified clustered system maintains log files and trace files that can be used to manage your system and diagnose problems.

You can view information about collecting CIM log files or you can view examples of a configuration dump, error log, or featurization log. To do this, click **Reference** in the left pane of the Storwize V7000 Unified Information Center and then expand the **Logs and traces** section.

Understanding the 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) that is held within 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 canisters save 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. The nodes save the critical data by using the ac power and enter service state. The nodes do not handle I/O operations until the remaining battery has sufficient charge to support the saving of the critical data. 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.

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 **dumpdiskbadblocks** command and the **dumpalldiskbadblocks** command are available to query the location of bad blocks.

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

The system creates alerts in the event log for the following situations:

- When it detects medium errors and creates a bad block
- When the bad block tables fill up

The following errors are identified:

Table 39. Bad block errors

Error code	Description
1840	The managed disk has bad blocks.
1226	The system has failed to create a bad block because the MDisk already has the maximum number of allowed bad blocks.
1225	The system has failed to create a bad block because the system already has the maximum number of allowed bad blocks.

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

Bad blocks are cleared 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.

Resolving a problem

This topic describes the procedures that you follow to resolve fault conditions that exist on your system. This topic assumes that you have a basic understanding of the Storwize V7000 Unified 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 of the management GUI as the starting point to diagnose and resolve a problem. The topics that follow describe the type of problem that you might experience that are not resolved by using the management GUI. In those situations, review the symptoms and follow the actions that are provided here.

Unless you are unable to detect a newly installed enclosure, problems on expansion enclosures are resolved using the recommended actions in the management GUI. The “Start here” 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 Unified system as soon as you have created a clustered system. If you cannot create a clustered system, see the problem that contains information about what to do if you cannot create one. Go to “Problem: Cannot create a clustered storage system” on page 185.

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: Storage system management IP address unknown” on page 184. 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 184.

Log on using your user name and password. If you are unable to log on, go to “Problem: Unable to log on to the storage system management GUI” on page 185.

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 191.

Problem: Storage system management IP address unknown

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

This topic also helps if the configuration communication between the file system (file modules) and the storage system (control enclosure) is not working because the wrong IP address is being used.

The storage system management IP address is set when the USB initialization is completed. An address for port 2 can be added later.

If you do not know the storage system 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 key. 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 192; otherwise, go to “Procedure: Getting node canister and system information using a USB key” on page 192.

Problem: Unable to connect to the management GUI

This topic helps you if you are unable to connect to the management GUI from your web browser. You might get a Page not found or a similar error from the browser.

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 192; otherwise, go to “Procedure: Getting node canister and system information using a USB key” on page 192 and obtain the state of each of the node canisters from the data that is returned. If there is not a node canister with

a state of active, resolve the reason why it is not in active state. If the state of both node canisters is candidate, then there is not a clustered system to connect to. If the node state is service, go to “Procedure: Fixing node errors” on page 199.

- Ensure that you are using the correct management 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 192; otherwise, go to “Procedure: Getting node canister and system information using a USB key” on page 192 and obtain the management IP address from the data that is returned.
- Ensure that all node canisters have an Ethernet cable that is connected to port 1 and that the port is working. To understand the port status, go to “Procedure: Finding the status of the Ethernet connections” on page 198.
- 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 you have just created the clustered system using the USB key or service assistant, and entered a management IP address that is not accessible, you can safely delete the system and perform the clustered-system creation again using a suitable address. It is safe to delete the clustered system in this situation because you have not configured any volumes or loaded any data onto the system. Do not delete the clustered system if you have created any volumes on your system because any data on those volumes will be lost. In this case, you must gain access to the management IP address. If you just created the clustered system and cannot access the management IP address, go to “Procedure: Deleting a system completely” on page 199 to reset the enclosure. After that procedure, repeat the procedures to create a new clustered system using an accessible IP address.

Problem: Unable to log on to the storage system management GUI

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

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

- If you are not logging on as superuser, contact your system administrator who can verify your user name and reset your account password.
- If the user name that you are using is authenticated through a remote authentication server, verify that the server is available. If the authentication server is unavailable, you can log on as user name superuser. This user is always authenticated locally.
- If you do not know the password for superuser, go to “Procedure: Resetting superuser password” on page 190.

Problem: Cannot create a clustered storage system

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

Note: This clustered storage system is different from the file system cluster on the file modules.

The failure is reported regardless of the method that you used to create a clustered storage system:

- USB key
- 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 192 or “Procedure: Getting node canister and system information using a USB key” on page 192.

- 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 199, 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 192 or “Procedure: Getting node canister and system information using a USB key” on page 192. If the node is in service state, fix the reported node errors. For more information, go to “Procedure: Fixing node errors” on page 199. After the node error is corrected, attempt to create a clustered storage system again.

Problem: Unknown service address of a node canister

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

- If you can access the management GUI, start the service assistant on the configuration node for the clustered system by pointing your web browser to the address: *control enclosure management IP address/service*. For example, if your control enclosure management IP address is 11.22.33.44, point your web browser to 11.22.33.44/service.

The service assistant home page lists the node canister within the clustered system that it can communicate with. 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. Use the service address to connect to the node or continue to manage the node using this session. If the service address of the node that you want is not listed, go to “Procedure: Getting node canister and system information using a USB key” on page 192 to get the service address.

- If you know the service address of any node canister in the system, follow a similar procedure to the one described previously. Rather than using *control enclosure management IP address/service* to start the service assistant, use the service address that you know.

- Use a USB key to find the service address of a node. For more information, go to “Procedure: Getting node canister and system information using a USB key” on page 192.

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: Unknown service address of a node canister” on page 186. 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 200.
- You cannot connect to the service assistant if the node canister is not able to start the code. To verify that the LEDs indicate that the code is active, see “Procedure: Understanding the system status using the LEDs” on page 193.
- 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 198 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 200 to change the service IP address of a node.
- A default service address is initially assigned to each node canister. The service IP address 192.168.70.121 subnet mask 255.255.255.0 is preconfigured on Ethernet port 1 of the upper canister, canister 1. The service IP address 192.168.70.122 subnet mask 255.255.255.0 is preconfigured on Ethernet port 2 of the lower canister, canister 2.

You might not be able to access these addresses because of the following conditions:

- These addresses are the same as the addresses that are used by other devices on the network.
- These addresses cannot be accessed on your network.
- There are other reasons why they are not suitable for use on your network.

If the previous conditions apply, see “Procedure: Changing the service IP address of a node canister” on page 200 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 key in the environment, see “Procedure: Accessing a canister using a directly attached Ethernet cable” on page 201.

Problem: Management GUI or service assistant does not display correctly

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

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

Support for Storwize V7000 Unified website at www.ibm.com/storage/support/storwize/v7000/unified

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

Problem: Node canister location error

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

To find out how to resolve the node error, go to “Procedure: Fixing node errors” on page 199.

Be aware of the following items:

- Each control enclosure must have two node canisters installed.
- Node canisters and expansion canisters are not interchangeable. A node canister cannot operate in an expansion enclosure. An expansion canister cannot operate in a control enclosure.
- After the node has been used in a clustered system, the node canister has saved information that can identify whether the canister has been moved to a different enclosure or a different slot in the same enclosure from where it was previously used. Moving a node canister might compromise its access to storage or access to volumes by a host application. 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 193.
- Verify that the SAS cabling to the expansion enclosure is correctly installed. To review the requirements, see “Problem: SAS cabling not valid” on page 188.

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: Code not processed from USB key

This topic helps you resolve why the code was not processed using a USB key.

You might encounter this problem during initial setup or when running commands if you are using your own USB key rather than the USB key 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 key. If the file does not exist, then the following problems are possible:
 - The USB key is not formatted with the correct file system type. Use any USB key that is formatted with FAT32, EXT2, or EXT3 file systems on its first partition; for example, NTFS is not a supported type. Reformat the key or use a different key.
 - The USB port is not working. Try the key in the other USB port.
 - The node is not operational. Check the node status using the LEDs. See “Procedure: Understanding the system status using the LEDs” on page 193.
- If there is an `satask_result.html` file, check the first entry in the file. If there is no entry that matches the time the USB key 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 193.
- If there is a status output for the time the USB key 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 key command action.

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 key 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 key to reset the superuser password, see “USB key and Initialization tool interface” on page 170.

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.

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. Model types 2076-112, 2076-124, 2076-312, and 2076-324 are control enclosures. Model types 2076-212 and 2076-224 are expansion enclosures.

Note: Model types 2073-700 are file modules.

- The model description that is shown on the left end cap. The description shows either Control or Expansion.

Note: The model description shows file module for a file module.

- The number of ports at the rear of the enclosure. Control enclosures have Ethernet ports, Fibre Channel ports, and USB ports on the canisters. Expansion enclosures do not have any of these ports.
- The number of LEDs on the power supply units. The power supply units in the control enclosure have six LEDs. The power supply units in the expansion enclosure have four LEDs.

Identify the 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 Unified system. However, if you have more than one Storwize V7000 Unified 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 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 node*N*, 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.

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.

An overview of the status is displayed under **Connectivity** in the lower-left corner of the management GUI window.

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

- **Monitoring > System Details**
- **Monitoring > Manage Device**
- **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.

To obtain the information, connect to and log on to the service assistant using the starting service assistant procedure. For more information, go to “Accessing the service assistant” on page 168.

1. Log on to the service assistant.
2. View the information about the node canister that you connected to or the other node canister in the same enclosure.

Note: If the node canister that you want to see information about is not the current node, change it to the current node from the home page.

3. Examine the data shown for the current node.

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 address and the service address for this node. The **Location** tab identifies the enclosure in which the node canister is located.

Procedure: Getting node canister and system information using a USB key

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

Use any USB key with a FAT32 file system, a EXT2 file system, or a EXT3 file system on its first partition.

1. Ensure that the USB key does not contain a file named `satask.txt` in the root directory.
If `satask.txt` does exist in the directory, the node attempts to run the command that is specified in the file. The information that is returned is appended to the `satask_result.html` file. Delete this file if you no longer want the previous output.
2. Insert the USB key in one of the USB ports of the node canister from which you want to collect data.
3. The node canister fault LED flashes. It continues to flash while the information is collected and written to the USB key.
4. Wait until the LED stops flashing before removing the USB key.
Because the LED is a fault indicator, it might remain permanently on or off.
5. View the results 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.

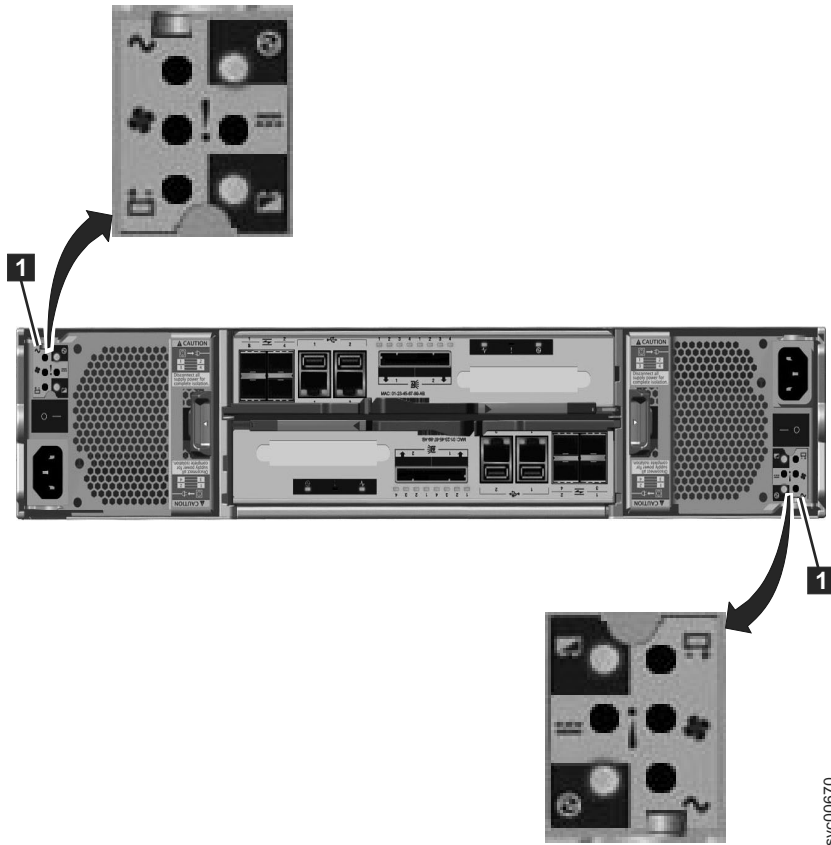
The LEDs provide a general idea of the system status. You can obtain more detail from the management GUI and the service assistant. Examine the LEDs when you are not able to access the management GUI or the service assistant, or when the system is not showing any information about a device. For information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

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 190.

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 48 on page 194 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.



svc00670

Figure 48. LEDs on the power supply units of the control enclosure

Table 40. Power-supply unit LEDs









Power supply OK 	ac failure 	Fan failure 	dc failure 	Status	Action
On	On	On	On	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.
Off	Off	Off	Off	No ac power to the enclosure.	Turn on power.
Off	Off	Off	On	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.

Table 40. Power-supply unit LEDs (continued)

Power supply OK 	ac failure 	Fan failure 	dc failure 	Status	Action
Off	On	Off	On	No ac power to this power supply	<ol style="list-style-type: none"> 1. Check that the switch on the power supply unit is on. 2. Check that the ac power is on. 3. Reseat and replace the power cable.
On	Off	Off	Off	Power supply is on and operational.	No actions
Off	Off	On	Off	Fan failure	Replace the power supply unit.
Off	On	On	On	Communication failure and power supply problem	Replace the power supply unit. If replacing the power supply unit does not fix the problem, replace the enclosure chassis.
Flashing	X	X	X	No canister is operational.	Both canisters are either off or not seated correctly. Turn off the switch on both power supply units and then turn on both switches. If this action does not resolve the problem, remove both canisters slightly and then push the canisters back in.
Off	Flashing	Flashing	Flashing	Firmware is downloading.	No actions. Do not remove ac power. Note: In this case, if there is a battery in a power supply unit, its LEDs also flash.

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

Table 41. Power LEDs


Power LED status 	Description
Off	There is no power to the canister. Try reseating the canister. Go to “Procedure: Reseating a node canister” on page 201. If the state persists, follow the hardware replacement procedures for the parts in the following order: node canister, enclosure chassis.

Table 41. Power LEDs (continued)


Power LED status 	Description
Slow flashing (1 Hz)	Power is available, but the canister is in standby mode. Try to start the node canister by reseating it. Go to “Procedure: Reseating a node canister” on page 201.
Fast flashing (2 Hz)	The canister is running its power-on self-test (POST). Wait for the test to complete. If the canister remains in this state for more than 10 minutes, try reseating the canister. Go to “Procedure: Reseating a node canister” on page 201. If the state persists, follow the hardware replacement procedure for the node canister.

Figure 49 shows the LEDs on the node canister.

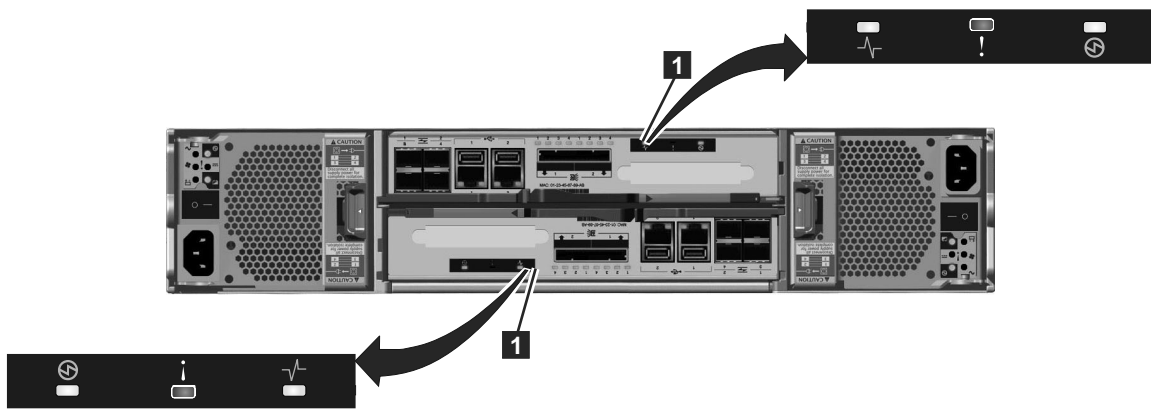


Figure 49. LEDs on the node canisters

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

Table 42. System status and fault LEDs







System status LED 	Fault LED 	Status 	Action
Off	Off	Code is not active.	<ul style="list-style-type: none"> Follow procedures for reviewing power LEDs. If the power LEDs show green, reseal the node canister. See “Procedure: Reseating a node canister” on page 201. If the LED status does not change, see “Replacing a node canister” on page 204.
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.

Table 42. System status and fault LEDs (continued)

System status LED 	Fault LED 	Status 	Action
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 199.
Flashing	Off	Code is active. Node state is candidate.	Create a clustered system on the node canister, or add the node canister to the clustered system. If the other node canister in the enclosure is in active state, it automatically adds this node canister into the clustered system. A node canister in this state can be managed using the service assistant.
Flashing	On	Code is active. Node state is service.	The node canister cannot become active in a clustered system. Several problems can exist: hardware problem, a problem with the environment or its location, or problems with the code or data on the canister. Follow the procedure to fix the node errors. Go to "Procedure: Fixing node errors" on page 199.
Any	Flashing	The node canister is being identified so that you can locate it.	The fix procedures in the management GUI might have identified the component because it requires servicing. Continue to follow the fix procedures. The service assistant has a function to identify node canisters. If the identification LED is on in error, use the service assistant node actions to turn off the LED.

To review the status of the control enclosure batteries, see Table 43.

Table 43. Control enclosure battery LEDs





Battery Good 	Battery Fault 	Description	Action
On	Off	Battery is good and fully charged.	None
Flashing	off	Battery is good but not fully charged. The battery is either charging or a maintenance discharge is being performed.	None
Off	On	Nonrecoverable battery fault.	Replace the battery. If replacing the battery does not fix the issue, replace the power supply unit.

Table 43. Control enclosure battery LEDs (continued)

Battery Good 	Battery Fault 	Description	Action
Off	Flashing	Recoverable battery fault.	None
Flashing	Flashing	The battery cannot be used because the firmware for the power supply unit is being downloaded.	None

Procedure: Finding the status of the Ethernet connections

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

Ensure that the software is active on the node before you begin this procedure. Go to “Procedure: Understanding the system status using the LEDs” on page 193. Ethernet port 1 must be connected to an active port on your Ethernet network.

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

- Use the USB key to obtain the most comprehensive information for the node status. Go to “Procedure: Getting node canister and system information using a USB key” on page 192.

The status, speed, and MAC address are returned for each port. Information is returned that identifies whether the node is the configuration node and if any node errors were reported.

- Examine the LEDs of the Ethernet ports. For the status of the LEDs, go to Ethernet ports and indicators .

The activity LED flashes when there is activity on the connection. The link state LED must be permanently on. If it is off, the link is not connected.

If your link is not connected, perform 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 key, review all the node errors that are reported.
5. Replace the Ethernet cable.
6. For the 10 Gbps Ethernet port, replace the small form-factor pluggable (SFP) transceiver. See “Replacing an SFP transceiver” on page 208.
7. Follow the hardware replacement procedure for a node canister. See “Replacing a node canister” on page 204.

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.

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

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

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

Procedure: Deleting a system completely

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

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, which includes the drives in the control enclosure, in the expansion enclosures, and on the managed disks on external storage systems. The only volumes not affected are image mode volumes on external storage systems.

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.

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

This action causes the system to reset.

6. Power each enclosure off and on before creating a system.

Procedure: Fixing node errors

This procedure describes how to fix a node error that is detected on one of the node canisters in your system.

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

1. Use the service assistant to view the current node errors on any node.
2. If available, use the management GUI to run the recommended action for the alert.
3. Follow the fix procedure instructions.

4. If the recommended action does not provide sufficient information to determine the service action, review the node error descriptions and service actions.
See the node error descriptions if you cannot access the management GUI or if the management GUI is not reporting an alert because it cannot connect to the node. When you cannot connect to the management GUI, follow the procedure for getting node canister and clustered-system information using the service assistant. Go to “Procedure: Getting node canister and system information using the service assistant” on page 192. Start with the node that displays an error. The home page shows the node errors on the current node in the priority that you must service them. Start with the node error with the highest priority.
5. Select a different node in the system to see the node errors on that node.
6. Attempt to service the node errors in the priority order that they are listed.
7. Use the error number as an index when reviewing the node error descriptions. The service actions for each error are listed with the error code.

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.

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.

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 key. Go to “Using the initialization tool” on page 171.

- Use a text editor to create the command file on the USB key. Go to “Using a USB key” on page 170.

Procedure: Accessing a canister using a directly attached Ethernet cable

Use this procedure 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.

Perform this procedure if you are not authorized to use a USB key 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 192.168.70.121 subnet mask: 255.255.255.0 and 190.168.70.122 subnet mask: 255.255.255.0 cannot be accessed on your network.

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, use the management GUI network configuration options to set the service IP to an address that is accessible on the network.

Perform 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 the upper node canister.

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

2. Connect the other end of the Ethernet cable directly to the Ethernet port on a personal computer that has a web browser installed.
3. Use the operating system tools on the computer to set the IP address of the Ethernet port that is used in the previous step to 192.168.70.10.
4. Point your web browser to the service address.
 - If you have connected to node canister 1, the upper canister, point your web browser from your personal computer to <https://192.168.70.121>.
 - If you have connected to node canister 2, the lower canister, point your web browser from your personal computer to <https://192.168.70.122>.
5. Log on with the superuser password. The default password is `passw0rd`.
6. After the action completes, disconnect your personal computer and reconnect the node canister to the Ethernet network.
7. Set the service address of the canister to one that can be accessed on the network as soon as possible.

Procedure: Reseating a node canister

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

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.

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 190.
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.

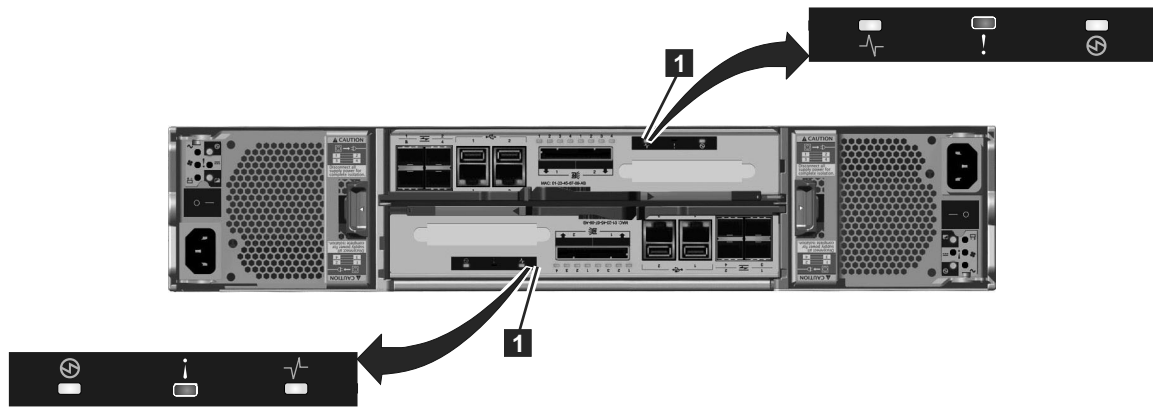
Procedure: Powering off your system

Use this procedure to power off your Storwize V7000 system when it must be serviced or to permit other maintenance actions in your data center. To turn off the Storwize V7000 Unified system, see “Turning off the system” in the Storwize V7000 Unified information center.

To power off your Storwize V7000 system, use the following steps:

1. Stop hosts.
2. Shut down the system by using the control enclosure 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.



svc00672

Figure 50. LEDs on the node canisters

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. Typically, you perform this task from the Storwize V7000 Unified management GUI. You can also collect information from the Storwize V7000 control enclosure itself.

The control enclosure 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.

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.
- 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.

A failure has indicated that the node software is damaged and must be reinstalled. Use the service assistant to reinstall the software.

1. Ensure that the node you want to reinstall the software on is the current node. Go to “Accessing the service assistant” on page 168.
2. Select **Reinstall Software** from the navigation.
3. Select **Rescue from another node**.

Removing and replacing parts

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

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

Even though many of these procedures are hot-swappable, 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.

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.

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

Replacing a node canister

This topic describes how to replace a node canister.

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

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

Attention: Do not replace one type of node canister with another type. For example, do not replace a model 2076-112 node canister with a model 2076-312 node canister.

Be aware of the following canister LED states:

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

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

To replace the node canister, perform the following steps:

1. Read the safety information to which “Preparing to remove and replace parts” on page 204 refers.
2. Confirm that you know which canister to replace. Go to “Procedure: Identifying which enclosure or canister to service” on page 190.
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**).

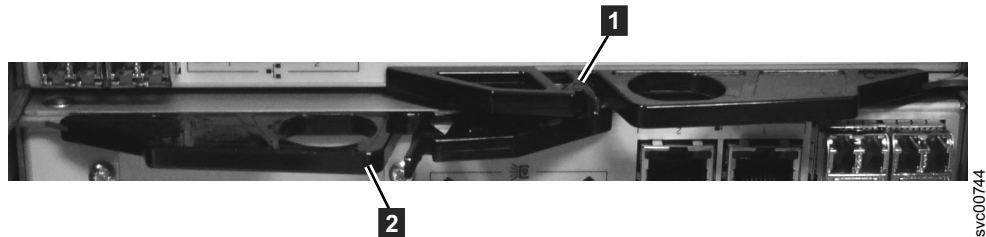
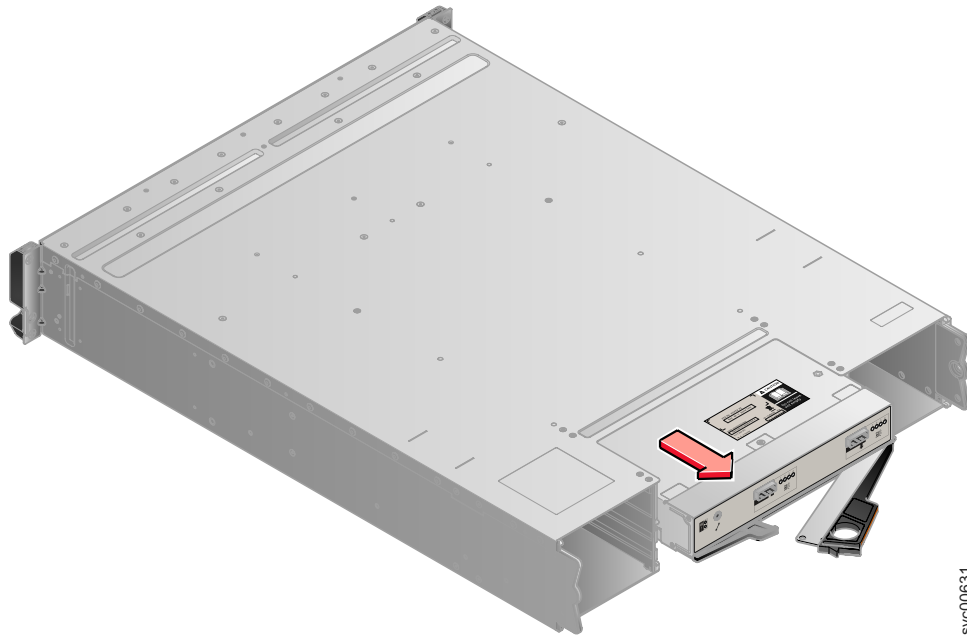


Figure 51. Rear of node canisters that shows the handles.

6. Squeeze them together to release the handle.



svc00631

Figure 52. Removing the canister from the enclosure

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

Replacing an expansion canister

This topic describes how to replace an expansion canister.

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.

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:

1. Read the safety information to which “Preparing to remove and replace parts” on page 204 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**).

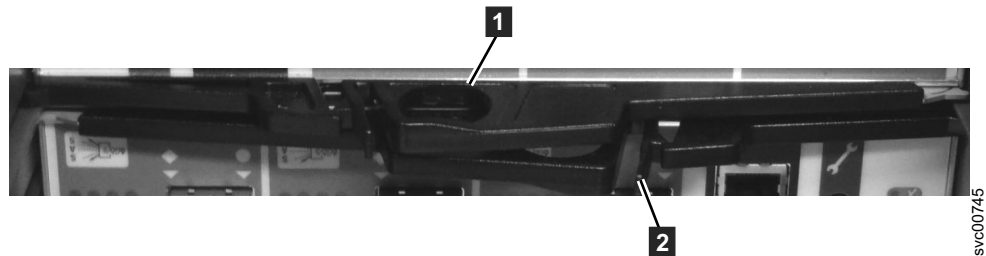


Figure 53. Rear of expansion canisters that shows the handles.

5. Squeeze them together to release the handle.

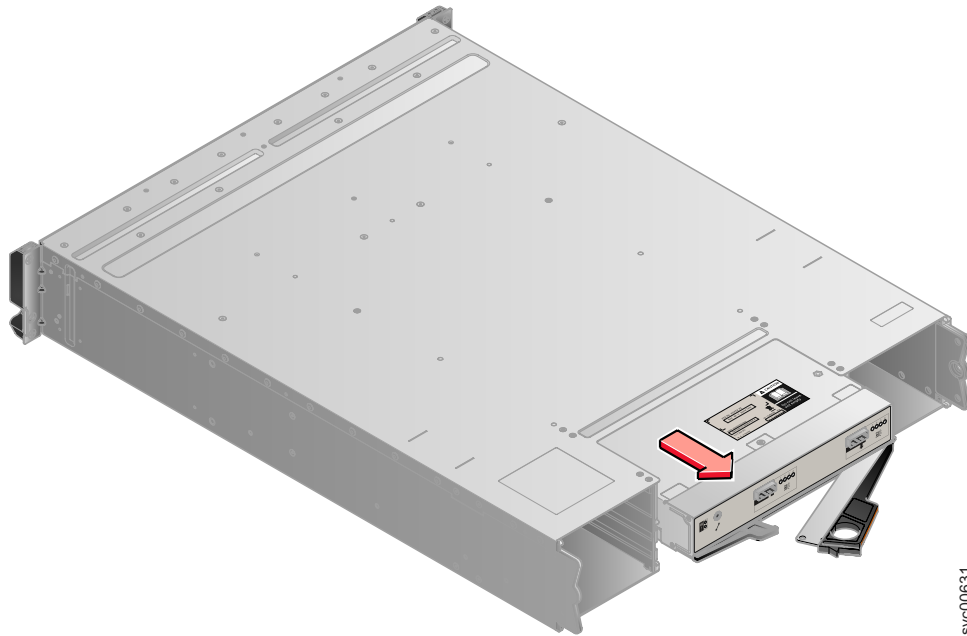


Figure 54. Removing the canister from the enclosure

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

Replacing an SFP transceiver

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

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.

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)

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

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 55 illustrates an SFP transceiver and its release handle.



Figure 55. SFP transceiver

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.

DANGER

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

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

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

To disconnect:

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

To connect:

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

(D005)

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

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

Even though many of these procedures are hot-swappable, 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.

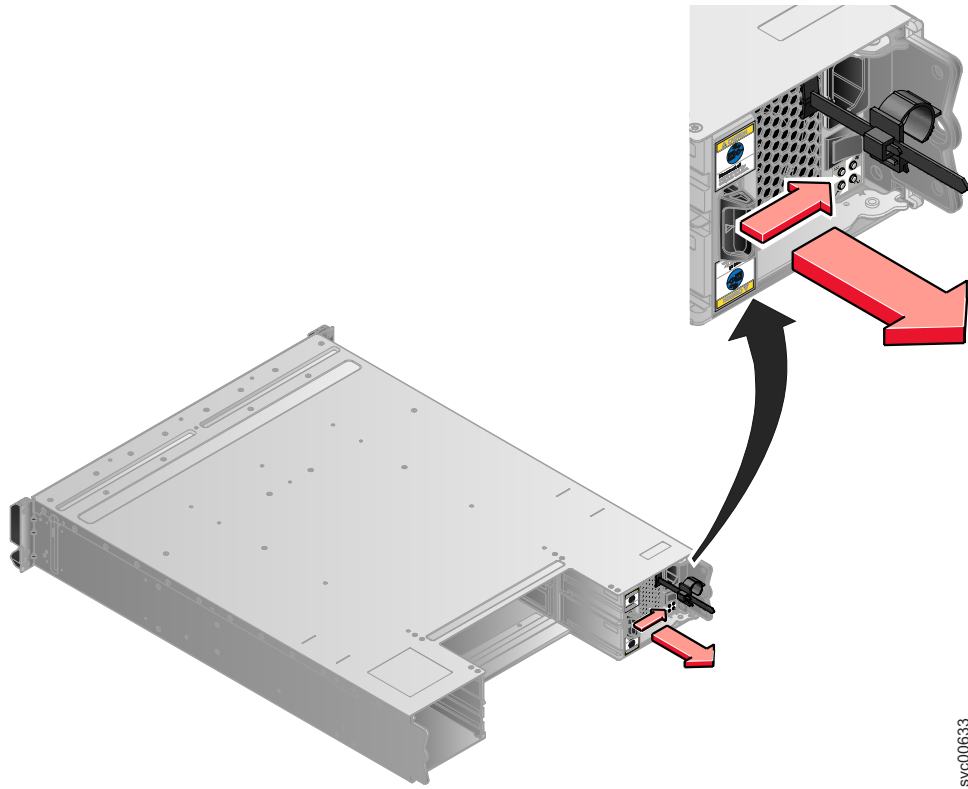
Attention: In some instances, it might not be advisable to remove a power supply unit when a system is performing I/O. For example, the charge in the backup battery might not be sufficient enough within the partner power-supply unit to continue operations without causing a loss of access to the data.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

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 217.

To replace the power supply, perform the following steps:

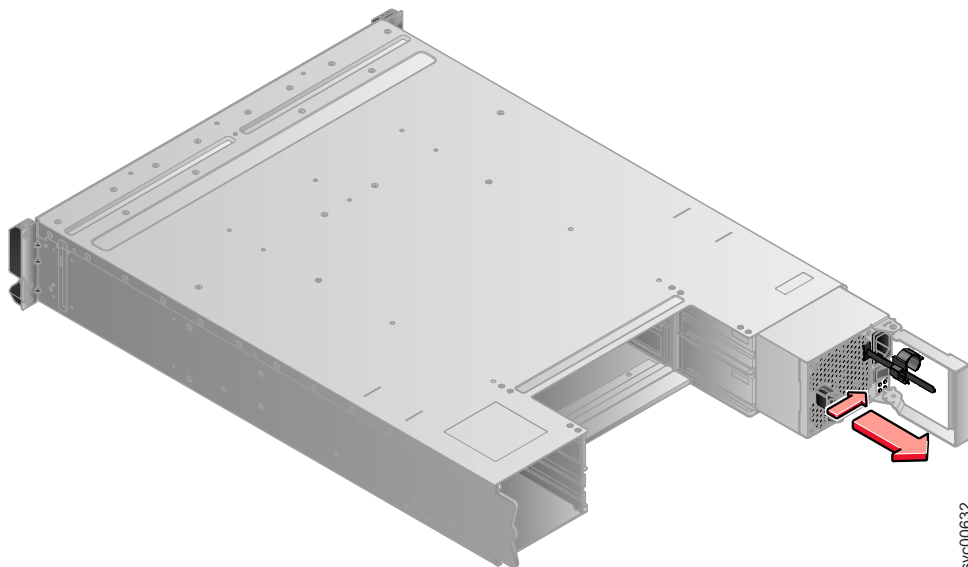
1. Read the safety information to which “Preparing to remove and replace parts” on page 204 refers.
2. Examine the Identify LED that is lit on the front of the enclosure to identify the correct enclosure.
3. Turn off the power to the power supply units using the switches at the back of the units.
4. Disconnect the cable retention bracket and the power cord from the power supply that you are replacing.
5. Remove the power supply unit. Record the orientation of the power supply unit. Power supply unit 1 is top side up, and power supply unit 2 is inverted.
 - a. Depress the black locking catch from the side with the colored sticker as shown in Figure 56 on page 212.



svc00633

Figure 56. Directions for lifting the handle on the power supply unit

- b. Grip the handle to pull the power supply out of the enclosure as shown in Figure 57.



svc00632

Figure 57. Using the handle to remove a power supply unit

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.

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.

DANGER

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

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

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

To disconnect:

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

To connect:

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

(D005)

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

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

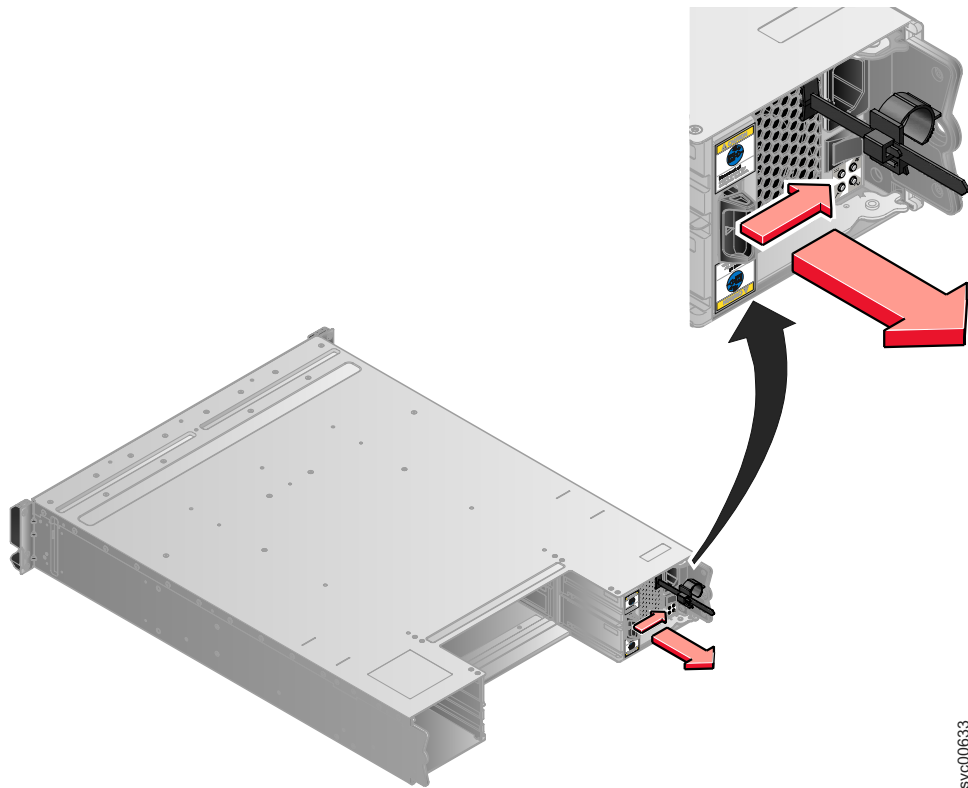
Even though many of these procedures are hot-swappable, these procedures are intended to be used only when your system is not up and running and performing I/O operations. Unless your system is offline, go to the management GUI and follow the fix procedures.

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 replace the power supply.

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

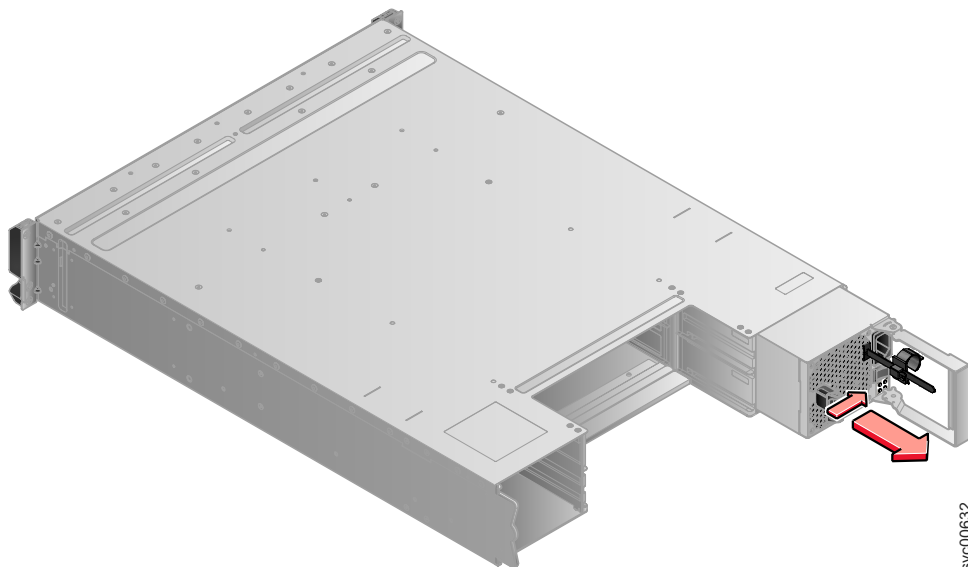
1. Read the safety information to which “Preparing to remove and replace parts” on page 204 refers.
2. Examine the Identify LED that is lit on the front of the enclosure to identify the correct enclosure.
3. Turn off the power to the power supply units using the switches at the back of the units.
4. Disconnect the cable retention bracket and the power cord from the power supply that you are replacing.
5. Remove the power supply unit. Record the orientation of the power supply unit. Power supply unit 1 is top side up, and power supply unit 2 is inverted.
 - a. Depress the black locking catch from the side with the colored sticker as shown in Figure 58 on page 216.



svc00633

Figure 58. Directions for lifting the handle on the power supply unit

- b. Grip the handle to pull the power supply out of the enclosure as shown in Figure 59.



svc00632

Figure 59. Using the handle to remove a power supply unit

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.

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.

DANGER

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

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

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

To disconnect:

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

To connect:

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

(D005)

CAUTION:

The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C007)

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

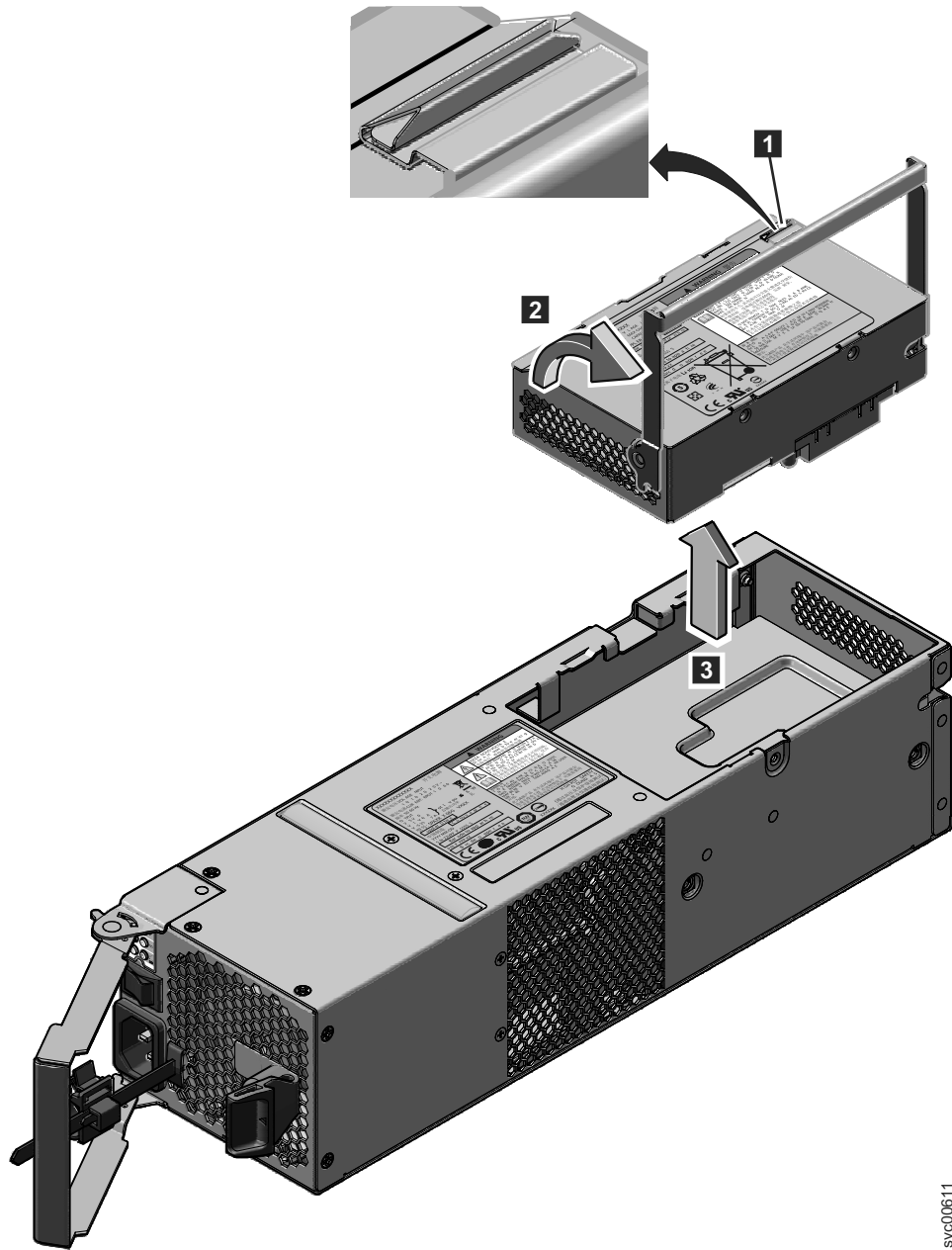
Even though many of these procedures are hot-swappable, these procedures are intended to be used only when your system is not up and running and performing I/O operations. Unless your system is offline, go to the management GUI and follow the fix procedures.

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.

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:

1. Read the safety information to which “Preparing to remove and replace parts” on page 204 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 209.
3. Remove the battery, as shown in Figure 60 on page 220.



svc00611

Figure 60. Removing the battery from the control enclosure power-supply unit

- a. Press the catch to release the handle **1**.
 - b. Lift the handle on the battery **2**.
 - c. Lift the battery out of the power supply unit **3**.
4. Install the replacement battery.

Attention: The replacement battery has protective end caps that must be removed prior to use.

- a. Remove the battery from the packaging.
- b. Remove the end caps.
- c. Attach the end caps to both ends of the battery that you removed and place the battery in the original packaging.

- d. Place the replacement battery in the opening on top of the power supply in its proper orientation.
 - e. Press the battery to seat the connector.
 - f. Place the handle in its downward location
5. Push the power supply unit back into the enclosure until the handle starts to move.
 6. Finish inserting the power supply unit into the enclosure by closing the handle until the locking catch clicks into place.
 7. Reattach the power cable and cable retention bracket.
 8. Turn on the power switch to the power supply unit.

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.

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:

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.

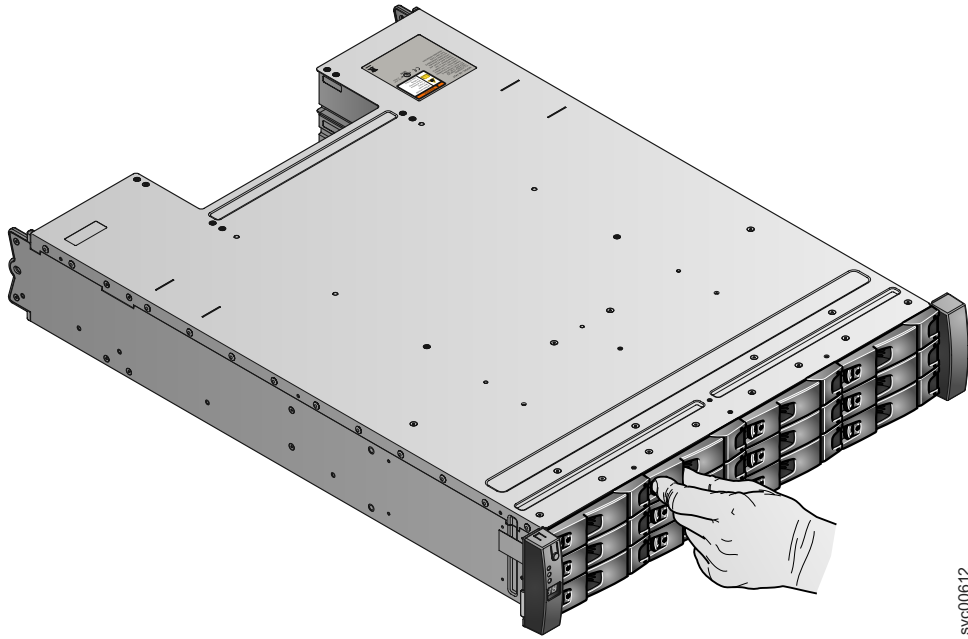
Attention: If your drive is configured for use, go to the management GUI and follow the fix procedures. Performing the replacement actions without the assistance of the fix procedures results in loss of data or access to data.

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

The drives can be distinguished from the blank carriers by the color-coded striping on the drive. The drives are marked with an orange striping. The blank carriers are marked with a blue striping.

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

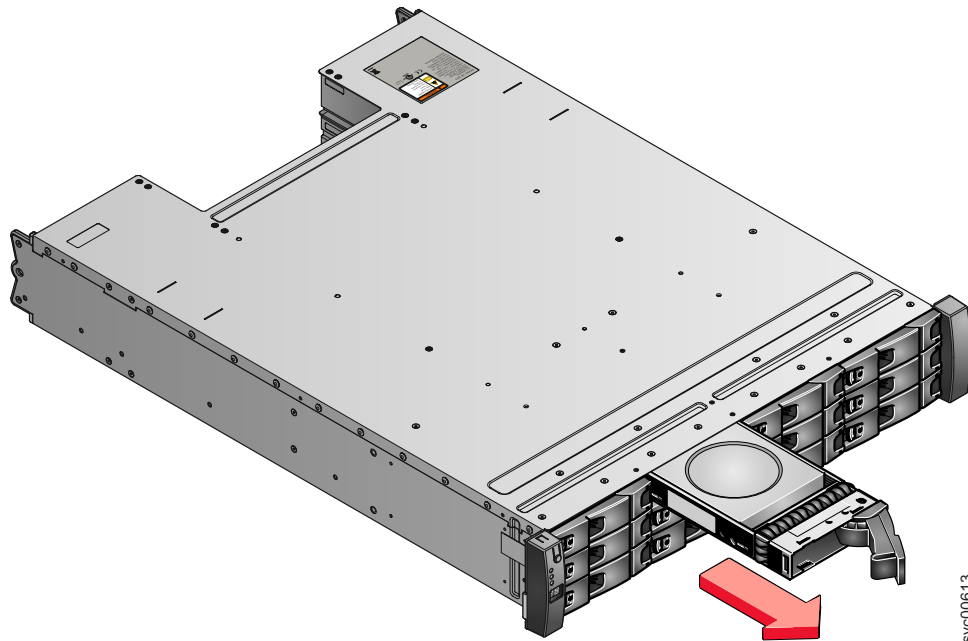
1. Read the safety information to which "Preparing to remove and replace parts" on page 204 refers.
2. Unlock the assembly by squeezing together the tabs on the side.



svc00612

Figure 61. Unlocking the 3.5" drive

3. Open the handle to the full extension.



svc00613

Figure 62. 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

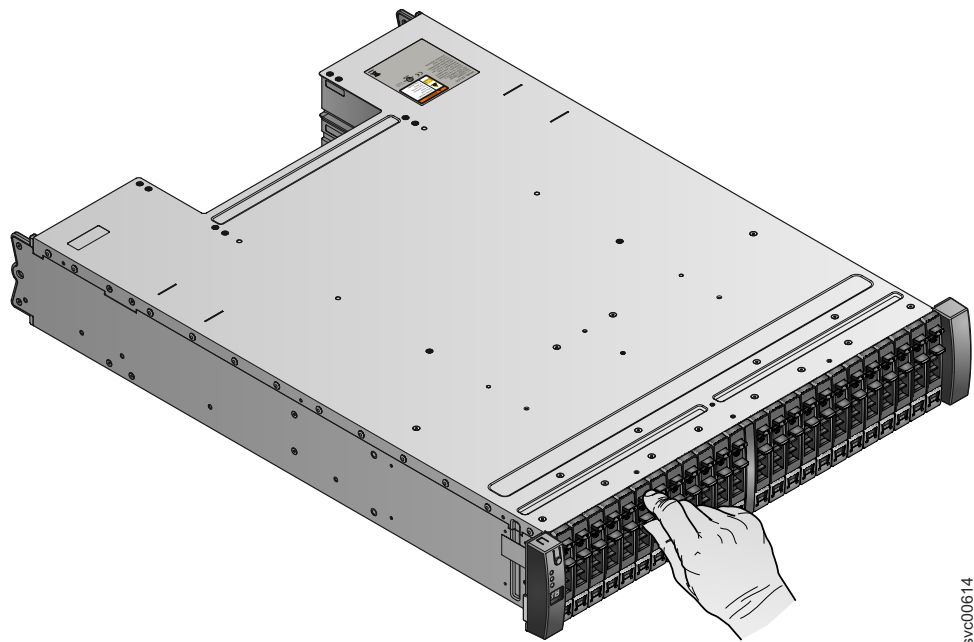
This topic describes how to remove a 2.5" drive assembly or blank carrier.

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

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

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

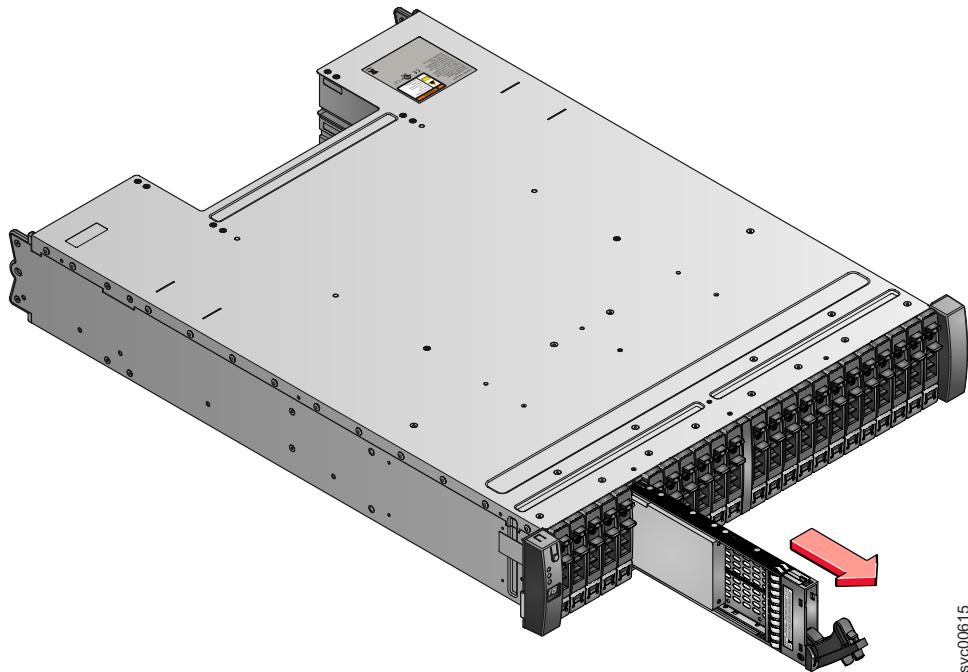
1. Read the safety information to which “Preparing to remove and replace parts” on page 204 refers.
2. Unlock the module by squeezing together the tabs at the top.



svc00614

Figure 63. Unlocking the 2.5" drive

3. Open the handle to the full extension.



svc00615

Figure 64. Removing 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 an enclosure end cap

This topic describes how to replace an enclosure end cap.

To replace the enclosure end cap, perform the following steps:

1. On either side of the drive assemblies, remove the enclosure end caps by squeezing the middle of the cap and pulling it away from the front of the rack.
2. Reattach the end cap by relocating it on either side of the drive assemblies and gently pushing it on.

Replacing a SAS cable

This topic describes how to replace a SAS cable.

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:

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.



Figure 65. SAS cable

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.

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 230.

DANGER

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

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

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

To disconnect:

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

To connect:

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

(D005)

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

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

Ensure that you are aware of the procedures for handling static-sensitive devices before you remove the enclosure.

To replace a control enclosure chassis, perform the following steps:

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 block 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 following the procedure in “Turning off the system”.
4. If your system contains more than one I/O group, you might not need to power down the file modules if the enclosure is not connected to the file modules and if the drives that are managed by this enclosure are not used in any file volumes. Use the following procedure to see if any file volumes are affected:

- a. Use the output from the **lsenclosure** CLI command to determine the enclosure_id for the control enclosure that is to be replaced.
- b. Use the following CLI command to find the volumes that depend on this enclosure:

```
lsdependentvdisks -enclosure <enclosure_id>
```

Dependent volume names that start with IFS are file volumes that are used by the file modules to provide file systems. Turn off these file modules. See the procedure "Turning off the system".

5. If the I/O group is still online, shut down the I/O group by using the control enclosure CLI.
 - a. Identify the two node canisters in the I/O group that are provided by the control enclosure to be replaced.
 - b. To shut down each node, issue the following CLI command once for each of the two node canisters:

```
stopssystem -force -node <node ID>
```
 - c. Wait for the shutdown to complete.

6. 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 227 or step 4 on page 227.

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.

7. Turn off the power to the enclosure using the switches on the power supply units.
8. 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.
9. Disconnect the cable retention brackets and the power cords from the power supply units.
10. Disconnect the data cables for each canister.
11. Remove the power supply units from the enclosure.
12. 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.
13. 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.
14. Remove both enclosure end caps from the enclosure. Keep the left end cap because it is used again.
15. Remove the clamping screws that attached the enclosure to the rack cabinet.
16. Remove the enclosure chassis from the front of the rack cabinet and take the chassis to a work area.
17. Install the new enclosure chassis in the rack cabinet.
18. Remove the end caps from the new enclosure and install the clamping screws that attach the enclosure to the rack cabinet.
19. Replace the end caps. Use the new right end cap and use the left end cap that you removed in step 14.

Using the left end cap that you removed preserves the model and serial number identification.
20. 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.
21. 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.

22. Install the power supply units.
23. 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.

24. Attach the power cords and the cable retention brackets to the power supply units.
25. 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.
26. 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 187.

- 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 227.

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 199. 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.

- e. Power up the file modules. See “Turning on the system”.
27. 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.
28. Select the original enclosure in the tree view.
Verify that it is offline and managed and that the serial number is correct.
29. 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.
30. 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.
31. Select the new enclosure in the tree view and verify that it is now online and managed.
32. 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.
33. Check the status of all volumes and physical storage to ensure everything is online.
34. Restart the host application and any FlashCopy activities, Global Mirror activities, or Metro Mirror activities that were stopped.

Replacing an expansion enclosure chassis

This topic describes how to replace an expansion enclosure chassis.

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 225.

DANGER

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

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

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

To disconnect:

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

To connect:

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

(D005)

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

Even though many of these procedures are hot-swappable, these procedures are intended to be used only when your system is not up and running and performing I/O operations. Unless your system is offline, go to the management GUI and follow the fix procedures.

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

Ensure that you are aware of the procedures for handling static-sensitive devices before you remove the enclosure.

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:

1. Shut down the I/O activity to the enclosure, which includes host access to GPFS file systems, 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 9.

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.

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.

Perform the following steps to replace the support rails:

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 **1** from the rail assembly on both sides of the rack cabinet.

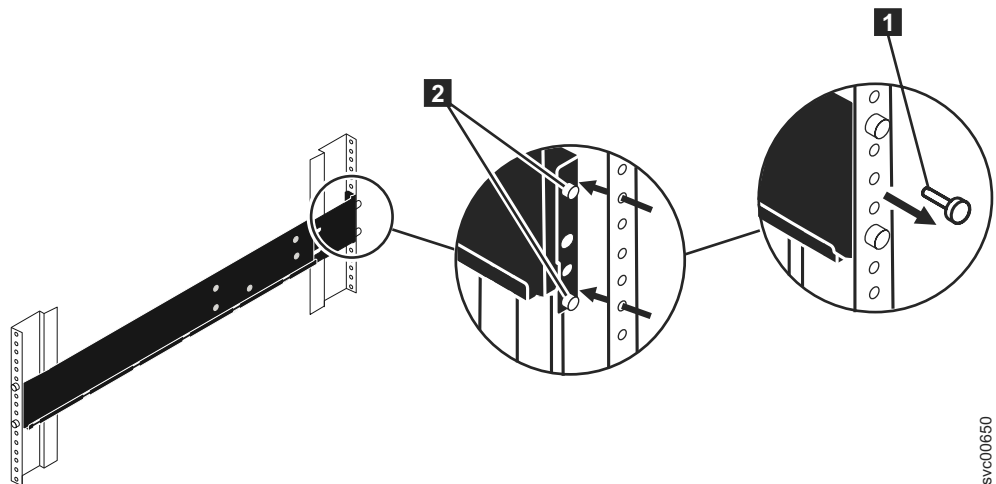


Figure 66. Removing a rail assembly from a rack cabinet

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 **2**.
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 **2**.
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.

General storage system procedures

This section provides general information about hardware and Fibre Channel link issues.

SAN problem determination

The procedures that are provided here help you solve problems on the Storwize V7000 Unified system and its connection to the storage area network (SAN).

SAN failures might cause Storwize V7000 Unified drives 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:

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

Fibre Channel link failures

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

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

- The customer's SAN monitoring tools
- The Fibre Channel status LEDs at the rear of the node canister
- An error that indicates that a single port has failed

Attempt each of the following 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 Unified node.

Note: Storwize V7000 Unified 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.

Ethernet iSCSI host-link problems

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

For network problems, you can attempt any of the following actions:

- Test your connectivity between the host and Storwize V7000 Unified ports.
- Try to ping the Storwize V7000 Unified system from the host.
- Ask the Ethernet network administrator to check the firewall and router settings.
- Check that the subnet mask and gateway are correct for the Storwize V7000 Unified host configuration.

For Storwize V7000 Unified problems, you can attempt any of the following actions:

- View the configured node port IP addresses by using the **lspportip** CLI command.
- View the list of volumes that are mapped to a host by using the **lshostvdiskmap** command to ensure that the volume host mappings are correct.
- Verify that the volume is online by using the **lsvdisk** command.

For host problems, you can attempt any of the following actions:

- Verify that the host iSCSI qualified name (IQN) is correctly configured.
- Use operating system utilities (such as Windows device manager) to verify that the device driver is installed, loaded, and operating correctly.

Recover system procedure

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.

After you perform the storage system recovery procedure, contact IBM support. They can assist you with recovering the file modules so that access to the file systems can be restored.

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 software 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 software, and where necessary, to upgrade or downgrade the level of software.

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

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

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

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

- Check to see if any node in the system has a node status of active. This status means that the system is still available. In this case, recovery is not necessary.
- Do not recover the system if the management IP address is available from another node. Ensure that all service procedures have been run.
- Check the node status of every node canister that is part of this system. Resolve all hardware errors except node error 578 or node error 550.
 - All nodes must be reporting either a node error 578 or a node error 550. These error codes indicate that the system has lost its configuration data. If any nodes report anything other than these error codes, do not perform a recovery. You can encounter situations where non-configuration nodes report other node errors, such as a 550 node error. The 550 error can also indicate that a node is not able to join a system.
 - If any nodes show a node error 550, record the error data that is associated with the 550 error from the service assistant.
 - In addition to the node error 550, the report can show data that is separated by spaces in one of the following forms:
 - Node identifiers in the format: *<enclosure_serial>-<canister slot ID>*(7 characters, hyphen, 1 number), for example, 01234A6-2
 - Quorum drive identifiers in the format: *<enclosure_serial>:<drive slot ID>[<drive 11S serial number>]* (7 characters, colon, 1 or 2 numbers, open square bracket, 22 characters, close square bracket), for example, 01234A9:21[11S1234567890123456789]
 - Quorum MDisk identifier in the format: *WWPN/LUN* (16 hexadecimal digits followed by a forward slash and a decimal number), for example, 1234567890123456/12
 - If the error data contains a node identifier, ensure that the node that is referred to by the ID is showing node error 578. If the node is showing a node error 550, ensure that the two nodes can communicate with each other. Verify the SAN connectivity, and if the 550 error is still present, restart one of the two nodes by clicking **Restart Node** from the service assistant.
 - If the error data contains a quorum drive identifier, locate the enclosure with the reported serial number. Verify that the enclosure is powered on and that the drive in the reported slot is powered on and functioning. If the node canister that is reporting the fault is in the I/O group of the listed enclosure, ensure that it has SAS connectivity to the listed enclosure. If the node canister that is reporting the fault is in a different I/O group from the listed enclosure, ensure that the listed enclosure has SAS connectivity to both node canisters in the control enclosure in its I/O group. After verifying these things, restart the node by clicking **Restart Node** from the service assistant.
 - If the error data contains a quorum MDisk identifier, verify the SAN connectivity between this node and that WWPN. Check the storage controller to ensure that the LUN referred to is online. After verifying these things, if the 550 error is still present, restart the node by clicking **Restart Node** from the service assistant.

- If there is no error data, the error is because there are insufficient connections between nodes over the Fibre Channel network. Each node must have at least two independent Fibre Channel logical connections, or logins, to every node that is not in the same enclosure. An independent connection is one where both physical ports are different. In this case, there is a connection between the nodes, but there is not a redundant connection. If there is no error data, wait 3 minutes for the SAN to initialize. Next check that the following items:
 - That there are at least two Fibre Channel ports that are operational and connected on every node.
 - That the SAN zoning allows every port to connect to every port on every other node
 - If redundant SANs are being used, that all of them are operational.
 After verifying these things, if the 550 error is still present, restart the node by clicking **Restart Node** from the service assistant.

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

- For any nodes that are reporting a node error 550, ensure that all the missing hardware that is identified by these errors is powered on and connected without faults.
- If you have not been able to restart the system and if any node other than the current node is reporting node error 550 or 578, you must remove system data from those nodes. This action acknowledges the data loss and puts the nodes into the required candidate state.
- Do not attempt to recover the system if you have been able to restart it.
- If back-end MDisks are removed from the configuration, those volumes that depended on that hardware cannot be recovered. All previously configured back-end hardware must be present for a successful recovery.
- Any nodes that were replaced must have the same WWNN as the nodes that they replaced.
- If any of the node canisters were replaced, they must not have participated in any other system. You can resolve this issue by performing a node rescue on the affected canister by using the service assistant. Do not perform this action on any of the other node canisters.
- The configuration backup file must be up to date. If any configuration changes had been made since the backup was taken, the data is inconsistent and further investigation is needed. Manual changes are required after the system is recovered.
- Any data that was in the cache at the point of failure is lost. The loss of data can result in data corruption on the affected volumes. If the volumes are corrupted, call the IBM Support Center.

Fix hardware errors

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

Obtain a basic understanding about the hardware failure. In most situations when there is no clustered system, a power issue is the cause.

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.

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:

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.

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

Performing system recovery using the service assistant

Start recovery when all node canisters that were members of the system are online and have candidate status. Use the service assistant to verify the status. If there are any nodes that display error code 550 or error code 578, you must remove their system data to get them into candidate status. Do not run the recovery procedure on different node canisters in the same system. This restriction includes remote systems also.

All node canisters must be at the same level of software 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 software, and where necessary, to upgrade or downgrade the level of software.

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

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

You might see any one of the following categories of messages:

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

- T3 incomplete. One or more of the volumes is offline because there was fast write data in the cache. Further actions are required to bring the volumes online again. See “Recovering from offline VDisks using the CLI” on page 241 for details.
- T3 failed. Call IBM Support. Do not attempt any further action.

The recovery can be run from any node canisters in the system. The node canisters must not have participated in any other system.

Note: Each individual stage of the recovery procedure might take significant time to complete. The time to complete depends on your specific configuration.

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

1. Point your browser to the service IP address of one of the node canisters.
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. See “Procedure: Changing the service IP address of a node canister” on page 200.
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 there are any nodes that display error code 550 or error code 578, you must remove their system data to get them into candidate status. See “Procedure: Removing system data from a node canister” on page 198.

4. Select **Recover System** from the navigation.
5. Follow the online instructions to complete the recovery procedure.

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.

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.

After the recovery completes successfully, perform the checks to get your environment operational.

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” on page 241.

After you perform the storage system recovery procedure, contact IBM support. They can assist you with recovering the file modules so that access to the file systems can be restored.

Recovering from offline VDisks using the CLI

If a recovery procedure (T3 procedure) completes with offline volumes, you can use the command-line interface (CLI) to access the volumes.

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 volumes are offline because of the loss of write-cache data during the event that led both nodes to lose their hardened data. These volumes might need additional recovery steps after the volume is brought back online.

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

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.

You can recover individual volumes by using the **recovervdisk** command. You can recover all the volumes in a clustered system by using the **recovervdiskbysystem** command.

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

What to check after running the system recovery

Several tasks must be performed before you use the volumes.

Be aware of the following differences regarding the recovered configuration:

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

Before using the block volumes that are accessed by the SAN or with iSCSI, perform the following tasks:

- Start the block host systems.

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

Before using the file volumes that are used by GPFS on the file modules to provide Network Attached Storage (NAS), perform the following task:

- Contact IBM support for assistance with recovering the GPFS quorum state so that access to files as NAS can be restored.

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 block 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 file systems and 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.

Contact the IBM support center to help you prepare the Storwize V7000 Unified system to do the restoring of the system configuration on the control enclosure.

The configuration restore procedure is designed to restore the information about your block storage configuration, such as block volumes, local Metro Mirror information, local Global Mirror information, storage pools, and nodes. All the data that is written to the block volumes is not restored.

To restore the data on the block volumes, you must restore the application data separately from any application that uses the volumes on the clustered system as

storage. The file volumes are not restored. You must restore the file module configuration and the file systems separately. Therefore, you must have a backup of this data before you follow the configuration recovery process.

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 Unified 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.

Before you begin, hardware recovery must be complete. The following hardware must be operational: hosts, Storwize V7000 Unified, 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 back up your block storage 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 (_).
- If the ID of the object is different from what is recorded in the current configuration data file, the default object names for controllers, I/O groups, and managed disks (MDisks) do not restore correctly.
- 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.

The backup feature of the **svconfig** 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. If a system is lost after a severe failure occurs, both configuration of 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.

The SSH coding examples that are provided are samples using the PuTTY scp (pscp) application code. The pscp application is available when you install an SSH client on your host system. You can access the pscp application through a Microsoft Windows command prompt.

Perform the following steps to back up your configuration data:

1. Back up all of the application data that you stored on your volumes using your preferred backup method.
2. Open a command prompt.
3. Using the command-line interface, issue the following command to log on to the system:

```
plink -i ssh_private_key_file
superuser@control_enclosure_management_IP
```

where *ssh_private_key_file* is the name of the SSH private key file for the superuser and *control_enclosure_management_IP* is the IP address or DNS name of the clustered system on the control enclosure for which you want to back up the configuration.

4. Issue the following CLI command to remove all of the existing configuration backup and restore files that are on your configuration node canister in the /tmp directory.

```
svcconfig clear -all
```

5. Issue the following CLI command to back up your configuration:

```
svcconfig backup
```

The following output is an example of the messages that are displayed during the backup process:

```
CMMVC6155I SVCCONFIG processing completed successfully
```

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

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

File name	Description
svc.config.backup.xml	This file that contains your configuration data.
svc.config.backup.sh	This file that contains the names of the commands that were issued to create the backup of the system.
svc.config.backup.log	This file contains details about the backup, including any error information that was reported.

6. Check that the **svcconfig backup** command completes successfully. 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 process again.

7. Issue the following command to exit the system:

exit

8. Issue the following command to copy the backup files to a location that is not in your system:

```
pscp -i ssh_private_key_file  
superuser@control_enclosure_management_IP:/tmp/svc.config.backup.*  
/offclusterstorage/
```

where *control_enclosure_management_IP* is the IP address or DNS name of the system and *offclusterstorage* is the location where you want to store the backup files.

If the configuration node changes, you must copy these files to a location outside of your system because the /tmp directory on this node canister becomes inaccessible. The configuration node might change in response to an error recovery action or to a user maintenance activity.

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

9. Ensure that the copies of the backup files are stored in the location that you specified in step 8.

You can rename the backup files to include the configuration node name either at the start or end of the file names so that you can easily identify these files when you are ready to restore your configuration.

Issue the following command to rename the backup files that are stored on a Linux or IBM AIX® host:

```
mv /offclusterstorage/svc.config.backup.xml  
/offclusterstorage/svc.config.backup.xml_myconfignode
```

where *offclusterstorage* is the name of the directory where the backup files are stored and *myconfignode* is the name of your configuration node.

To rename the backup files that are stored on a Windows host, right-click the name of the file and select **Rename**.

Deleting backup configuration files using the CLI

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

Perform the following steps to delete backup configuration files:

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

```
plink -i ssh_private_key_file superuser@control_enclosure_management_ip
```

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

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

```
svconfig clear -all
```

Chapter 6. Call home and remote support

This topic provides instructions for setting up call home support which transmits data with IBM support.

To set up call home support, perform the following steps:

1. Go to **Setting > Support** on the GUI.
2. Under the **Call home** tab, the **General** group displays. Click the **Edit** button at the bottom of the page.
3. Configure **Call home** by completing the text fields. Complete these fields:
 - a. Select the **Enable Call Home** check box. This field enables call home to transmit data with IBM support.
 - b. Complete the information for **Company**, **Customer Email**, and **Customer Phone Number** in case that a PMR must be created.
4. Select the **Outbound Connectivity** group. Complete the fields if the system is behind a proxy:
 - a. Check the **A proxy server is required to access internet** field.
 - b. The **Proxy Address** and **Proxy Port** fields appear. Fill in both fields.
 - c. If the proxy requires authentication, check the **Use Authentication** field:
 - d. Complete the information for the **User** and **Password** fields that appear.
5. Now, select the **Advanced** group and do the following:
 - a. Select the number of **Heart Beat Interval (Days)**, which is used to send small package with general information about the system health. The default is seven days.
 - b. **Machine location** contains information about the physical location of the system. Complete this field as appropriate for the location.
 - c. Enter **Special Instructions** that you want IBM Support to know about the system.
6. Save the new configuration by clicking the **OK** button.

Configuring the remote support system

IBM Storwize V7000 Unified uses IBM Tivoli Assist On Site software to establish remote connections to IBM support representatives.

Establishing an AOS connection

Use this information to establish an AOS connection with IBM remote support for diagnosing and reviewing issues and problems on your Storwize V7000 Unified system.

Before establishing a connection, be sure that you configure the system for AOS by using the Enable IBM Tivoli Assist On-Site (AOS).

AOS supports two different types of connections.

Lights on

Is a connection to the local console on the targeted file module. A lights-on connection requires that a keyboard, video, and mouse connection be made

on the targeted file module and that there is a physical person at the console for the duration of the remote system.

Lights out

Is a connection that allows for a remote support connection to be accepted automatically by the system.

Establishing a lights-out AOS connection

Use this information to establish a lights-out AOS connection with IBM remote support for diagnosing and reviewing issues and problems on your Storwize V7000 Unified system.

Configure the system for a lights-out connection using the Enable IBM Tivoli Assist On-Site (AOS) task.

After you configure the system, no other tasks are needed. The remote support contact might ask you for machine information, such as machine type and models, serial numbers, and your machine name. This information helps them locate the system within the back-end AOS connection point repository. The repository is an internal list that shows all available systems that are configured for lights-out connectivity.

Establishing a lights-on AOS connection

Use this information to establish a lights-on AOS connection with IBM remote support for diagnosing and reviewing issues and problems on your Storwize V7000 Unified system.

This procedure requires that a keyboard, video, and mouse is attached to the local Storwize V7000 Unified file module and that a customer representative is physically present at the connection for the duration of the remote support session.

To establish the AOS connection, perform the following steps:

Note: Each step at the beginning identifies whether the **remote IBM support representative** or the **customer** in the customer data center performs the step.

1. **Remote IBM support representative:** Start the connection process from your remote location.
 - a. Establish telephone or Sametime[®] communications to the IBM authorized servicer at the customer site to find out the problem maintenance request (PMR) number if you do not know it already, and the customer name and geography.
 - b. Open the AOS console and click the connect icon (the plug icon).
 - c. Enter your AOS user ID and password.
 - d. Select the HTTP link type of connection.
 - e. Enter the customer name, the case number (use the PMR number), and the geography.
 - f. Talk to the IBM authorized servicer at the customer site to make sure that the servicer is ready to establish the link before you submit the form.
 - g. Submit the form to the AOS server.
2. **Remote IBM support representative:** Wait for the AOS console to display the connection code when the AOS server returns the code.
3. **Remote IBM support representative:** Communicate the connection code to the IBM authorized servicer at the customer site.

Note: The connection code has a default timeout of 5 minutes. If the IBM authorized servicer at the customer site takes longer than 5 minutes to link to the AOS server, you can extend it for 5 minutes (twice). After the link is established, the link stays active until either you or the authorized servicer breaks the connection.

4. **Customer:** From the file module, log in as root and run **cnrs1launchaos**.
5. **Customer:** Enter the connection code that the IBM support representative gave you.

The script launches the Firefox browser and downloads the executable for establishing the AOS session. Confirm the file download. The file is stored in the /home/root/desktop directory.

6. **Customer:** When the executable file finishes downloading, close the Firefox download window and close the browser.

The launch script runs the AOS binary executable file that it downloaded.

7. **Customer:** Grant the IBM support representative the appropriate level of access (Active, Monitor, or Chat) according to customer security for conducting the maintenance action. For example, click **Active**.

Active mode gives full remote access.

Monitor mode restricts the IBM support representative to a view of the console, where the representative can offer guidance on what actions you might take to analyze and correct the problem.

Chat mode opens a chat window with no view of the console.

Chapter 7. Recovery procedures

This section covers the recovery procedures for the file modules and control enclosure.

User ID and system access

This section covers the recovery procedures for the topics that support the user ID and system access.

Accessing a file module as root

Some procedures require that you log on to a file module as root.

You can use the following methods to access a file module as root.

Access a file module as root.

- Type the following command in an X terminal, for example, a Windows or a Linux operating system:

```
ssh -p 1602 root@<file module IP>
```
- Use a Windows application like PuTTY to ssh to port 1602 of a file module service IP and log in as root with the root password that you recorded in your access information. See “Record access information” on page 3.

Recovering from losing the root password

Some recovery procedures require the root password to be entered for the file module.

If you have forgotten the file module root password, you can change it from any file module user ID that has sufficient authority to run the **chrootpwd** command successfully. If you do not have a user ID or if you have lost the password, then use this procedure to recover. You must have physical access to the file module to perform this procedure. Plug a keyboard and video monitor (KVM) directly into the front of one of the file modules. Stall the boot sequence at the Linux Grub boot loader screen.

To recover a lost root password, perform the following steps:

1. Check that the system is in good health by using the management GUI. Fix any hardware errors that do not require the root password.
2. Use the management GUI to identify the file module that is not the active management node and plug the KVM into that file module.
3. Log in to the management CLI as admin.
 - a. Issue the **suspendnode** command to remove the file module that is not the active management node from the system so that you can reboot it in single-user mode.
 - b. To remove the mgmt001st001 file module from the system, issue the following command

```
suspendnode mgmt001st001
```
4. To boot the Grub boot loader into single-user mode, log in as admin on the KVM. Issue the following Linux command:

```
shutdown -fr now
```

- a. Watch out for the grub boot screen on the KVM and select the kernel on the screen.
- b. Press the e key to edit the entry.
- c. Select the second line, the line that starts with the word kernel.
- d. Press the e key to edit the kernel entry to append single-user mode.
- e. Append the letter S or word Single to the end of the kernel line.

The following screen is an example.

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
  lists possible command completions. Anywhere else TAB lists the possible
  completions of a device/filename. ESC at any time exits. ]
```

```
grub edit> kernel /boot/vmlinuz-2.6.15-1-686 root=/dev/sda1 ro Single_
```

- f. Press the Enter key.
5. From the root shell, type **passwd**.
The passwd program prompts you for the new root password. This root password changes at the end of the procedure.
 6. Reboot the file module to normal mode. Issue the following command:

```
shutdown -fr now
```

 - a. Wait until the KVM goes past the Grub screen this time and log in when you are prompted to log in.
 - b. Log in as root with the new password on the KVM.
 7. Go back to the management CLI to resume the file module back in to the GPFS cluster.
 - a. Add the mgmt001st001 file module back to the system. Issue the following command:

```
resumenode mgmt001st001
```
 - b. Wait until the **lsnode** command shows that there are 2 online nodes in the cluster.
 8. From the KVM where you logged on as root, use the **chrootpwd** command to change the root password on both file modules.

The chrootpwd program prompts you for the new root password.

The chrootpwd program sets the new root password on both file modules in the cluster.

Resetting the NAS ssh key for configuration communications

The configuration communications between the Storwize V7000 file modules and the control enclosure are done by using ssh over the site 1 Gbps Ethernet LAN; whereas the file data traffic is passed over the direct connect Fibre Channel links by using the SCSI protocol.

During the USB initialization of the Storwize V7000 Unified system, one of the node canisters in the control enclosure creates a public/private key pair to use for ssh. The node canister stores the public key and writes the private key to the USB key memory.

One of the file modules then takes the private key from the USB key memory to use for ssh. The file module passes it to the other file module over the direct connect Ethernet link and then deletes the private key from the USB key memory so that it cannot be used on the wrong system.

It might be necessary to reset the NAS ssh key in the following circumstances:

- When communications between the Storwize V7000 file module and the Storwize V7000 control enclosure is not authorized because of a bad key.
- When both Storwize V7000 file modules have lost the original NAS ssh key.
- When the Storwize V7000 control enclosure has lost the NAS ssh key.

Perform the following steps to reset the NAS ssh key so that the communications between the file modules and the Storwize V7000 control enclosure resume:

1. Log on to the Storwize V7000 control enclosure management CLI as superuser:

```
satask chnaskey -privkeyfile NAS.ppk
```

The private key is left in the /dumps directory.

2. Use SCP to copy the private key file to the Storwize V7000 file module:

```
scp -P 1602 /dumps/NAS.ppk root@<file module management IP>:/files
```

You are prompted for the file module root password.

3. Log on to the Storwize V7000 Unified management CLI as admin:

```
chstoragesystem --sonasprivkey/files
```

Working with NFS clients that fail to mount NFS shares after a client IP change

Use this information to resolve a refused mount or Stale NFS file handle response to an attempt to mount Network File System (NFS) shares after a client IP change.

After a client IP change, a **df -h** command returns no results as shown in the following example:

```
Filesystem          Size  Used Avail Use% Mounted on
machinename: filename: -    -    -    -    /sharename
```

Also, you can see the following error from the **ls** command:

```
ls: .: Stale NFS file handle
```

Also, the hosting file module in the Storwize V7000 Unified system displays the following error:

```
mgmt002st001 mountd[3055867]: refused mount
request from hostname for sharename (/): not exported
```

If you receive one of the errors above, perform the following steps:

1. Access the file module that hosts the active management node role using root privileges. Then issue the following command to flush the NFS cache in each file module: **onnode all /usr/sbin/exportfs -a**.

Verify that the NFS mount is successful. If the problem persists, restart the NFS service on the file module that is refusing the mount requests from that client.

2. Verify that the NFS share mount is successful.

Working with file modules that report a stale NFS file handle

To recover from a file system state of “Stale NFS file handle” on a file module, you must suspend, reboot, and resume the file module.

Note: If “Stale NFS file handle” was displayed after a client IP change, refer to “Working with NFS clients that fail to mount NFS shares after a client IP change” on page 253.

Due to errors or conditions related to this file module, the file module disconnected itself from the shared file system with the other nodes. All of the file descriptors opened to the file system through this file module have become “stale”—as indicated by command output or an error message denoting a Stale NFS file handle—and cannot access their corresponding files. When this occurs, all affected file modules enter an unhealthy state, and a CIM similar to the following is sent to the alert log:

```
GPFS Error - check stale file handle failed with error code 1:
  see stale file handle on /ibm/gpfs0 on file module: mgmt001st001
```

If you receive the error above, perform the following steps:

1. Open the CLI in the active management node using root privileges and issue `/usr/sbin/exportfs -a` to flush the NFS cache in each file module. Verify that the state of each affected file module is healthy and that no new “Stale NFS file handle” CIMs appear in the alert log after resuming the file module. If the problem persists, proceed through the following steps.
2. Review the event log to identify the affected file system and all of the nodes where the file system has a state of “Stale NFS file handle”.
3. Suspend each affected file module.
4. Reboot each affected file module.
5. Resume each affected file module.
6. Verify that the state of each affected file module is healthy and that no new “Stale NFS file handle” CIMs appear in the alert log after resuming the file module.

File module-related issues

This section covers the recovery procedures related to file module issues.

Restoring System x firmware (BIOS) settings

During critical repair actions such as the replacement of a system planar in an IBM Storwize V7000 Unified file module, you might have to reset the System x firmware.

The firmware and software code package for the Storwize V7000 Unified microcode can automatically configure the default settings for the System x firmware to the required Storwize V7000 Unified settings. However, to enable the automatic configuration, you must reset the System x firmware from its current state to the default configuration.

Use the following procedure to set the System x firmware to the default state and start the automatic Storwize V7000 Unified configuration.

1. SSH to the affected file module.
2. Turn on the affected file module.

3. From the IBM System x Server Firmware screen, press **F1** to set up the firmware.
A few seconds after the IBM System x Server Firmware screen is displayed, F1 and other options are displayed at the bottom of the screen:
 - F1 - Setup
 - F2 - Diagnostics
 - F12 - Select Boot Device
4. From the System Configuration and Boot Management screen, scroll down to click **Load Default Settings**, and then press **Enter**.
The screen goes blank for a few seconds and then returns to the System Configuration and Boot Management screen.
5. Click **System Settings > Integrated Management Module > Network Configuration > DHCP Control > Static IP**
6. Specify the IP address, the subnet mask, and the default gateway.
For example, the static IP address for the mgmt001st001 file module is found from the management node terminal, using an appropriate command, such as `cat /etc/hosts |grep mgmt001st001`.
The subnet mask is always **255.255.128.0**.
The gateway IP address is **0.0.0.0**.
7. Click **Save**.
8. A window displays a prompt to ask to reset the IMM now. Select **Y**.
9. Press **ESC** twice to return to the System Configuration and Boot Management screen.
10. Scroll down to click **Boot Manager**, and then press **Enter**.
11. Scroll down to click **Add Boot Option**, and then press **Enter**.
12. Scroll down to click **Legacy Only**, and then press **Enter**.
The option is not visible until you scroll down. Selecting the option removes it from the list of available options.
13. Press **ESC** twice to return to the System Configuration and Boot Management screen.
14. Scroll down to click **Save Settings**, and then press **Enter**.
15. Press **ESC** or click **Exit Setup**, and then press **Enter**.
16. When prompted, click **Y** to exit the setup menu.
The system now reboots. During the reboot, the Storwize V7000 Unified code automatically modifies the configuration of the System x firmware (BIOS) to change the default settings to the required settings.

Recovering from a multipath event

Use this procedure to recover a node from a **multipathd** failure.

Use this procedure after completing the procedure in “Fibre connectivity between file modules and control enclosure” on page 26.

The Storwize V7000 Unified system can experience problems where the **multipathd** failures occur. If the paths are not automatically restored, a system reboot can recover the paths.

Important: Perform this procedure against the passive management node only.

1. Verify that the node that the **multipathd** event occurred against is the passive management node. If the node that experiences the **multipathd** problems is the active node, then perform the management node failover procedure. See “Performing management node role failover on a “good” system” on page 153.
2. Reboot the file module. See “Rebooting a file module” on page 47.

Diagnosing a multipath event

The **multipath -ll** command verifies that all storage devices are either active or not active.

The following output shows that all storage devices are active.

```
[root@yourmachine.mgmt001st001 ~]# multipath -ll
array1_sas_89360007 (360001ff070e9c0000000001989360007) fm-0 IBM,2073-700
[size=3.1T][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=50][active]
\_ 6:0:0:0 sdb 8:16 [active][ready]
\_ round-robin 0 [prio=10][enabled]
\_ 8:0:0:0 sdg 8:96 [active][ready]
array1_sas_89380009 (360001ff070e9c0000000001b89380009) fm-1 IBM,2073-700
[size=3.1T][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=50][active]
\_ 6:0:0:2 sdd 8:48 [active][ready]
\_ round-robin 0 [prio=10][enabled]
\_ 8:0:0:2 sdi 8:128 [active][ready]
```

The following output shows that the storage devices are not active.

```
[root@kd271f6.mgmt002st001 ~]# multipath -ll
mpathq (360050768029180b06000000000000007) dm-8 IBM,2145
size=2.5G features='1 queue_if_no_path' hwhandler='0' wp=rw
| ^- 5:0:0:7 sdr 65:16 failed ready running
^- 6:0:0:7 sdi 8:128 failed ready running
mpathp (360050768029180b06000000000000005) dm-3 IBM,2145
size=2.5G features='1 queue_if_no_path' hwhandler='0' wp=rw
| ^- 5:0:0:5 sdp 8:240 failed ready running
^- 6:0:0:5 sdg 8:96 failed ready running
```

The output `[active][ready]` identifies an active device. The output `failed ready running` identifies a device that is not active.

Recovering from an NFSD service error

Use this procedure to recover from an NFSD service error.

This recovery procedure starts the NFSD when it is down.

1. Log in as root.
2. Issue the **service nfsd start** command.
3. If the problem persists, restart the node.
4. If the restart action does not resolve the issue, contact the next level of support.

Recovering from an SCM error

Use this procedure to recover from a service configuration management (SCM) error.

Complete the following procedure if output from the **lshhealth -r** CLI command contains a line similar to the following:

```
SCM ERROR SCM system has found some errors
```


Note: This procedure involves analyzing various logs depending on the errors displayed by the initial SCM error log.

1. Open the CNSCM log located at `/var/log/cnlog/cnscm` for the file module that reported the error.
2. Review the error entries around the listed time stamp and then check the log for issues that seem related that occurred before the listed time stamp. For example, you might find GPFS-related issues appearing earlier and later, too.
3. Based on the log entries, check the appropriate corresponding log. If the issue appeared to be related to GPFS, for example, you could look for the root cause in `/var/adm/ras/mmfs.log`.
4. Continue to evaluate and analyze the logs until you resolve the error.

Recovering from an httpd service error

Use this procedure to recover from an httpd service error when the service is reported as unhealthy or off.

To fix the httpd error, perform the following steps:

1. Attempt to start the http service manually.
 - a. Log in as root.
 - b. Issue the **service http start** command.
2. When you complete the service action, refer to “Health status and recovery” on page 21.

Recovering from an sshd_data service error

Use this procedure to recover from an sshd_data service error.

This recovery procedure starts the sshd_data when it is down.

1. Log in as root.
2. Issue the service **sshd_data start** command.
3. If the problem persists, restart the node.
4. If the restart action does not resolve the issue, contact the next level of support.

Recovering from an sshd_int service error

Use this procedure to recover from an sshd_int service error.

This recovery procedure starts the sshd_int when it is down.

1. Log in as root.
2. Issue the service **sshd_int start** command.
3. If the problem persists, restart the node.
4. If the restart action does not resolve the issue, contact the next level of support.

Recovering from an sshd_mgmt service error

Use this procedure to recover from an sshd_mgmt service error.

This recovery procedure starts the sshd_mgmt when it is down.

1. Log in as root.
2. Issue the service **sshd_mgmt start** command.
3. If the problem persists, restart the node.
4. If the restart action does not resolve the issue, contact the next level of support.

Recovering from an sshd_service service error

Use this procedure to recover from an sshd_service service error.

This recovery procedure starts the sshd_service when it is down.

1. Log in as root.
2. Issue the service **sshd_service start** command.
3. If the problem persists, restart the node.
4. If the restart action does not resolve the issue, contact the next level of support.

Control enclosure-related issues

This section covers the recovery procedures that involve control enclosure issues.

Recovering when file volumes come back online

Use this procedure to recover a file system after all the file volumes are back online after a repair or recovery action.

Each fix procedure that brings the file volumes back online also suggests that you run this procedure. This procedure checks that the file systems have also come back online.

Perform the following steps to check that the file systems are back online after their file volumes are back online following an outage.

1. In the management GUI, check that all volumes are back online.
2. Go to **Monitoring > Events** and click the **Block** tab.
3. Run any **Next recommended action**.
4. When all volumes are back online, go to **Filesystems** in the management GUI.
5. If any file systems are not online, recover them by using the recover a GPFS file system procedure. See “Recovering a GPFS file system” on page 162.
6. If there are file systems that have not come back online, go to **Monitoring > Events** and click the **File** tab to fix any errors.
7. If there are any stale NFS handle errors for the offline file systems, follow the “Working with file modules that report a stale NFS file handle” on page 254.

Recovering when a file volume does not come back online

An offline volume can normally be fixed by performing the fix procedures in the management GUI.

To run the fix procedures, perform the following steps:

1. Log in to the Storwize V7000 Unified management GUI.
2. Go to **Monitoring > Events** and click the **Block** tab.
3. Run any **Next recommended action**.

If the fix procedures do not bring back a file system volume online, contact your service provider for assistance.

Recovering from a 1001 error code

A 1001 error code indicates that the Storwize V7000 control enclosure has automatically performed a recovery. The CLI is now restricted to make sure that

there are no more configuration changes until IBM support has checked that it is safe for configuration changes to be allowed again.

The problem that caused the recovery to be triggered might have caused the file volumes to go offline long enough to cause the file systems to become unmounted. You can immediately remount the file systems without waiting for IBM support to tell you that it is safe for you to re-enable the Storwize V7000 CLI. See “Checking the GPFS file system mount on each file module” on page 157.

There is a known issue with the Fibre Channel adapter. The adapter stops scanning for LUNs if the adapter cannot detect any. When this situation happens, the multipath does not have any active connections to the volumes on the Storwize V7000.

The most reliable work-around for this situation is to reboot each of the file modules in turn by using the following procedure:

1. Reboot the active management node by using the **initnode -r** command. The active management node fails over to the other file module first before rebooting.
2. Wait for a few minutes before you log back on to the CLI and watch for the rebooting file module to come back up completely by using the **lsmodule -r** command.

This action can take approximately 10 minutes.

Note: The **-r** is important; it refreshes the CLI database so that you see the real state of the file modules.

3. When both file modules are up, use the **initnode -r** command to reboot the file module that is now the active management node.
The active management node fails over to the file module that you rebooted first.
4. Wait a few minutes before you log back on to the Storwize V7000 Unified CLI and watch for the rebooting file module to come back up completely by using the **lsmodule -r** command.

This action can take approximately 10 minutes.

5. When both file modules are back up, they automatically remount the file systems.
6. Check that the file systems are mounted by using the **lsmount -r** management CLI command.

The management GUI becomes very slow when the Storwize V7000 CLI is restricted. When you log on to the management GUI, it issues a warning that the Storwize V7000 CLI is restricted. The management GUI runs the fix procedure to direct you to send logs to IBM. The management GUI also directs you back to this procedure to make the file systems accessible again.

To collect the Storwize V7000 logs, select the **Collect Logs** option from the navigation in the service assistant. Select **With statesave**.

Restoring data

This section covers the recovery procedures that relate to restoring data.

Restoring asynchronous data

Recovering a file system with asynchronous replication requires that you configure and start a replication relationship from the target site to the source site.

After the source site (site A) has failed, set the target site (Site B) as the new source site and replicate back to Site A. To restore asynchronous data, perform the following steps:

1. Where the previous replication relationship was Site A replicating to Site B, configure the asynchronous replication by reversing the source and target site information. Site B replicates to Site A. See “Configuring asynchronous replication” and transpose the source and target information.
2. Start the replication that was configured in step 1 by using the **startrepl -fullsync** CLI command. See “Starting and stopping asynchronous replication” for more information.
3. If the amount of data that is to be replicated back to Site A is large, multiple replications from Site B to Site A might be required. Multiple replications are required until modifications to Site B can be suspended to perform a final replication to Site A to enable Site A to synch up.

Note: Do not use the **fullsync** option for these incremental replications.

4. After you verify that the data on Site A has been replicated accurately, you can reconfigure Site A as the primary site. Remove any replication tasks from Site B to Site A by using the **rmtask** CLI command.

Restoring Tivoli Storage Manager data

The Storwize V7000 Unified system contains a Tivoli Storage Manager client that works with your Tivoli Storage Manager server system to perform high-speed data backup and recovery operations.

Before restoring a file system, determine whether a backup is running and when backups were completed. To restore the data, perform the following steps:

1. Determine whether a backup is running and when backups were completed by running the **lsbackup** CLI command. Specify the file system.

For example, the command to display the gpfs0 file system backup listing shows the output in the following format:

```
# lsbackup gpfs0 Filesystem Date
Message gpfs0 20.01.2010 02:00:00.000 G0300IEFSSG0300I The filesystem
gpfs0 backup started. gpfs0 19.01.2010 06:10:00.123 G0702IEFSSG0702I The
filesystem gpfs0 backup was done successfully. gpfs0 15.01.2010
02:00:00.000 G0300IEFSSG0300I The filesystem gpfs0 backup started.
```

2. Restore the backup by using the **startrestore** CLI command. Specify a file system name pattern.

You cannot restore two file systems at the same time; therefore, the file pattern cannot match more than one file system name.

Use the **-t** option to specify a date and time in the format "dd.MM.yyyyHH:mm:ss.SSS" to restore files as they existed at that time. If a time is not specified, the most recently backed up versions are restored. For example, to restore the `/ibm/gpfs0/temp/*` file pattern to its backed up state as of January 19, 2010 at 12:45 PM, enter the following command:

```
# startrestore "/ibm/gpfs0/temp/*" -t "19.01.2010 12:45:00.000"
```

See the **startrestore** CLI command for additional command information, default options, and file pattern examples.

Attention: The **-R** option overwrites files and has the potential to overwrite newer files with older data.

3. Use the **lsbackupfs** CLI command to determine whether a restore is running. The **Message** field displays **RESTORE_RUNNING** if a restore is running on a file system.
4. Monitor the progress of the restore process by using the **QUERY SESSION** command in the Tivoli Storage Manager administrative CLI client.
Run this command twice and compare the values in the Bytes Sent column of the output. Incremental values indicate that the process is in progress; whereas, identical values indicate that the restore process has stopped.

Note: The following error message can occur while restoring millions of files:
ANS1030E The operating system refused a TSM request for memory allocation. 2010-07-09 15:51:54-05:00 dsmc return code: 12

If the file system is managed by Tivoli Storage Manager for Space Management, break down the restore into smaller file patterns or subdirectories that contain fewer files.

If the file system is not managed by Tivoli Storage Manager for Space Management, try to force a no-query-restore (NQR) by altering the path that is specified for the restore. To do this action, include all files by putting a wildcard ("*") after the file system path:

```
# startrestore "ibm/gpfs0/*"
```

This example attempts a no query restore, which minimizes memory issues with the Tivoli Storage Manager client because the Tivoli Storage Manager server does the optimization of the file list. If you are still unable to restore a larger number of files at the same time, break down the restore into smaller file patterns or subdirectories that contain fewer files.

Upgrade recovery

This section covers the recovery procedures that relate to upgrade.

Error codes and recommendations when running the **applysoftware** command

If any errors are posted after you issue the **applysoftware** command, see Table 44 and take the described course of action. Follow these guidelines:

1. Follow the actions in the order presented.
2. After each recommended fix, restart the upgrade by issuing the **applysoftware** command again. If the action fails, try the next recommended action.
3. If the recommended actions fail to resolve the issue, call the IBM Support Center.

*Table 44. Upgrade error codes from using the **applysoftware** command and recommended actions*

Error Code	The applysoftware command explanation	Action
EFSSG4100	The command completed successfully.	None.

Table 44. Upgrade error codes from using the **applysoftware** command and recommended actions (continued)

Error Code	The applysoftware command explanation	Action
EFSSG4101	The required parameter was not specified.	Check the command and verify that the parameters are entered correctly.
EFSSG4102	The software package does not exist.	Verify that the file actually exists where specified. Also verify that the command is passing the correct location parameters.
EFSSG4103	The software package is not valid.	The package might be corrupt. If this problem persists, download a new package and try again.
EFSSG4104	An unexpected return code.	Call your next level of support.
EFSSG4105	Unable to mount the USB flash drive.	Run <code>umount /media/usb</code> , then remove the USB flash drive. Reinsert the USB flash drive. If the error persists, remove the USB flash drive and reboot. After the system reboots, reinsert the USB flash drive.
EFSSG4153	The required parameter was not specified.	Verify that the file actually exists where specified. Also verify that the command is passing the correct location parameters.
EFSSG4154	You must start on primary management node <code>mgmt001st001</code> .	Switch to the other node and try the command again.
EFSSG4155	Unable to mount USB flash drive.	Back up to a USB flash drive. Enter <code># backupmanagementnode --umount /media/usb</code> . Remove the USB flash drive and insert again. If the error persists, remove the USB flash drive and reboot. When the system is running, insert the USB flash drive again.
EFSSG4156	The specified International Organization for Standardization (ISO) does not exist.	Verify that the file actually exists where specified. Also verify that the command is passing the correct location parameters.
EFSSG4157	The specific upgrade International Organization for Standardization (ISO) content is not valid.	The package might be corrupt. If this problem persists, download a new package and try again.

Table 44. Upgrade error codes from using the **applysoftware** command and recommended actions (continued)

Error Code	The applysoftware command explanation	Action
EFSSG4158	The specific upgrade cannot be installed over the current version.	Check the upgrade documentation and verify that the level you are coming from is compatible with the level you are going to. If the upgrade level is not compatible, download the correct level and try again. If the upgrade level is compatible and the error persists, call the IBM Support Center.
EFSSG4159	The system is in an unhealthy state and the upgrade cannot start.	See Chapter 3, "Getting started troubleshooting," on page 9. Determine if the system has issues.
EFSSG4160	The system has insufficient file system space.	At least 3 GB of space is required. Remove unneeded files from the /var file system.

General upgrade error codes and recommended actions

If any errors are posted during the upgrade process, see Table 45 and take the described course of action. If the error you see is not listed in this table, call the IBM Support Center. Follow these guidelines:

1. Follow the actions in the order presented.
2. After each recommended fix, restart the upgrade by issuing the **applysoftware** command again. If the action fails, try the next recommended action.
3. If the recommended actions fail to resolve the issue, call the IBM Support Center.

Table 45. Upgrade error codes and recommended actions

Error Code	Explanation	Action
019A	Yum update failed.	Contact your next level of support.
019B	Unable to remove StartBackupTSM task.	Enter the lscluster command to verify that the management service is running on the active node. (The command fails if the management service is not running on the active node.) If the command fails, type startmgtsrv to start it.
019C	Unable to determine active management node.	Enter the lscluster command to verify that the management service is running on the active node. (The command fails if the management service is not running on the active node.) If the command fails, type startmgtsrv to start it.

Table 45. Upgrade error codes and recommended actions (continued)

Error Code	Explanation	Action
019D	Check the system health.	Type <code>lsnode</code> to determine which node is unhealthy (CTDB or GPFS). Reboot the unhealthy node and wait for the node to come back up. Then check the health of the node by entering <code>lsnode</code> .
019E	Internal error system or node not provided	Contact your next level of support.
019F	CIM failed to start again.	Contact your next level of support.
01A0	Failed to reboot.	Determine the cause of the failed reboot: <ol style="list-style-type: none"> 1. Connect to the system console on the node that failed to reboot. <ol style="list-style-type: none"> a. Investigate and correct any problems identified from the console output. 2. Verify that all cables are connected correctly to the system. 3. Review the light path diagnostics for any error indications. <ol style="list-style-type: none"> a. Correct any problems identified, then reboot the node from the system console. b. If it is not possible to reboot the node from the system console, then use the power button on the front of the server to power-cycle the system. c. After the system reboots, restart the upgrade process.
01A1	Internal upgrade error.	Contact your next level of support.
01A3	Unable to uninstall CNCSM callbacks.	Contact your next level of support.
01A4	Unable to stop backup jobs.	<ol style="list-style-type: none"> 1. Check the status of the backups by typing <code>lsjobstatus -j backup</code>. 2. Attempt to stop the backups by typing <code>stopbackup --all</code>. Then check the status again to see if backups are stopping.
01A5	Backup cron jobs are running.	<ol style="list-style-type: none"> 1. Check the condition of tasks by typing <code>lstask -t cron</code>. 2. Attempt to remove the backup by typing <code>rmtask StartBackupTSM</code>.
01A6	Unable to install CNCSM callbacks.	Contact your next level of support.
01A7	Internal vital product data (VPD) error.	Contact your next level of support.
01A8	Check the health of management service.	Attempt to start the management service by typing <code>startmgtsrv</code> on the passive management node.
01A9	Unable to stop performance collection daemon.	Contact your next level of support.

Table 45. Upgrade error codes and recommended actions (continued)

Error Code	Explanation	Action
01AB	Internal upgrade error in <code>node_setup_system</code> .	Contact your next level of support.
01B1	Management node replication failed.	1. Go to "Resolving issues reported for lshealth " on page 163. 2. Contact your next level of support.
01B2	Unable to start performance collection daemon.	Contact your next level of support.
01B3	Failed to copy upgrade package to Storwize V7000.	See Chapter 5, "Control enclosure," on page 167.
01B4	Failed to start upgrade on Storwize V7000 with the applysoftware command.	See Chapter 5, "Control enclosure," on page 167.
01B5	Storwize V7000 multipaths are unhealthy.	Check the Fibre Channel connections to the system. Reseat Fibre Channel cables. For more information, see "Mounting a file system" in the <i>IBM Storwize V7000 Unified Information Center</i> .
01B6	System volumes are unhealthy as indicated by using the lsdisk command.	See Chapter 5, "Control enclosure," on page 167.
01B7	Failed to query status of upgrade by using the lssoftwareupgradestatus command.	See Chapter 5, "Control enclosure," on page 167.
01B8	Failed to query status of Storwize V7000 nodes by using the svcinfolnode command.	See Chapter 5, "Control enclosure," on page 167.
01B9	Failed to check the Storwize V7000 version.	See Chapter 5, "Control enclosure," on page 167.
01BA	Unable to verify the correct software version.	Contact your next level of support.
01BC	Check the health of DDN storage systems.	Contact your next level of support.
01BD	Unable to update software repository.	Contact your next level of support.
01BE	Unable to distribute upgrade callbacks.	Contact your next level of support.
01C0	Asynchronous replication is running. Stop asynchronous replication and continue with the upgrade.	Stop asynchronous replication by typing <code>stoprepl gpfs0 --kill</code> .
01C1	Asynchronous replication failed to stop. Stop asynchronous replication and continue with the upgrade.	Stop asynchronous replication by typing <code>stoprepl gpfs0 --kill</code> .
01C2	Failed while checking for current running asynchronous jobs.	Type <code>lsrepl;echo \$?</code> . If the return code is 0, start the upgrade again. If the return code is any other number, contact your next level of support.

Table 45. Upgrade error codes and recommended actions (continued)

Error Code	Explanation	Action
01C3	Could not stop CTDB.	Contact your next level of support.
01C5	Could not reinstall Lib_Utils.	Contact your next level of support.
01C6	Failed while running sonas_update_yum.	Contact your next level of support.
01C8	Failed while running cnrssconfig.	Contact your next level of support.
01C9	Unable to install CIM configuration.	Contact your next level of support.
01CB	Unable to install GPFS packages.	Contact your next level of support.
01CC	Could not install platform. Upgrade on target system.	Contact your next level of support.
01CD	Unable to mount GPFS file systems.	See "Checking the GPFS file system mount on each file module" on page 157.
01CF	Unable to configure node.	Contact your next level of support.
01D0	Unable to disable call home.	Contact your next level of support.
01D1	Unable to enable call home.	Contact your next level of support.
01D2	Failed to stop GPFS.	Contact your next level of support.
01D3	Could not determine if backups are running.	Type <code>lsjobstatus -j backup;echo \$?</code> . If the return code is 0, start the upgrade again. If the return code is any other number, contact your next level of support.
01D5	Storwize V7000 stalled_non_redundant.	Contact your next level of support.
01D6	Storwize V7000 system stalled.	Contact your next level of support.
01D8	CTDB system is unhealthy.	See "Checking CTDB health" on page 155.
01DA	GPFS system is unhealthy.	See "Checking the GPFS file system mount on each file module" on page 157.
01DB	Failed to stop performance center.	Contact your next level of support.
01DC	Failed to configure performance center.	Contact your next level of support.
01DD	Failed to start performance center.	Contact your next level of support.
01E0	HSM upgrade failed.	Contact your next level of support.

Appendix. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Features

This list includes the major accessibility features in the management GUI:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. The following screen reader has been tested: JAWS 11.
- Most of the GUI features are accessible by using the keyboard. For those features that are not accessible, equivalent function is available by using the command-line interface (CLI).

Navigating by keyboard

You can use keys or key combinations to perform operations and initiate many menu actions that can also be done through mouse actions. You can navigate the management GUI and help system from the keyboard by using the following key combinations:

- To navigate between different GUI panels, select the Low-graphics mode option on the GUI login panel. You can use this option to navigate to all the panels without manually typing the web addresses.
- To go to the next frame, press Ctrl+Tab.
- To move to the previous frame, press Shift+Ctrl+Tab.
- To navigate to the next link, button, or topic within a panel, press Tab inside a frame (page).
- To move to the previous link, button, or topic within a panel, press Shift+Tab.
- To select GUI objects, press Enter.
- To print the current page or active frame, press Ctrl+P.
- To expand a tree node, press the Right Arrow key. To collapse a tree node, press the Left Arrow key.
- To scroll all the way up, press Home; to scroll all the way down, press End.
- To go back, press Alt+Left Arrow key.
- To go forward, press Alt+Right Arrow key.
- For actions menus:
 - Press Tab to navigate to the grid header.
 - Press the Left or Right Arrow keys to reach the drop-down field.
 - Press Enter to open the drop-down menu.
 - Press the Up or Down Arrow keys to select the menu items.
 - Press Enter to launch the action.
- For filter panes:
 - Press Tab to navigate to the filter panes.
 - Press the Up or Down Arrow keys to change the filter or navigation for nonselection.

- Press Tab to navigate to the magnifying glass icon in the filter pane and press Enter.
- Type the filter text.
- Press Tab to navigate to the red X icon and press Enter to reset the filter.
- For information areas:
 - Press Tab to navigate to information areas.
 - Press Tab to navigate to the fields that are available for editing.
 - Type your edit and press Enter to issue the change command.

Accessing the publications

You can find the HTML version of the IBM Storwize V7000 Unified information at the following website:

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

You can access this information using screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. The information was tested using the following screen reader: JAWS Version 10 or later.

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 give 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 (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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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
Bldg 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 measurement 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 may be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application

programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, 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.

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Xeon, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Electronic emission notices

The following electronic emission statements apply to this product. The statements for other products that are intended for use with this product are included in their accompanying documentation.

Federal Communications Commission (FCC) statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
E-mail: [mailto: tjahn @ de.ibm.com](mailto:tjahn@de.ibm.com)

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

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
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
e-mail: [mailto: tjahn @ de.ibm.com](mailto:tjahn@de.ibm.com)

**Generelle Informationen: Das Gerät erfüllt die
Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Japan VCCI Council Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

People's Republic of China Class A Electronic Emission Statement

中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

International Electrotechnical Commission (IEC) statement

This product has been designed and built to comply with (IEC) Standard 950.

Korean Communications Commission (KCC) Class A Statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу A.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

russemi

Taiwan Class A compliance statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。^{taitemi}

European Contact Information

This topic contains the product service contact information for Europe.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
Email: [mailto: tjahn @ de.ibm.com](mailto:tjahn@de.ibm.com)

Taiwan Contact Information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Index

Numerics

- 10-Gbps Ethernet PCI adapter
 - removing 101
- 2.5" drive assembly
 - replacing 223
- 240 VA safety cover
 - installing 150
 - removing 149
- 3.5" drive assembly
 - replacing 221

A

- about this document
 - sending comments xxii
- accessibility
 - keyboard 267
 - repeat rate
 - up and down buttons 267
 - shortcut keys 267
- accessing
 - canisters
 - Ethernet cable 201
 - management GUI 43
 - publications 267
 - service assistant 168, 203
 - service CLI 170
 - system CLI 169
- actions
 - reset service IP address 172
 - reset superuser password 172
- adapter
 - installing 99, 101, 102
- adapter bracket
 - storing full-length 106
- advanced feature key
 - installing 118
 - removing 117
- air baffle
 - DIMM
 - installing 90
 - removing 89
 - microprocessor
 - installing 88
 - removing 86
- alerts
 - best practices 6
- ANSI267E 163
- AOS connection
 - establishing 247
- apply software command 174
- authenticating
 - trouble 159

B

- backing up
 - best practices 5
 - system configuration files 243

- backup configuration files
 - deleting
 - using the CLI 245
- bad blocks 181
- battery
 - maintenance 179, 180
 - removing 81, 218
 - replacing 85
- best practices
 - alerts 6
 - backing up data 5
 - drive characteristics 5
 - IP address 3
 - notifications 4
 - passwords 3
 - power management 4
 - RAID 5
 - record
 - location information 6
 - subscribe
 - notifications 6
 - troubleshooting 3
 - warranty agreement
 - maintenance agreement 7
- blank carrier
 - replacing 221, 223
- browsers
 - supported 188

C

- cable retention bracket
 - releasing 221
- call home support 247
- Canadian electronic emission notice 272
- canister
 - expansion 206
 - identification 191
 - node 204
 - replacing 204, 206
- CD drive 124, 125
- CD-RW/DVD drive
 - installing 125
 - removing 124
 - replacing 125
- changing
 - service IP address 200
- CLI
 - service commands 169
 - storage system commands 169
- CLI commands
 - configuration
 - installation problems 18
- client access
 - pinging 161
- clustered storage system
 - failure to create 185
- clustered system
 - restore 241
- clustered systems
 - restore 237

- clustered systems (*continued*)
 - T3 recovery 237
- commands
 - apply software 174
 - create cluster 174
 - query status 175
 - reset service assistant password 173
 - satask.txt 171
 - snap 173
 - svcconfig backup 243
- comments, sending xxii
- component or device
 - returning 52
- components
 - hardware 1
- configuring remote support 247
- connectivity issues
 - during installation 22
- contact information
 - European 275
 - Taiwan 275
- control enclosure chassis
 - replacing 225
- cover
 - installing 80
 - removing 79
- create cluster command 174
- CRUs, replacing
 - cover 80
- CTDB
 - checking health 155
- Customer replaceable units (CRUs) 77

D

- deleting
 - backup configuration files
 - using the CLI 245
 - system 199
- detection error
 - expansion location 189
- determining
 - SAN problem 234
- Deutschsprachiger EU Hinweis 273
- device or component
 - returning 52
- DIMMs
 - installing 127
 - removing 126
- documentation
 - improvement xxii
- drive characteristics
 - best practices 5
- drive, hot-swap, installing 116
- DVD drive 124, 125

E

- electronic emission notices
 - Avis de conformité à la réglementation d'Industrie Canada 272
 - Deutschsprachiger EU Hinweis 273
 - European Union (EU) 272
 - Federal Communications Commission (FCC) 271
 - French Canadian 272
 - Germany 273
 - Industry Canada 272
 - International Electrotechnical Commission (IEC) 274
 - Japanese Voluntary Control Council for Interference (VCCI) 274
 - Korean 274
 - New Zealand 272
 - People's Republic of China 274
 - Taiwan 275
- EMC statement, People's Republic of China 274
- enclosure 37
 - hardware indicators 37
 - identification 191
- enclosure end cap
 - replacing 224
- environmental notices xi
- error
 - expansion enclosure 189
 - node canister 188
 - not detected 189
 - SAS cabling 188
 - USB key 190
- error codes
 - understanding 72, 178
 - upgrading 261
- error events 176
- errors
 - logs
 - describing the fields 176
 - error events 176
 - managing 176
 - understanding 176
 - viewing 176
 - power supply LEDs 36
- Errors and messages 72
- establishing
 - AOS connection 247
 - lights-on AOS connection 248
 - lights-out AOS connection 248
- Ethernet
 - accessing
 - canister 201
 - status 198
- European contact information 275
- European Union (EU), EMC Directive conformance statement 272
- event IDs 178
 - understanding 76
- event notification 177
- events
 - reporting 175
- expansion enclosure
 - detection error 189
 - replacing 230

F

- failover procedures
 - management node role 152
- failover procedures for management node role 154
- failure
 - storage system creation 185
- fan bracket
 - installing 92
 - removal 91
- FCC (Federal Communications Commission) electronic emission notice 271
- feature key
 - installing 118
 - removing 117
- Federal Communications Commission (FCC) electronic emission notice 271
- Fibre Channel
 - link failures 235
 - SFP transceiver 235
- Fibre Channel PCI adapter
 - removing 101
- Field replaceable units (FRUs) 77
- fields
 - event log 176
- file module
 - removal 47
 - removing and replacing 50
 - time synchronization 165
- file module FRUs
 - installation guidelines 50
- file module reliability guidelines 51
- file module to control enclosure connectivity troubleshooting 25
- File module to file module 24
- file node hardware indicators 29
- file system mounts
 - gpfs, troubleshooting 157
 - identifying created and mounted file systems 157
 - missing 158
- finding
 - Ethernet
 - status 198
- firmware
 - System x, restoring 254
- fix
 - errors 238
- fixing
 - node errors 199
- French Canadian electronic emission notice 272
- FRU
 - install
 - 240 VA safety cover 150
 - installing
 - 10-Gbps Ethernet PCI adapter 102
 - DIMM 127
 - Fibre Channel PCI adapter 101
 - memory module 127
 - PCI adapter 99
 - removal
 - 10-Gbps Ethernet PCI adapter 101
 - 16-drive-capable server 107

FRU (continued)

- removal (continued)
 - 240 VA safety cover 149
 - CD-RW/DVD drive 124
 - DIMM 126
 - DIMM air baffle 89
 - fan bracket 91
 - Fibre Channel PCI adapter 101
 - hot-swap fan 129
 - IBM virtual media key 93
 - memory module 126
 - microprocessor 137
 - microprocessor 2 air baffle 86
 - PCI adapter 98
 - PCI riser-card assembly 95
 - SAS riser-card and controller assembly 107
 - ServeRAID SAS controller 113
 - sserveRAID SAS controller
 - battery 120, 122
 - tape-enabled server 107
- removing
 - hot-swap power supply 131
- replace
 - hot-swap power supply 132
- replacement
 - microprocessor 2 air baffle 88
- replacing
 - 16-drive-capable server 109
 - CD-RW/DVD drive 125
 - DIMM air baffle 90
 - fan bracket 92
 - hot-swap fan 130
 - IBM virtual media key 94
 - PCI riser-card assembly 96
 - SAS riser-card and controller assembly 109
 - ServeRAID SAS controller 114
 - tape-enabled server 109
- storing
 - full-length-adapter bracket 106
- FRUs, file module
 - installation guidelines 50
- FRUs, removing
 - battery 81
 - heat-sink retention module 143
- FRUs, replacing
 - CD-RW/DVD drive 124, 125
 - DIMMs 126
 - heat-sink retention module 145
 - memory 126
 - microprocessor 138
 - operator information panel assembly 135, 136
 - system board 145, 147
- full-length-adapter bracket
 - storing 106

G

- Germany electronic emission compliance statement 273
- gpfs
 - troubleshooting the mount 157
 - identifying created and mounted file systems 157
 - missing file systems 158

gpfs (continued)
troubleshooting the mount (continued)
resolving stale NFS file systems 159

GPFS

analyzing logs 164
recovering 162

GPFS file system
error 164

grease, thermal 143

GUI access issues 19

GUI connectivity issues
troubleshooting procedure 184, 187

guidelines

file module reliability 51
hot-swap 51

H

handling static-sensitive devices 51

hard disk drive

installing 116
problems 52
removing 115

hardware components 1

hardware indicators 37

file node 29
LEDs 29

heat-sink

installing 138

heat-sink, applying thermal grease 138

hot-swap and hot-plug devices

power supplies 131, 132

hot-swap fan

removing 129
replacing 130

hot-swap guidelines 51

hot-swap power supply, installing 132

hot-swap power supply, removing 131

HSM 163

httpd service

error 257

I

IBM virtual media key

removal 93
replacing 94

identifying

canister 191
enclosure 191
status 192

IEC (International Electrotechnical Commission) electronic emission notice 274

information

center xix

initialization tool

interface 170
using 171

installation

problems
reported by CLI commands 18
troubleshooting
problems 9, 10, 19, 22, 24, 29

installation guidelines

file module FRUS 50

installing

10-Gbps Ethernet PCI adapter 102

240 VA safety cover 150

advanced feature key 118

battery 85

CD-RW/DVD drive 125

cover 80

DIMMs 127

Fibre Channel PCI adapter 101

hard disk drive 116

hot-swap drive 116

memory modules 127

microprocessor 138

PCI adapter 99

RAID controller 114

system board 147

International Electrotechnical Commission (IEC) electronic emission notice 274

inventory information 177

IP address

best practices 3

iSCSI

link problems 235

J

Japanese electronic emission notice 274

K

keyboard

accessibility 267

Korean electronic emission statement 274

L

LED hardware indicators 29

LEDs

file node hardware indicators 29

light path diagnostics 32

power supply 36

system status 193

legal notices

Notices 269

trademarks 271

light path diagnostics

LEDs 32

lights-on AOS connection

establishing 248

lights-out AOS connection

establishing 248

link failures

Fibre Channel 235

link problems

iSCSI 235

location information

record
best practices 6

log files

viewing 176

logical devices

physical port locations 152

lshealth

database replication failed 163

Mount state of the file system

changed to error level 163

M

maintenance

battery 179, 180

file module 48

maintenance agreement

best practices 7

management failover 153

management file module

removal 47

management GUI

accessing 43

cannot log on 185

supported browsers 188

troubleshooting procedure

start here 183

management GUI interface

when to use 43

management IP address

troubleshooting procedure 184

management node failover 154

management node role

failover procedures 152

management node roles

determining service IP 152

managing

event log 176

medium errors 181

memory

monitoring usage 72

memory module

removing 126

memory module, installing 127

microprocessor

applying thermal grease 138

heat sink 138

removal 137

replacing 138

mirrored volumes

not identical 189

multipath events

outputs 256

N

network interface

availability 161

New Zealand electronic emission

statement 272

NFS clients

stale NFS file handle 253

unable to mount NFS shares after
client IP change 253

node canister

location error 188

reseating 201

unknown service address 186

node errors

fixing 199

node rescue

performing 203

- notifications
 - best practices 4
 - sending 177
 - subscribe
 - best practices 6

O

- on a "good" Storwize V7000 Unified system 153
- operator information panel assembly, replacing 135, 136
- outputs
 - multipath event 256

P

- parts
 - removing
 - overview 204
 - preparing 204
 - replacing
 - overview 204
 - preparing 204
- Parts
 - removing and replacing 77
- passwords
 - best practices 3
- PCI adapter
 - removing 98
- People's Republic of China, electronic emission statement 274
- performing
 - node rescue 203
- physical port locations
 - logical devices 152
- POST (power-on self-test) 178
- power management
 - best practices 4
- power supply
 - installing 132
 - LED errors 36
 - operating requirements 131, 132
 - removing 131
 - replacing 210, 214
- power-on self-test 178
- powering off
 - system 202
- problem
 - mirrored volumes
 - not identical 189
- procedures
 - directed maintenance 44
- procedures for failure conditions 154
- publications
 - accessing 267

Q

- query status command 175

R

- RAID
 - best practices 5

- reader feedback, sending xxii
- recovering
 - offline virtual disks (volumes)
 - using CLI 241
- recovering the file system 162
- recovery
 - system
 - when to run 237
 - systems
 - starting 239
 - upgrade 261
- related information xix
- releasing
 - cable retention bracket 221
- reliability
 - file module guidelines 51
- remote support
 - configuring 247
- removal
 - file module 47, 48
- removing
 - 240 VA safety cover 149
 - 550 errors 239
 - 578 errors 239
 - advanced feature key 117
 - battery 81
 - CD-RW/DVD drive 124
 - cover 79
 - DIMM 126
 - fan 129
 - hard disk drive 115
 - heat-sink retention module 143
 - operator information panel assembly 135, 136
 - parts
 - overview 204
 - preparing 204
 - ServeRAID SAS controller 113
 - SFP transceiver 208
 - system 199
 - system board 145
 - system data 199
- removing and replacing
 - file module components 50
- removing and replacing parts 77
- replacing
 - 2.5" drive assembly 223
 - 3.5" drive assembly 221
 - battery 85, 218
 - blank carrier 221, 223
 - CD-RW/DVD drive 124, 125
 - control enclosure chassis 225
 - enclosure end cap 224
 - expansion canister 206
 - expansion enclosure 230
 - heat-sink retention module 145
 - microprocessor 138
 - node canister 204
 - operator information panel assembly 135, 136
 - parts
 - overview 204
 - preparing 204
 - power supply
 - control enclosure 210
 - expansion enclosure 214
 - SAS cable 224

- replacing (*continued*)
 - SFP transceiver 208
 - support rails 233
 - replacing parts 77
 - reporting
 - events 175
 - rescue
 - performing
 - for a node 203
 - reseating
 - node canister 201
 - reset service assistant password 173
 - reset service IP address 172
 - reset superuser password 172
 - resetting
 - superuser password 190
 - restore
 - system 236, 241
 - returning
 - device or component 52
 - riser card
 - removing 95
 - replacing 96
 - riser-card assembly
 - location 98, 101
- ## S
- safety notices xi
 - sound pressure xvii
 - safety statements xiii
 - SAN (storage area network)
 - problem determination 234
 - SAS cable
 - replacing 224
 - SAS cabling
 - location error 188
 - SAS riser-card and controller assembly
 - 16-drive-capable server 107, 109
 - removing 107
 - replacing 109
 - tape-enabled server 107, 109
 - satask.txt
 - commands 171
 - SCM
 - error recovery 256
 - sending
 - comments xxii
 - ServeRAID SAS controller
 - installing 114
 - removing 113
 - serveRAID SAS controller battery
 - install 122
 - removal 120
 - service action
 - file module 48
 - service address
 - unknown 186
 - service assistant
 - accessing 168, 203
 - interface 167
 - supported browsers 188
 - when to use 167
 - service CLI
 - accessing 170
 - when to use 170

- service commands
 - apply software 174
 - CLI 169
 - create cluster 174
 - reset service assistant password 173
 - reset service IP address 172
 - reset superuser password 172
 - snap 173
- service IP
 - determining for management nodes 152
- service IP address
 - changing 200
- setting up
 - call home support 247
- SFP transceiver
 - removing 208
 - replacing 208
- shortcut keys
 - accessibility 267
 - keyboard 267
- snap command 173
- sound pressure
 - safety notices xvii
- stale file systems
 - gpfs, troubleshooting resolving stale NFS file systems 159
- stale NFS file handle 253, 254
- starting
 - system recovery 239
- static-sensitive devices 51
- status
 - Ethernet 198
 - identifying 192
 - node canister 192
 - system 192
- storage area network (SAN)
 - problem determination 234
- storage system CLI
 - accessing 169
 - when to use 169
- storage system commands
 - CLI 169
- storage systems
 - restore 236
- Storwize V7000 37
 - hardware indicators 37
- Storwize V7000 Unified library
 - related publications xix
- superuser
 - password resetting 190
- supported browsers 188
- system
 - backing up configuration file using the CLI 243
 - deleting 199
- system data
 - removing 199
- system status
 - LEDs 193
- System x firmware
 - restoring 254

T

- T3 recovery
 - removing
 - 550 errors 239
 - 578 errors 239
 - when to run 237
- Taiwan
 - contact information 275
 - electronic emission notice 275
- thermal grease 143
- thermal material
 - heat sink 138
- time
 - synchronizing on file module 165
- Tivoli Storage Manager server
 - configuration 163
- trademarks 271
- troubleshooting
 - best practices 3
 - during installation 10
 - event notification email 177
 - getting started 9
 - gpfs 157
 - identifying created and mounted file systems 157
 - missing mounted file systems 158
 - resolving stale NFS file systems 159
 - GPFS 162
 - node errors 199
 - SAN failures 234
 - upgrade 261
- troubleshooting procedure
 - GUI connectivity issues
 - main GUI 184
 - service assistant 187
 - management IP address 184
- start here
 - management GUI 183

U

- understanding
 - error codes 178
 - event log 176
- upgrading
 - error codes 261
 - recovery 261
- USB key
 - detection error 190
 - using 170
 - when to use 170
- using
 - directed maintenance procedures 44
 - fix procedures 44
 - GUI interfaces 167
 - initialization tool 171
 - initialization tool interface 170
 - management GUI 42
 - service assistant 167
 - USB key 170

V

- VDisks (volumes)
 - recovering from offline using CLI 241
- viewing
 - event log 176
 - log files 179
 - node canister
 - status 192
 - system
 - status 192
 - trace files 179
- volumes (VDisks)
 - recovering from offline using CLI 241

W

- warranty agreement
 - best practices 7
- when to use
 - management GUI interface 43
 - service assistant 167
 - service CLI 170
 - storage system CLI 169
 - USB key 170
- working inside file module
 - with power on 51



Part Number: 00L4662

Printed in USA

GA32-1057-01



(1P) P/N: 00L4662

