IBM FlashSystem 840

Troubleshooting, Recovery, and Maintenance Guide

SC27-6297-00

Note

Before using this information and the product it supports, read the general information in "Notices" on page 67, the information in the "Safety and environmental notices" on page ix, as well as the information in the *IBM Environmental Notices and User Guide* , which is provided on a DVD.

This edition applies to IBM FlashSystem 840 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Safety and environmental notices

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

Here are examples of a caution and a danger notice:

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

DANGER

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

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

1. Look for the identification number at the end of each caution notice or each danger notice. In the preceding examples, the numbers (C001) and (D002) are the identification numbers.
2. Locate with the user publications that were provided with the hardware.
3. Find the matching identification number in the system.. Then review the topics concerning the safety notices to ensure that you are in compliance.

Safety notices and labels

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

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

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

IBM® Systems Safety Notices

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

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

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

Danger notice definition

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

Caution notice definition

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

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

Finding translated notices

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

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

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

   DANGER

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

   CAUTION:
   A caution notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury. (C001)
2. Open the IBM Systems Safety Notices.
3. Under the language, find the matching identification number. Review the topics about the safety notices to ensure that you are in compliance.

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

Caution notices

Ensure that you understand the caution notices.

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

CAUTION:

The weight of this part or unit is between 32 and 55 kg (70.5 and 121.2 lb). It takes three persons to safely lift this part or unit. (C010)

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

CAUTION:
Use safe practices when lifting.

(27)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

CAUTION:
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. (C045)

CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in splattered metal, burns, or both. (L005)

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

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

(R002)

CAUTION:

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

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

CAUTION:
Use safe practices when lifting. (R007)

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

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

Danger notices

Ensure that you are familiar with the danger notices for your storage system.

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

DANGER

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

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

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

  To disconnect:

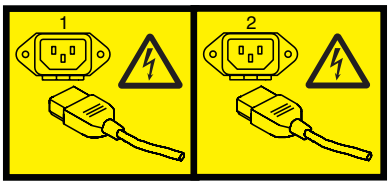
  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices.**

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)**

DANGER

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



DANGER

Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. (L003)

DANGER

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

DANGER

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

DANGER

Main Protective Earth (Ground):

This symbol is marked on the frame of the rack.

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

Special caution and safety notices

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

Handling static-sensitive devices

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

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

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

- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully, holding it by its edges or frame.
- Do not touch solder joints, pins, or exposed printed circuitry.
- Do not leave the device where others can handle and possibly damage the device.
- While the device is still in its antistatic bag, touch it to an unpainted metal part of the system unit for at least two seconds. (This action removes static electricity from the package and from your body.)
- Remove the device from its package and install it directly into your system, without putting it down. If it is necessary to put the device down, place it onto its static-protective bag. (If your device is an adapter, place it component-side up.) Do not place the device onto the cover of the system or onto a metal table.

- Take additional care when you handle devices during cold weather because heating reduces indoor humidity and increases static electricity.

Sound pressure

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

Environmental notices

The IBM Systems Environmental Notices and User Guide, Z125-5823 document contains all the required environmental notices for IBM Systems products in English and other languages.

It includes statements on limitations, product information, product recycling and disposal, battery information, flat panel display, refrigeration, and water-cooling systems, external power supplies, and safety data sheets.

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

About this guide

This guide describes how to service, maintain, and troubleshoot the IBM FlashSystem™ 840.

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

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

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

Who should use this guide

This guide is intended for system administrators who use and diagnose problems with the FlashSystem 840.

Related websites

The following websites provide information about FlashSystem 840 or related products or technologies:

Type of information	Website
Technical support for IBM storage products	www.ibm.com/storage/support/
IBM Electronic Support registration	www.ibm.com/support/electronicsupport

How to get information, help, and technical assistance

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

Information

IBM maintains pages on the web where you can get information about IBM products and fee services, product implementation and usage assistance, break and fix service support, and the latest technical information. For more information, refer to Table 1.

Table 1. IBM websites for help, services, and information

Website	Address
Directory of worldwide contacts	http://www.ibm.com/planetwide
Support for FlashSystem 840	www.ibm.com/support
Support for IBM System Storage® and IBM TotalStorage products	www.ibm.com/storage/support/

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

Help and service

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

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

If you call from somewhere other than the US or Canada, you must choose the **hardware** option when calling for assistance. When calling IBM for service regarding the product, follow these guidelines for the **hardware** :

Hardware option
Provide the serial number and appropriate 4-digit machine type.

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

Getting help online

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

To find up-to-date information about products, services, and partners, visit the IBM website at .

Before you call

Make sure that you have taken steps to try to solve the problem yourself before you call.

Some suggestions for resolving the problem before calling IBM Support include:

- Check all cables to make sure that they are connected.
- Check all power switches to make sure that the system and optional devices are turned on.
- Use the troubleshooting information in your system documentation. The troubleshooting section of the information center contains procedures to help you diagnose problems.
- Go to the IBM Support website at to check for technical information, hints, tips, and new device drivers or to submit a request for information.

Using the documentation

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

That documentation includes printed documents, online documents, readme files, and help files in addition to the information center. See the troubleshooting information for diagnostic instructions. The troubleshooting procedure might

require you to download updated device drivers or software. IBM maintains pages on the web where you can get the latest technical information and download device drivers and updates. To access these pages, go to and follow the instructions. Also, some documents are available through the IBM Publications Center.

Sign up for the Support Line Offering

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

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

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

Chapter 1. Hardware components

Components on the front of the enclosure

Learn about the components on the front of the enclosure.

The components on the front side of the enclosure include the two battery modules and the flash modules. Your enclosure may have up to 12 flash modules installed. (If fewer than 12 flash modules are installed, flash module blanks must be installed in the empty bays to maintain cooling airflow in the system enclosure.) Figure 1 shows the components on the enclosure front panel.

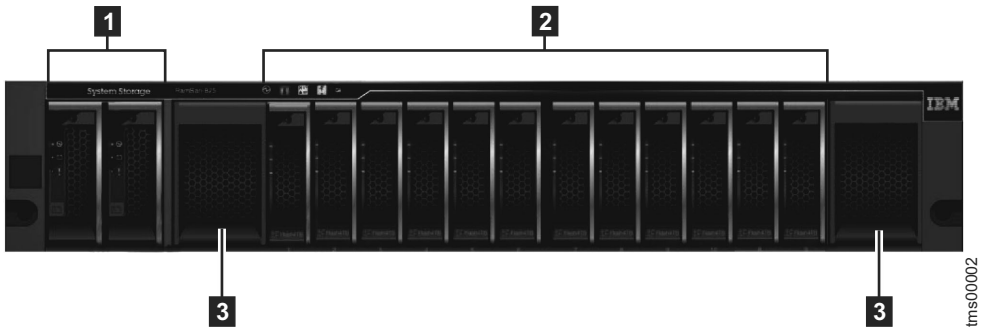


Figure 1. Components in the front of the enclosure

1. Battery modules
2. Flash modules
3. Chassis filler panels (nonremovable)

Front panel indicators

Learn about the location and function of the LEDs on the front panel of the enclosure.

Enclosure health LEDs

The front panel of the system has five LED indicators that display the overall health of the enclosure.

Figure 2 on page 2 shows the enclosure health LED indicators on the enclosure front panel.

Figure 2. Enclosure health LEDs

Table 2 describes the various LED states that you may observe.

Table 2. Enclosure health LED indicators

LED Name	Color	States
1 Power	green	• OFF – No power is supplied to the enclosure. • SOLID – The enclosure is powered on. • SLOW BLINK – The enclosure is in a powered down state and in standby mode.
2 Identify	blue	• OFF – The enclosure is not in an identify state. • SOLID – The enclosure was identified in response to the management system or chassis ecosystem.
3 Check Logs	amber	• OFF – There are no error log entries or general FRU failures. • SOLID – The system requires attention. Use the management interface to review the error logs and identify the problem.
4 Fault	amber	• OFF – No isolated FRU failures have occurred in the enclosure. • SOLID – One or more isolated FRU failures occurred in the enclosure. Service or parts replacement is required.
5 Battery module in Use	green	• OFF – The battery module is not in use. • BLINK – The system is committing the volatile cache memory to a persistent storage device.

Flash module LEDs

Each flash module has three LED indicators.

Figure 3 shows the LEDs on the flash module front panel.

Figure 3. Flash module LEDs

Table 3 on page 3 describes the various LED states that you may observe.

Table 3. Flash module LED descriptions

LED Name	Color	States
1 Power	green	• OFF – There is no power to the flash module. • SOLID – The flash module is powered on.
2 Flash module activity	green	• OFF – There is no read or write activity on the flash module. • FLASHING – The flash module is performing reads and writes.
3 Flash module fault	amber	• OFF – No known fault exists on the flash module. • SOLID – A fault exists on the flash module. • BLINK – The flash module is being identified. A fault might or might not exist.

Battery module LEDs

Each battery module has three LED indicators, visible on the enclosure front panel.

Figure 4 shows the LEDs on the battery module front panel.

Figure 4. Battery module LEDs

Table 4 describes the various LED states that you may observe.

Table 4. Battery module LED descriptions

LED Name	Color	States
1 Battery module power state	green	• OFF – No power is supplied to the battery module. • SOLID– The battery module power state is on.
2 Battery module status	green	• OFF – Indicates that the battery module is not in a state where it can support a save of volatile cache data. This is an error condition. For more information, refer to the battery module fault LED and the enclosure status that is provided by the management GUI. • SOLID – Indicates that the battery module is fully charged and can support a save of volatile cache data. This appearance is the normal state. • BLINK – Indicates that the battery module is charging and can support at least one save of cache data. • FAST BLINK – Indicates that the battery module is charging, but cannot yet support a save of cache data.
3 Battery module fault	amber	• OFF – No faults are detected within the battery module. • SOLID – A fault is detected within the battery module. The battery module must be replaced. • BLINK – The battery module has been identified.

Components in the rear of the enclosure

The rear of the enclosure includes two canisters and two power supply units. Each canister contains two interface cards and two fan modules.

Figure 5 shows the components on the rear of the enclosure.

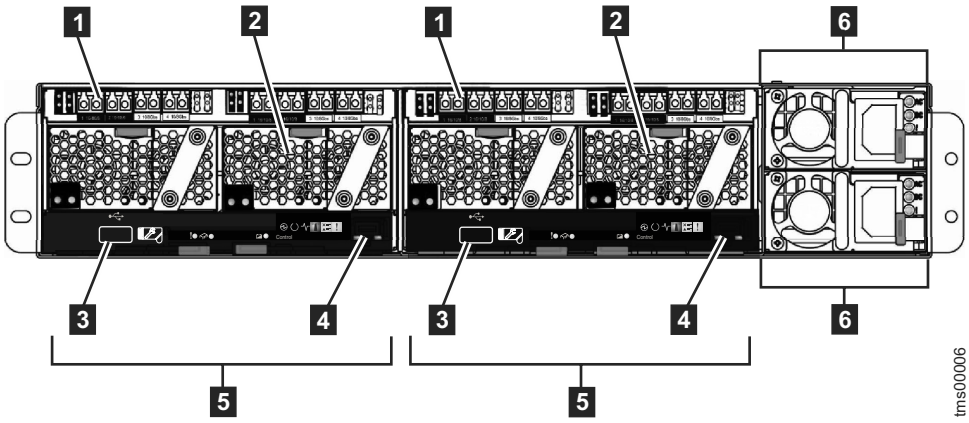


Figure 5. Components on the rear of the enclosure

1. Interface cards
2. Fan modules
3. USB connectors
4. Ethernet management ports
5. Canisters
6. Power supply units

Rear panel indicators and ports

Learn about the location and function of the LED indicators and ports on the rear panel of the enclosure.

USB ports

Each of the two canisters in the system includes a USB port.

Figure 6 shows the location of the two ports on the rear panel of the system.

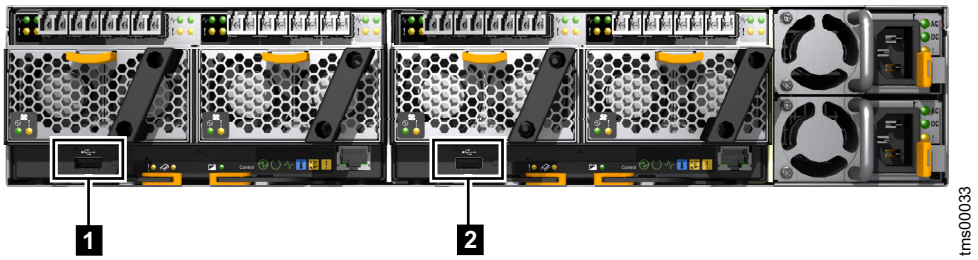


Figure 6. USB ports

1 , 2 USB ports

Canister state LEDs

Each of the two canisters has six LED indicators that display the overall state of the canister.

Figure 7 shows the state LEDs on each canister.

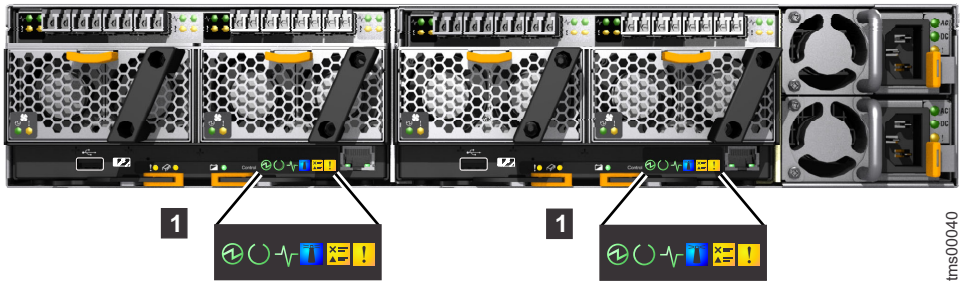


Figure 7. Canister state LEDs

1 Canister state LEDs

Table 5 describes the various LED states that you may observe.

Table 5. Canister state LED descriptions

LED Name	Icon	Color	States
Canister power		green	• OFF – There is no power supplied to the canister. • SOLID – The canister is powered on. • SLOW BLINK – The canister is in a powered down state (standby mode).
Canister status		green	• OFF – The canister is not operational. • SOLID – The canister is active. • BLINK – The canister is in candidate or service state. • FAST BLINK – The canister is in a firmware update cycle.
Canister activity		green	• OFF – The canister is in an idle state. • FLASHING – The canister is processing interface card input/output (I/O) traffic.
Identify		blue	• OFF – The canister is not in an identify state. • SOLID – The canister has been identified in response to the management system or enclosure ecosystem.
Check Logs		amber	• OFF – There are no error log entries or general FRU failures. • SOLID – The system requires attention. Use the management GUI to review the error logs and identify the problem.
Canister fault		amber	• OFF – No known fault exists on the canister. • SOLID – A fault exists on the canister.

Canister FRU LEDs

Each canister has two LED indicators that alert you to faults if they occur.

Figure 8 shows the field replaceable unit (FRU) LEDs on a canister.

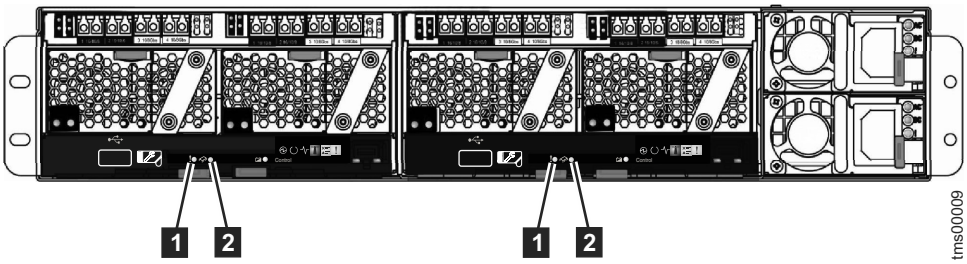


Figure 8. Canister FRU LEDs

Table 6 describes the various LED states that you may observe.

Table 6. Canister FRU LED descriptions

LED Name	Color	States
1 Canister FRU fault	amber	• OFF – There are no failures on the canister. • SOLID – The canister requires service or replacement • BLINK – The canister is being identified.
2 Internal FRU fault	amber	• OFF – There are no failures that are isolated to internal components of the canister. • SOLID – An internal component of the canister requires service or replacement. • BLINK – An internal component of the canister is being identified.

Fibre Channel interface card ports and indicators

Each canister on the rear of the enclosure supports two optional Fibre Channel interface cards.

Both 8 Gb and 16 Gb Fibre Channel (FC) cards are supported. Both types of cards have four physical ports. The number of enabled ports depends on the type of card installed:

- If the card is an 8 Gb card, all four ports are used. The ports on each card are numbered from 1 to 4, beginning with the left port.
- If the card is a 16 Gb card, only the left two ports on each card are used. The ports on each card are numbered from 1 to 2, beginning with the left port.

Each FC port is connected by using a short wave small form-factor pluggable (SFP) transceiver. The SFPs are connected to hosts or FC switches by using FC cables.

There are two LEDs for each FC port. Figure 9 on page 7 shows the location of the FC ports and the LEDs.

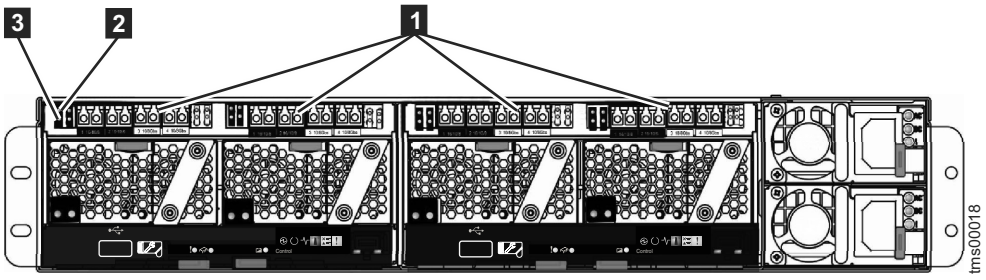


Figure 9. FC ports and LEDs

1 FC ports
2 Link state LED (one for each port)
3 Link speed LED (one for each port)

Table 7 describes the various LED states that you may observe.

Table 7. FC port LED descriptions

LED Name	Color	States
2 Link state	green	• OFF – No SFP transceiver installed. • SLOW BLINK – SFP transceiver installed, no link. • SOLID – Link connected.
3 Link speed	amber	• OFF – No link. • Two fast blinks – 4 Gb FC connection. • Three fast blinks – 8 Gb FC connection. • Four fast blinks – 16 Gb FC connection.

InfiniBand interface card ports and indicators

Each canister on the rear of the enclosure supports two optional InfiniBand interface cards.

The InfiniBand ports on each interface card are numbered from 1 to 2, starting from the left.

There are two LED indicators for each InfiniBand port, or a total of two pairs per interface card. Figure 10 shows the InfiniBand ports and the LEDs for each port.

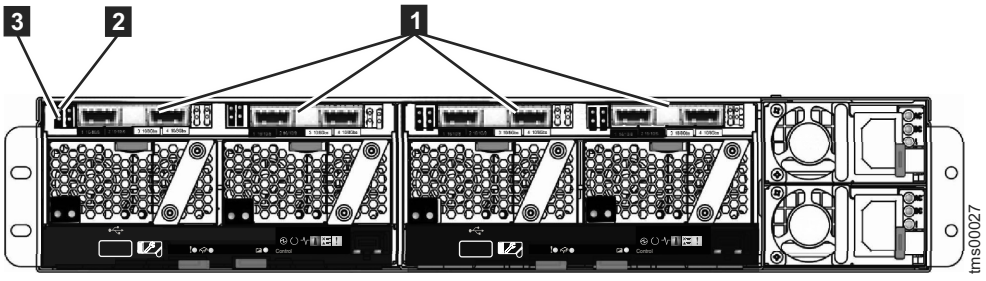


Figure 10. InfiniBand ports and LEDs

1 InfiniBand ports
2 Link state LED (one for each port)

3 Activity LED (one for each port)

Table 8 describes the various LED states that you may observe.

Table 8. InfiniBand port LED descriptions

LED Name	Color	States
2 Link state	green	• OFF – No link established. • SOLID – Link is established.
3 Activity	amber	• OFF – No Physical Link. • SOLID – Link is established. No activity. • FLASHING – Activity on the link.

FCoE interface card ports and indicators

Each canister on the rear of the enclosure supports two optional FCoE (Fibre Channel over Ethernet) interface cards.

The FCoE ports on each interface card are numbered from 1 to 4, starting from the left.

There are two LED indicators for each FCoE port, or a total of four pairs per interface card. Figure 11 shows the FCoE ports and LEDs for each port.

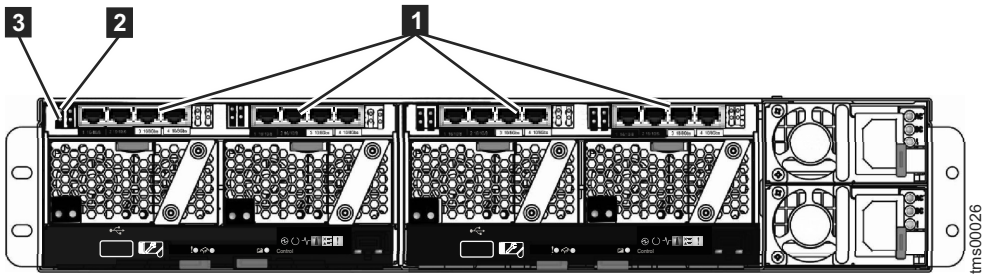


Figure 11. FCoE ports and LEDs

1 FCoE ports
2 Activity LED (one for each port)
3 Link state LED (one for each port)

Table 9 describes the various LED states that you may observe.

Table 9. FCoE port LED descriptions

LED Name	Color	States
2 Activity	green	• FLASHING – Activity on the link. • OFF – No activity.
3 Link state	amber	• OFF – No link established. • SOLID – Link is established.

Fan module LEDs

Each fan module has two LED indicators.

Figure 12 shows the LEDs on a fan module.

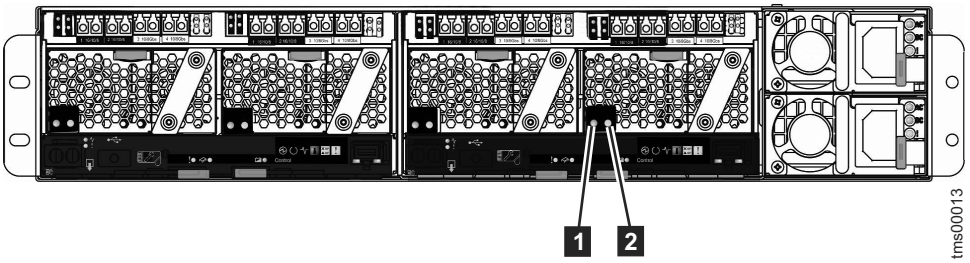


Figure 12. Fan module LEDs

Table 10 describes the various LED states that you may observe.

Table 10. Fan module LED descriptions

LED Name	Color	States
1 Fan module power	green	• OFF – There is no power to the fan module. • SOLID – The fan module is powered on.
2 Fan module fault	amber	• OFF – No known fault exists in the fan module. • BLINK – The fan module is being identified. • SOLID – A fault exists in the fan module.

Management port LEDs

The Ethernet management port on each canister has two LED indicators.

The two canisters in the enclosure each support an Ethernet management port. Figure 13 shows the LEDs for each management port.

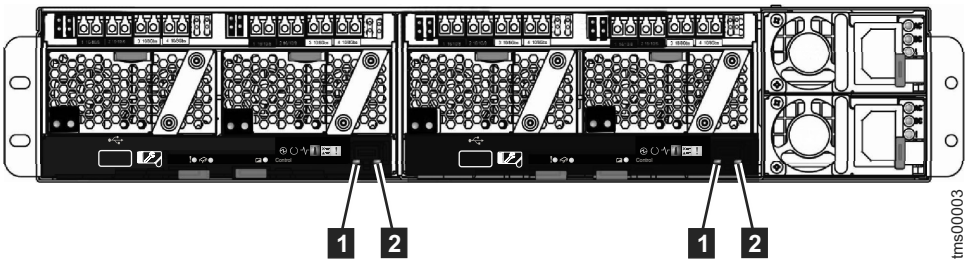


Figure 13. Management port LEDs

1 Port link LED
2 Port activity LED

Table 11 describes the various LED states that you may observe.

Table 11. Management port LED descriptions

LED Name	Color	States
1 Link	green	• OFF – Management port is not connected to a remote device. • SOLID – Management port is connected to a remote device.

Table 11. Management port LED descriptions (continued)

LED Name	Color	States
2 Activity	green	• OFF – No activity. • BLINK – Activity on the port.

Power supply unit LEDs

Each power supply unit has three LED indicators that display the status of the power supply unit and related power connections.

Figure 14 shows the LEDs on a power supply unit.

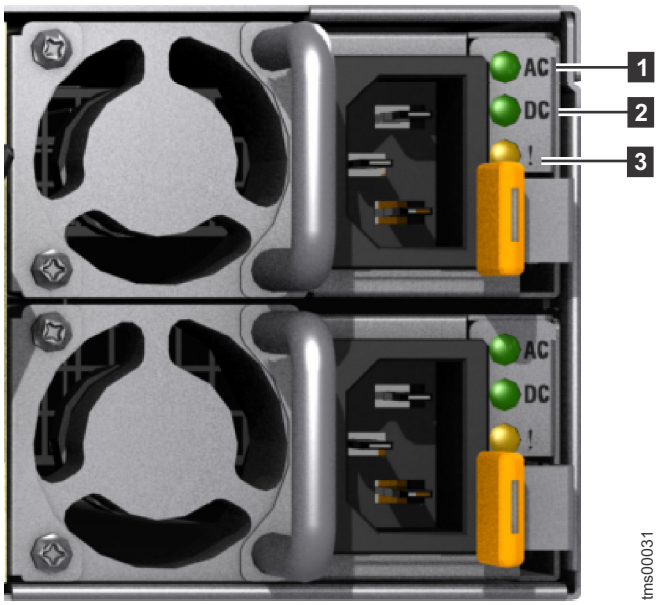


Figure 14. Power supply unit LEDs

Table 12 describes the various LED states that you may observe.

Table 12. Power supply unit LED descriptions

LED Name	Color	States
1 AC OK	green	• OFF – The power supply unit is not connected to a valid AC power source, or the power supply unit has failed. • SOLID – The power supply unit is connected to a valid AC power source.
2 DC OK	green	• OFF – The power supply unit is not connected to a valid AC power source, or the power supply unit is not providing DC power correctly to the enclosure. • SOLID – The power supply unit is supplying DC power to the enclosure.
3 Fault	amber	• OFF – No known fault exists in the power supply unit. • BLINKING – A fault exists in the power supply unit. • SOLID – The power supply unit is in a fault state.

Chapter 2. Best practices for troubleshooting

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

FlashSystem 840 technology and troubleshooting

Learn about the features of the FlashSystem 840 that may affect troubleshooting procedures.

Flash memory technology and troubleshooting

Array access issues may occur if the storage system is not stored properly when not in use.

Important: Although the flash modules retain data if the enclosure is disconnected from power, if the system is powered off for an extended period, the array may become inaccessible. It is recommended that the system remain powered on, or be powered on periodically, to retain array consistency.

Flash memory is also heat-sensitive. Use standard guidelines for sensitive electronic equipment when storing or transporting the storage system.

Battery module technology and troubleshooting

The battery module reconditions itself by being discharged and then recharged. Reconditioning occurs every three months, or when a battery module has been used for two or more power failures. Reconditioning takes approximately 12 hours.

Important: A battery module is unavailable when in reconditioning state. If the second battery module fails, or is in the process of reconditioning, the battery module attempting to recondition causes an error.

Parts redundancy and troubleshooting

Redundant parts in the FlashSystem 840 include the following:

- Flash modules
- Battery modules
- Canisters
- Power supply units
- Fan modules
- Interface cards

If a fan module, controller, or interface card requires replacement, temporarily remove the canister that contains the failed component to replace the failed part.

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

The following table displays the information to record:

Table 13. Access information for your system

Item	Value	Notes
The management IP address for the GUI and CLI		
The management user ID (the default is `superuser`)		
The management user ID password		
Cluster IP address		
Canister 1 IP address		
Canister 2 IP address		
Access information for attached switch 1		
Access information for attached switch 2		
Access information for attached switch 3		
Access information for attached switch 4		
Access information for attached host 1		
Access information for attached host 2		
Access information for attached host 3		
Access information for attached host 4		

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 **`stopsystem`** command to power off a system. Using either of these methods ensures that any volatile data is written to the flash

modules and the system is shut down in an orderly manner. After the system is shut down, use Wake on LAN (WOL) to power the system back up.

Note: You can also reboot your system in an orderly manner using the **stopsystem -rebootcommand**.

Set up event notifications

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

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

- Email. An event notification can be sent to one or more email addresses. This mechanism notifies individuals of problems. Individuals can receive notifications wherever they have email access which includes mobile devices.
- Simple Network Management Protocol (SNMP). An SNMP trap report can be sent to a data-center management system that consolidates SNMP reports from multiple systems. Using this mechanism, you can monitor your data center from a single workstation.
- Syslog. A syslog report can be sent to a data-center management system that consolidates syslog reports from multiple systems. Using this mechanism, you can monitor your data center from a single workstation.
- Call Home. If your system is within warranty, or you have a hardware maintenance agreement, configure your system to send email events to IBM if an issue that requires hardware replacement is detected. This mechanism is called Call Home. When the event is received, IBM automatically opens a problem report, and if appropriate, contacts you to verify if replacement parts are required. If you set up Call Home to IBM, ensure that the contact details that you configure are correct and kept up to date as personnel change.

Set up inventory reporting

Inventory reporting is an extension to the Call Home email.

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

Back up your data

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.

Resolve alerts in a timely manner

Your system reports an alert when there is an issue or a potential issue that requires user attention.

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

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

Keep your software up to date

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

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

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.

Subscribe to support notifications

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

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

www.ibm.com/support and search for IBM FlashSystem 840.

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.

Support personnel also ask for your customer number, machine location, contact details, and the details of the problem.

Chapter 3. User interfaces for servicing your 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.

- Use the management GUI to monitor and maintain the configuration of storage that is associated with your clustered systems.
- Complete service procedures from the service assistant.
- Use the command-line interface (CLI) to manage your system. The front panel on the node provides an alternative service interface.

Management GUI interface

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

About this task

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

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

Recommended action (default)
Shows only the alerts that require attention and have an associated fix procedure. Alerts are listed in priority order and should be fixed sequentially by using the available fix procedures. For each problem that is selected, you can:

- Run a fix procedure.
- View the properties.

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

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

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

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

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

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

- Recommended Actions. For each problem that is selected, you can:
  - Run a fix procedure.
  - View the properties.
- Event log. For each entry that is selected, you can:
  - Run a fix procedure.
  - Mark an event as fixed.
  - Filter the entries to show them by specific minutes, hours, or dates.
  - Reset the date filter.
  - View the properties.

When to use the management GUI

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

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

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

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

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

Accessing the management GUI to view events

To view events, you must access the management GUI.

About this task

You can use the management GUI to manage your system.

Procedure

1. Start a supported web browser and point the browser to the management IP address of your system.
2. When the connection is successful, you will see a login panel.
3. Log on by using your user name and password.
4. When you have logged on, select **Monitoring** > **Events**.
5. Ensure that the events log is filtered using **Recommended actions**.
6. Select the recommended action and run the fix procedure.
7. Continue to work through the alerts in the order suggested, if possible.

Results

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

Using fix procedures

You can use fix procedures to diagnose and resolve problems with the system.

About this task

For example, to repair the system, you might complete 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.

The example uses the management GUI to repair a system.

Procedure

Complete 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. One or more panels might be displayed with instructions for you to replace parts or complete other repair activity.
5. 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 17. After you have followed all the instructions, 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.`

Command-line interface

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

For a full description of the commands and how to start an SSH command-line session, see the "Command-line interface" section of the Information Center.

Service assistant interface

The service assistant interface is a browser-based GUI that is used to service your nodes.

When to use the service assistant

The primary use of the service assistant is when the enclosure is in a service state.

Attention: Complete service actions 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 enclosure 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 system 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 the system is in service state.

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

You can also complete the following service-related actions:

- Collect logs to create and download a package of files to send to support personnel.
- Remove the data for the system from a node.
- Recover a system if it fails.
- Install a temporary SSH key if a key is not installed and CLI access is required.

- Restart the services used by the system.

Accessing the service assistant

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

About this task

Procedure

To start the application, complete the following steps.

1. Start a supported web browser and point your web browser to *serviceaddress*/service for the node 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.
2. Log on to the service assistant using the superuser password.

   If you are accessing a new node canister, the default password is passw0rd. If the node canister is a member of a system or has been a member of a system, use the password for the superuser password.

   If you do not know the current superuser password, reset the password.

Results

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

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

Event reporting

Events that are detected are saved in an event log. As soon as an entry is made in this event log, the condition is analyzed. If any service activity is required, a notification is sent.

Event reporting process

The following methods are used to notify you and the IBM Support Center of a new event:

- If you enabled Simple Network Management Protocol (SNMP), an SNMP trap is sent to an SNMP manager that is configured by the customer.
- If enabled, log messages can be forwarded on an IP network by using the syslog protocol.
- If enabled, event notifications can be forwarded by email by using Simple Mail Transfer Protocol (SMTP).
- Call Home can be enabled so that critical faults generate a problem management record (PMR) that is then sent directly to the appropriate IBM Support Center by using email.

Understanding events

When a significant change in status is detected, an event is logged in the event log.

Error data

Events are classified as either alerts or messages:

- An alert is logged when the event requires some action. Some alerts have an associated error code that defines the service action that is required. The service actions are automated through the fix procedures. If the alert does not have an error code, the alert represents an unexpected change in state. This situation must be investigated to see if it is expected or represents a failure. Investigate an alert and resolve it as soon as it is reported.
- A message is logged when a change that is expected is reported, for instance, an an array build completes.

Viewing the event log

You can view the event log by using the management GUI or the command-line interface (CLI).

About this task

You can view the event log by using the **Monitoring** > **Events** options in the management GUI. The event log contains many entries. You can, however, select only the type of information that you need.

You can also view the event log by using the command-line interface (**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 14 describes some of the fields that are available to assist you in diagnosing problems.

Table 14. 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.

Table 14. Description of data fields for the event log (continued)

Data field	Description
Event count	The number of events coalesced into this event log record.
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

The system 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 active service actions. If a recommended service action is active, these events are notified only if they are still unfixed when the service action completes.

Each event that the system detects is assigned a notification type of Error, Warning, or Information. When you configure notifications, you specify where the notifications should be sent and which notification types are sent to that recipient.

Events with notification type Error or Warning are shown as alerts in the event log. Events with notification type Information are shown as messages.

SNMP traps

Simple Network Management Protocol (SNMP) is a standard protocol for managing networks and exchanging messages. The system can send SNMP messages that notify personnel about an event. You can use an SNMP manager to view the SNMP messages that the system sends. You can use the management GUI or the command-line interface to configure and modify your SNMP settings. You can specify up to a maximum of six SNMP servers.

You can use the Management Information Base (MIB) file for SNMP to configure a network management program to receive SNMP messages that are sent by the

system. This file can be used with SNMP messages from all versions of the software. More information about the MIB file for SNMP is available at this website:

www.ibm.com/support

Search for IBM FlashSystem 840, then search for **MIB**. Go to the downloads results to find **Management Information Base (MIB) file for SNMP**. Click this link to find download options.

Call Home email

The Call Home feature transmits operational and event-related data to you and service personnel through a Simple Mail Transfer Protocol (SMTP) server connection in the form of an event notification email. When configured, this function alerts service personnel about hardware failures and potentially serious configuration or environmental issues.

To send email, you must configure at least one SMTP server. You can specify as many as five additional SMTP servers for backup purposes. The SMTP server must accept the relaying of email from the management IP address. You can then use the management GUI or the command-line interface to configure the email settings, including contact information and email recipients. Set the reply address to a valid email address. Send a test email to check that all connections and infrastructure are set up correctly. You can disable the Call Home function at any time using the management GUI or the command-line interface.

To send automated notifications, use one of the following email addresses:

- `flash-sc1@vnet.ibm.com`
- `flash-sc2@vnet.ibm.com`

Power-on self-test

When you turn on the system, the node canisters perform self-tests.

A series of tests is performed to check the operation of components and some of the options that have been installed when the system is first turned on. This series of tests is called the power-on self-test (POST).

When the code is loaded, additional testing takes place, which ensures that all of the required hardware and code components are installed and functioning correctly.

Understanding event codes

The system generates informational events when significant changes to the state of the system are detected.

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.

Understanding the error codes

Error codes are generated by the event-log analysis and system configuration code.

Error codes help you to identify the cause of a problem, a failing component, and the service actions that might be needed to solve the problem.

Viewing logs

The system maintains log files that can be used to manage your system and diagnose problems.

You can view information about collecting 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 Information Center and then expand the **Logs and traces** section.

Chapter 4. Resolving a problem

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

The following procedures are often used to find and resolve problems:

- Procedures that involve data collection and system configuration
- Procedures that are used for hardware replacement.

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

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

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 to run fix procedures

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

You can connect to and manage a system as soon as you have created a clustered system. If you cannot create a clustered system, see Problem: Cannot create a clustered system.

To run the management GUI, start a supported web browser and point it to the management IP address of your system.

After the connection is successful, you see a login panel. If you are unable to access the login panel, see “Problem: Unable to connect to the management GUI” on page 26.

Log on using your user name and password. If you are unable to log on, go to “Problem: Unable to log on to the management GUI” on page 27.

After you have logged on, select **Monitoring** > **Events** to view the system event log, then select the **Recommended Actions** filter.

An event in the log can be an informational message, or it can alert you to an error that requires fixing. Errors are prioritized by their error code, and each has a fix procedure that can be run.

A fix procedure is a wizard that helps you troubleshoot and correct the cause of an error. Some fix procedures will reconfigure the system, based on your responses;

ensure that actions are carried out in the correct sequence; and, prevent or mitigate loss of data. For this reason, you must always run the fix procedure to fix an error, even if the fix might seem obvious.

To run the fix procedure for the error with the highest priority, go to the Recommended Action panel at the top of the Event page and click `Run This Fix Procedure`. When you fix higher priority events first, the system can often automatically mark lower priority events as fixed.

While the **Recommended Actions** filter is active, the event list shows only alerts for errors that have not been fixed, sorted in reducing order of priority. The first event in this list is the same as the event displayed in the Recommended Action panel at the top of the Event page of the management GUI.

If you find it necessary to fix errors in a different order, this can be done by selecting an error alert in the event log and then clicking **Action** > **Run Fix Procedure**.

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

Problem: Management IP address unknown

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

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

If you do not know the management IP address, it is part of the data that is shown in the service assistant home panel. “Procedure: Getting node canister and system information using the service assistant” on page 31

Problem: Using the USB flash drive encryption key

This information assists you if you encounter difficulties using the USB encryption key.

- If the USB flash drive encryption key is not found by the system, check the physical USB flash drive and update a new key file on the USB flash drive.
- If the USB flash drive and the key file seem to be valid, the USB port on the canister may be faulty. You can failover the control node to the other canister, and the USB flash drive can then be used.
- If there is only USB flash drive encryption key, it will need to be used in the active canister. The drive can then be moved to the other canister, or a failover can be performed.

Problem: Unable to connect to the management GUI

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

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

- 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.

Problem: Unable to log on to the management GUI

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

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

- If you are not logging on as `superuser`, contact your system administrator to verify your user name and reset your account password.
- If the user name that you are using is authenticated through a remote authentication server, verify that the server is available. If the authentication server is unavailable, you can log on as user name `superuser`. This user is always authenticated locally.
- If you do not know the password for `superuser`, follow the steps at "Procedure: Resetting superuser password" on page 30 to reset the superuser password.

Problem: Management GUI or service assistant does not display correctly

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

For a list of supported browsers, see "Planning for software Web browser requirements to access the management GUI" in the Planning section.

Problem: Cannot connect to the service assistant

If you are unable to display the service assistance on your browser, refer to these tips.

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. Follow the procedure to find the IPv4 and IPv6 addresses that are configured on the node. 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, follow the procedure for changing a service IP address on a node canister.

- You cannot connect to the service assistant if the node canister is not able to start the code. Verify that the LEDs indicate that the code is active by viewing the system status LEDs.
- 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 follow the procedure 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 The service IP address 192.168.70.122 subnet mask 255.255.255.0 is preconfigured on Ethernet port 1

  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, follow the procedure to change the service IP address to one that works in your environment.

  If you are unable to change the service address, for example, because you cannot use a USB flash drive, see the topic that contains information about how to access a canister using an Ethernet cable.

Problem: Node canister service IP address unknown

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

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

If you are unable to access the management GUI but you know the management IP address of the system, you can use the address to log into the service assistant that is running on the configuration node.

1. Point your browser at the `/service` directory of the management IP address of the system. If your management IP address is `11.22.33.44`, point your web browser to `11.22.33.44/service`.
2. Log into the service assistant.
3. The service assistant home page lists the node canister that can communicate with the node.
4. If the service address of the node canister that you are looking for is listed in the Change Node window, make the node the current node. Its service address is listed under the Access tab of the node details.

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

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

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

Procedure: Fixing node errors

To fix node errors that are detected by node canisters in your system, use this procedure.

About this task

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

Procedure

1. Carry out "Procedure: Getting node canister and system information using the service assistant" on page 31 to understand the state of each node.
2. View information about the node canisters to understand the state of each node. See *Procedure: Getting node canister and system information using the service assistant*.
3. If possible, log into the management GUI and use the monitoring page to run the recommended fix procedure.
   a. Follow the fix procedure instructions to completion.
   b. Repeat this step for each subsequent recommended fix procedure.
4. If it is not possible to access the management GUI, or no recommended actions are listed, refer to the Error event IDs and error codes refer to the *Error event IDs and error codes* and follow the identified user response for each reported node error.

Problem: Command file not processed from USB flash drive

.Determine the reasons a command file is not being processed when you use a USB flash drive.

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

If you encounter this situation, verify the following items:

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

- If there is a `satask_result.html` file, check the first entry in the file. If there is no entry that matches the time the USB flash drive was used, it is possible that the USB port is not working or the node is not operational. Check the node status using the LEDs.
- If there is a status output for the time the USB flash drive was used, then the `satask.txt` file was not found. Check that the file was named correctly. The `satask.txt` file is automatically deleted after it has been processed.

Procedure: Resetting superuser password

You can reset the superuser password to the default password of `passw0rd` by using a USB flash drive command action.

About this task

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

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

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

To use a USB flash drive, see the topic that contains information about using a USB flash drive.

Results

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

Procedure: Changing the service IP address of a node canister

Identify the method that you will use to change the service IP address of a node canister.

About this task

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

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

You can set an IPv4 address, an IPv6 address, or both, as the service address of a node. Enter the required address correctly. If you set the address to 0.0.0.0 or

0000:0000:0000:0000:0000:0000:0000, you disable the access to the port on that protocol.

Procedure

Change the service IP address.

- Use the control enclosure management GUI when the system is operating and the system is able to connect to the node with the service IP address that you want to change.
  1. Select **Settings** > **Network** from the navigation.
  2. Select **Service IP Addresses**.
  3. Complete the panel. Be sure to select the correct node to configure.
- Use the service assistant when you can connect to the service assistant on either the node canister that you want to configure or on a node canister that can connect to the node canister that you want to configure:
  1. Make the node canister that you want to configure the current node.
  2. Select **Change Service IP** from the menu.
  3. Complete the panel.

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

Use the service assistant to view information about node canisters and your system.

About this task

To obtain the information:

1. Log on to the service assistant, as described in "Accessing the service assistant" on page 19.
2. View the information about the node canister to which you connected or the other node canister in the enclosure. To change which node's information is shown, select the node in the **Change Node** table of the Home page.

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

The node details are divided into several sections. Each section has a tab. Examine the data that is reported in each tab for the information that you want.

- The Node tab shows general information about the node canister that includes the node state and whether it is a configuration node.
- The Hardware tab shows information about the hardware.
- The Access tab shows the management IP addresses and the service addresses for this node.
- The Location tab identifies the enclosure in which the node canister is located.
- The Ports tab shows information about the I/O ports.

Procedure: Initializing a clustered system using the service assistant

Use this procedure to initialize a clustered system using the service assistant rather than the USB flash drive.

About this task

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

Procedure

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

1. Point your web browser to the service assistant address of a node canister. It is best to use node canister in slot 1; when viewed from the rear of the control enclosure, the left node canister. The default service address for this canister is *192.168.70.121/service*.
2. Log on with the superuser password. The default password is `passw0rd`.
3. Select **Manage System**.
4. Enter the system name and the management IP address.
5. Click **Create System**.
6. Point a supported browser to the management IP address that you specified to start the management GUI. The management GUI logon panel is displayed.
7. Log on as superuser. Use `passw0rd` for the password.
8. Follow the on-screen instructions.

Results

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

Procedure: Accessing a canister using a directly attached Ethernet cable

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

About this task

Follow this procedure if you are not authorized to use a USB flash drive in your data center and when the service address of your nodes cannot be accessed over your Ethernet network. This situation might occur for a new installation where the default service IP addresses cannot be accessed on your network.

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

Procedure

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

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

   Note: A cross-over Ethernet cable is not required.
2. Connect the other end of the Ethernet cable directly to the Ethernet port on a personal computer that has a web browser installed.
3. Get the service IP address of the node canister attached at step 1. If the service IP address is unknown, refer to "Problem: Node canister service IP address unknown" on page 28.
4. Use the operating system tools on the computer to set the IP address and subnet mask of the Ethernet port that is used in step 2. Set them to the same subnet of the node canister service IP address.
5. Point the web browser to the service IP address for the node canister.
6. Log on with the superuser password. The default password is `passw0rd`.
7. Set the service address of the canister to one that can be accessed on the network as soon as possible.
8. Wait for the action to complete.
9. Disconnect your personal computer.
10. Reconnect the node canister to the Ethernet network.

Understanding the system status using the LEDs

To determine the system status using the LED indicators on the enclosure, use this procedure.

About this task

A detailed view of the system state is provided in the Monitoring sections of the management GUI. If the management GUI is accessible, use this procedure to determine the system status using the LED indicators on the enclosure.

The system status LED visible on the front of the enclosure can show one of several states, as described in Table 15.

Table 15. LED state descriptions

State description	Detail
Off	The LED is continuously not lit.
Blinking slowly	The LED turns on and off at a frequency of 1 Hz: It is on for 500 ms (1/2 second), then off for 500 ms, then repeats.
Blinking	The LED turns on and off at a frequency of 2 Hz: It is on for 250 ms, then off for 250 ms, then repeats.
Blinking fast	The LED turns on and off at a frequency of 4 Hz: It is on for 125 ms, then off for 125 ms, then repeats.
On	The LED is continuously lit.
Flashing	The LED is lit to indicate some activity, then turns off. The rate and duration that the LED is lit depends on the rate and duration of the activity.

Procedure

Complete the following steps to understand when an enclosure is not responsive, and what remedial action to take.

1. Identify the enclosure that you are troubleshooting.
2. Check the status of each power supply unit (PSU) in the enclosure.
3. If at least one PSU is providing power to the enclosure, check the status of each controller in the enclosure.

Procedure: Finding the status of the Ethernet connections

Learn how to find the status of the Ethernet management port connections when you cannot connect.

About this task

Each Ethernet management port 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:

- Examine the LEDs of the Ethernet management ports. For these ports, the link state LED is ON if the link is connected.

Procedure

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

1. Verify that each end of the cable is securely connected.
2. Verify that the port on the Ethernet switch or hub is configured correctly.
3. Connect the cable to a different port on your Ethernet network.
4. Replace the Ethernet cable.

Procedure: Collecting information for support

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

About this task

The management GUI has features to assist you in collecting the required information. 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.

Procedure

1. Using the management GUI, select **Settings** > **Support**.
2. Click **Download Support Package**, and then follow the instructions to download the appropriate log files.

SAN problem determination

Learn how to solve problems with your system connection to the storage area network (SAN).

About this task

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

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

- Installed small form-factor pluggable (SFP) transceiver
- Fiber-optic cables

Complete the following steps if you were sent here from either the maintenance analysis procedures or the error codes:

Procedure

1. If the customer has changed the SAN configuration by changing the Fibre Channel cable connections or switch zoning, ask the customer to verify that the changes were correct and, if necessary, reverse those changes.
2. Verify that the power is turned on to all switches that the system uses, and that they are not reporting any hardware failures. If problems are found, resolve those problems before proceeding further.
3. Verify that the Fibre Channel cables that connect the systems to the switches are securely connected.

Fibre Channel link failures

To help you solve problems on the system and its connection to the storage area network (SAN) when an optional Fibre Channel host interface card is being used, follow this procedure.

Before you begin

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

- The Fibre Channel port LEDs at the rear of the enclosure. The upper, green physical link state LED and lower, amber link status LED for the port will both be off if the link has failed.
- An error that indicates a single port has failed

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

1. Use the **chportfc** command to set the port on the FC interface card to the correct speed and topology.
2. Ensure that the Fibre Channel cable is securely connected at each end.
3. Replace the Fibre Channel cable.
4. Replace the SFP transceiver for the failing port on the enclosure
5. Perform the Fibre Channel switch service procedures for a failing Fibre Channel link. This might involve replacing the SFP transceiver at the switch.
6. Contact IBM Support for assistance in replacing the canister in the enclosure.

InfiniBand link failures

To help you solve problems on the system and its connection to the storage area network (SAN) when an optional InfiniBand interface card is being used, follow this procedure.

Before you begin

The following items can indicate that an InfiniBand link has failed:

- The SAN monitoring tools of the customer.
- The InfiniBand status LEDs at the rear of the enclosure. The upper, green physical link LED for the port will be off if the link has failed.
- An error that indicates a single port has failed.
- If there is a solid green light but no amber, there is no active Subnet Manager for the port. Check your configuration or restart the missing manager.

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

1. Ensure that the InfiniBand cable is securely connected at each end.
2. Replace the InfiniBand cable.
3. Perform the InfiniBand switch service procedures for a failing link.
4. Contact IBM Support for assistance in replacing the canister in the enclosure.

Chapter 5. Backing up and restoring the system configuration

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

Configuration data for the system provides information about your system and the objects that are defined in it. You must regularly back up your application data by using the appropriate backup methods.

You can maintain your configuration data for the system by completing the following tasks:

- Backing up the configuration data
- Restoring the configuration data
- Deleting unwanted backup configuration data files

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

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

Note:

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

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

- You have the Security Administrator role associated with your user name and password.
- You have a copy of your backup configuration files on a server that is accessible to the system.
- You have a backup copy of your application data that is ready to load on your system after the restore configuration operation is complete.
- You know the current license settings for your system.
- You did not remove any hardware since the last backup of your configuration.

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

Backing up the system configuration using the CLI

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

Before you begin

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

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

About this task

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

You must regularly back up your configuration data and your application data to avoid data loss. Do this after any significant changes in configuration have been made to the system.

Note: The system automatically creates a backup of the configuration data each day at 1 AM. This is known as a **cron** backup and is written to `/dumps/svc.config.cron.xml_serial#` on the configuration node.

A manual backup can be generated at any time using the instructions in this task. If a severe failure occurs, both the configuration of the system and application data might be lost. The backup of the configuration data can be used to restore the system configuration to the exact state it was in before the failure. In some cases, it might be possible to automatically recover the application data. This can be attempted with the Recover System Procedure, also known as a Tier 3 (T3) procedure. To restore the system configuration without attempting to recover the application data, use the Restoring the System Configuration procedure, also known as a Tier 4 (T4) recovery. Both of these procedures require a recent backup of the configuration data.

Complete the following steps to back up your configuration data:

Procedure

1. Back up all of the application data that you stored on your volumes using your preferred backup method.
2. Issue the following CLI command to back up your configuration:

   ```
   svcconfig backup
   ```

   The following output is an example of the messages that might be displayed during the backup process:

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

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

Table 16. Files created by the backup process

File name	Description
`svc.config.backup.xml_<serial#>`	Contains your configuration data.

Table 16. Files created by the backup process (continued)

File name	Description
svc.config.backup.sh_<serial#>	Contains the names of the commands that were issued to create the backup of the system.
svc.config.backup.log_<serial#>	Contains details about the backup, including any reported errors or warnings.

3. Check that the **svcconfig backup** command completes successfully, and examine the command output for any warnings or errors. The following output is an example of the message that is displayed when the backup process is successful:

```
CMMVC6155I SVCCONFIG processing completed successfully.
```

   If the process fails, resolve the errors, and run the command again.
4. Keep backup copies of the files above outside the system to protect them against a system hardware failure. Copy the backup files off the system to a secure location using either the management GUI or scp command line. For example:

```
pscp  -unsafe superuser@cluster_ip:/dumps/svc.config.backup.*
 /offclusterstorage/
```

   The cluster_ip is the IP address or DNS name of the system and **offclusterstorage** is the location where you want to store the backup files.

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

Restoring the system configuration

Before you begin

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

About this task

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

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

To restore your configuration data, follow these steps:

Procedure

1. Verify that all nodes are available as candidate nodes before you run this recovery procedure. You must remove errors 550 or 578 to put the node in candidate state.
2. Identify the configuration backup file from which you want to restore.

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

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

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

   a. From the management GUI, click **Settings** > **Support**.
   b. Click **Show full log listing**.
   c. For each node (canister) in the system, complete the following steps:
      1) Select the node to operate on from the selection box at the top of the table.
      2) Find all the files with names matching the pattern `svc.config.*.xml*`.
      3) Double-click the files to download them to your computer.

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

   ```
   pscp full_path_to_identified_svc.config.file
   superuser@cluster_ip:/tmp/svc.config.backup.xml
   ```
4. Issue the following CLI command to compare the current configuration with the backup configuration data file:

   ```
   svcconfig restore -prepare
   ```

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

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

   ```
   pscp superuser@cluster_ip:/tmp/svc.config.restore.prepare.log
   full_path_for_where_to_copy_log_files
   ```
6. Open the log file from the server where the copy is now stored.
7. Check the log file for errors.
   - If you find errors, correct the condition that caused the errors and reissue the command. You must correct all errors before you can proceed to step 8.
   - If you need assistance, contact the IBM Support Center.
8. Issue the following CLI command to restore the configuration:

   ```
   svcconfig restore -execute
   ```

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

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

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

10. Open the log file from the server where the copy is now stored.
11. Check the log file to ensure that no errors or warnings have occurred.

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

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

What to do next

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

```
svcconfig clear -all
```

Deleting backup configuration files using the CLI

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

About this task

Perform the following steps to delete backup configuration files:

Procedure

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

   ```
   svcconfig clear -all
   ```

Chapter 6. Replacing parts

You can remove and replace customer-replaceable units (CRUs) in the enclosure.

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

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

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

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

Preparing to remove and replace parts

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

Before you begin

First, read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the FlashSystem 840.

Replacing a flash module

Learn how to safely replace a flash module. You must follow the fix procedures to avoid data loss. It is also possible to lose access to data if an incorrect part is removed.

Before you begin

Attention: When replacing this part, you must follow recommended procedures for handling electrostatic discharge (ESD)-sensitive devices.

About this task

Attention: Before you replace a flash module, 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 loss of access to data.

Attention: The replacement flash module must match the capacity of all other flash modules in the system. Do not mix flash modules with different capacities.

Attention: To avoid adversely affecting cooling airflow, do not leave a flash module slot empty. Do not remove a flash module before you have a replacement available.

To replace a flash module, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Follow the fix procedure in the management GUI. The fix procedure will identify the faulty flash module by causing the amber fault LED to blink.
3. Unlock the failed module by pressing the latch at the top of the handle, shown in Figure 15.

Figure 15. Flash module

1 Release latch on handle

4. Open the handle fully, and then slide the flash module out of the enclosure.
5. Slide the new flash module into the slot until the handle starts to move.
6. Finish inserting the module by closing the handle until the latch clicks into place.

Replacing a power supply unit

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

Before you begin

DANGER

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

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

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

  To disconnect:

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

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)**

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

Attention: The enclosure will continue to operate if the second power supply unit is fully functional while the faulty power supply unit is replaced. (The DC power LED will be on, and the fault LED will be off.) If there is a fault displayed on the working power supply unit, removing the other power supply unit will shut down the enclosure.

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: When replacing this part, you must follow recommended procedures for handling electrostatic discharge (ESD)-sensitive devices.

About this task

To replace a power supply unit, complete the following steps:

Procedure

1. Read the safety information to which “Preparing to remove and replace parts” on page 43 refers.
2. Examine the power supply unit LEDs to identify the power supply unit that failed.
3. Disconnect the cable retention bracket and the power cord from the power supply unit that you are replacing.
4. To remove a power supply unit, press the release latch shown in Figure 16 on page 48 towards the handle, and then grip the handle and slide the power supply unit out of the enclosure.

Figure 16. Power supply unit

1 Release latch

5. Insert the replacement power supply unit into the enclosure, in the same orientation as the other power supply unit.
6. Finish inserting the power supply unit into the enclosure until the latch clicks into place.
7. Reattach the power cable and cable retention bracket.

What to do next

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

Replacing a battery module

Contact IBM support for assistance in replacing a failed battery module.

Replacing an SFP transceiver

When a failure occurs on an optical link, the SFP transceiver in the port providing the link might need to be replaced. To replace a faulty SFP transceiver, use this procedure.

Before you begin

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

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

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

Attention: When replacing this part, you must follow recommended procedures for handling electrostatic discharge (ESD)-sensitive devices.

About this task

Complete the following steps to remove and then replace an SFP transceiver:

Procedure

1. Carefully determine the failing physical port connection.

   Important: Removing the wrong SFP transceiver might result in loss of data access.
2. Figure 17 illustrates an SFP transceiver.

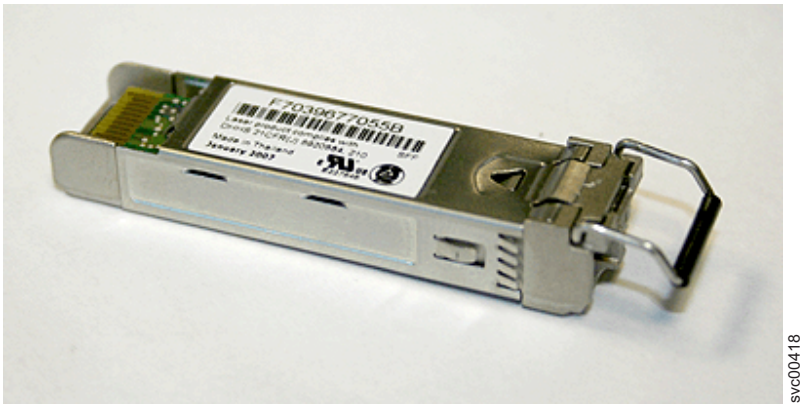


Figure 17. SFP transceiver

3. Remove the cable from the SFP.
4. Remove the faulty SFP transceiver from its aperture.
   a. Examine the SFP transceiver to see how it is secured to the port. The SFP transceiver may have a handle that clips onto the port, a tab that you pull to release the SFP transceiver, or a sliding tab that unlocks the SFP transceiver.
   b. Use the handle or tab to release the SFP transceiver from the port.
   c. Slide the SFP transceiver out of its slot.
5. Verify that the optical cable end is clean. If necessary, use an appropriate cleaning kit to clean the cable end.

6. Verify that the replacement transceiver matches the type of transceiver removed in the previous step.
7. Install the replacement SFP transceiver into the aperture vacated in step 4.
   a. Open the lock on the replacement SFP transceiver.
   b. Push the new SFP transceiver into the aperture until it stops.
   c. If the SFP transceiver uses a release handle, close the handle to secure the SFP.
   d. Gently pull the SFP transceiver. If it is installed correctly, it does not move from its aperture.
8. Reconnect the optical cable.
9. Confirm that the error is now fixed. Either mark the error as fixed or restart the node depending on the failure indication originally noted.

Replacing a fan module

You can independently replace either of the two hot-swap fan modules in each canister. Each fan module contains four fans. If one of the fans fails, you must replace the entire fan module, as the individual fans are not field-replaceable.

Before you begin

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: When replacing this part, you must follow recommended procedures for handling electrostatic discharge (ESD)-sensitive devices.

About this task

To replace a fan module, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Examine the fan module LEDs on the enclosure rear panel. The amber fan fault LED on the lower left corner of the failed fan module will be on.
3. To remove a fan module, press the release latch shown in Figure 18 on page 51, and then grip the handle and slide the fan module out of the canister.

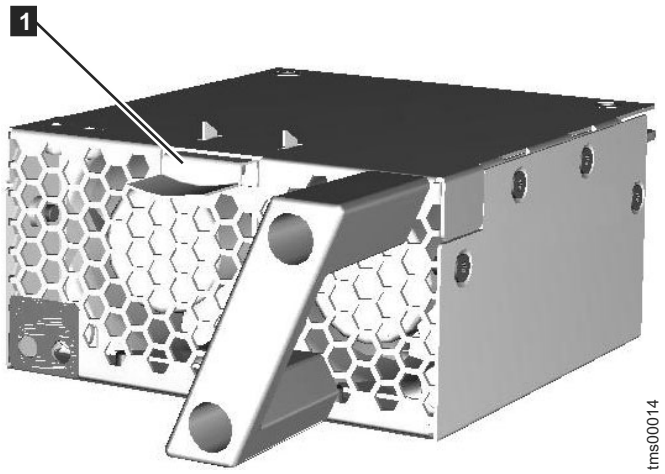


Figure 18. Fan module

1 Release latch

4. Insert the replacement fan module into the canister, in the same orientation as the one that you removed.
5. Finish inserting the fan module into the canister until the latch clicks into place. The green fan power LED turns on once the fan module is powered on.

What to do next

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

Service-only parts replacement procedures

Certain components in the enclosure should only be replaced by trained service providers.

Even though many of these components are hot-swappable, they are intended to be used only when your system is not active (no I/O operations). If your system is powered on and processing I/O operations, go to the management GUI and follow the fix procedures. Initiating the replacement actions without the assistance of the fix procedures can result in loss of data or loss of access to data.

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

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

After carrying out a part replacement under warranty, ensure compliance with any requirements to return parts. Follow all packaging instructions, and use all supplied packaging materials for shipping.

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.

Installing the support rails for the storage enclosure

Before you install the storage enclosure, you must first install the support rails.

Procedure

To install the support rails, complete the following steps.

1. Locate the rack mounting rails and screws (Figure 19). The rail assembly consists of two rails that must be installed in the rack cabinet.

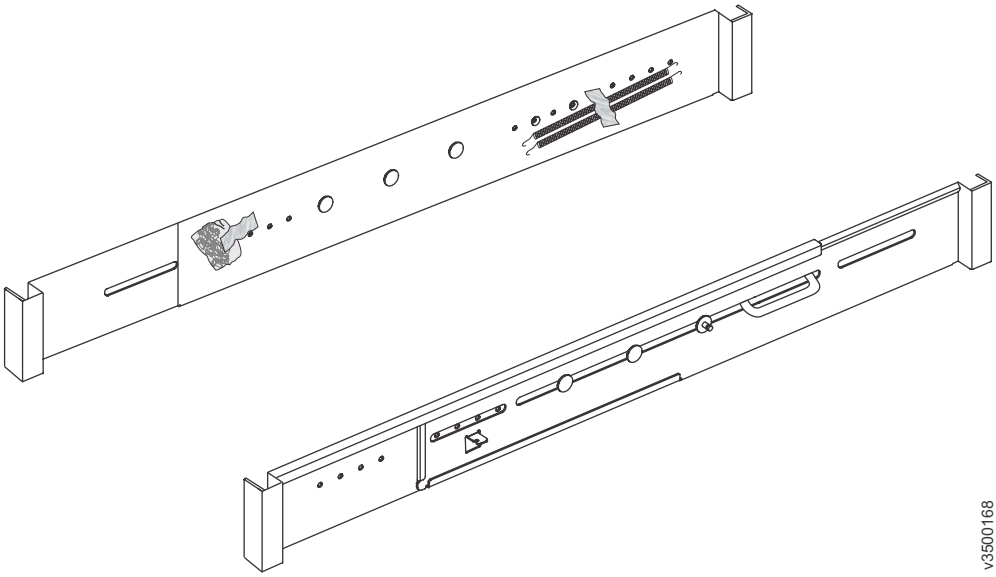


Figure 19. Rack mounting rails and screws

2. Your rack mounting rails may include a u-shaped bolt, which is shown in Figure 19, that must be removed before installing the rails. If this u-bolt is present, remove the u-bolt by removing the two nuts that secure the bolt to the rail.
3. Remove the springs that are taped to one of the rails.
4. Attach a spring to the outside of each rail.
   a. Attach the circle end of the spring around the stud on the rail (see Figure 20 on page 53).
   b. Pulling on the spring, attach the hook end of the spring to the tab on the rail.

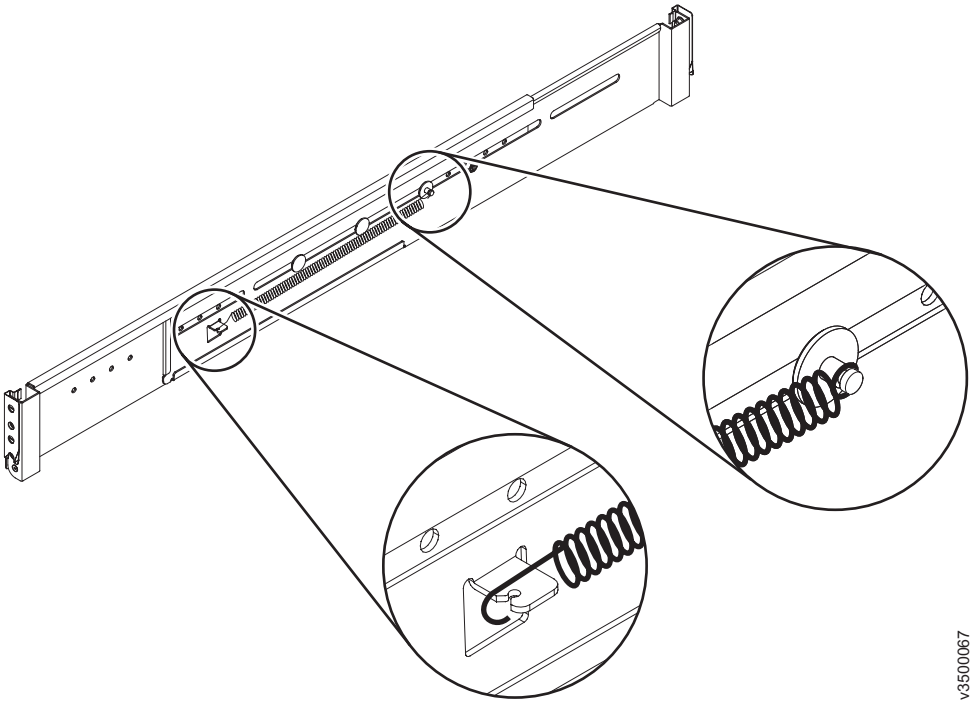


Figure 20. Installing the rail spring

5. At the front of the rack cabinet, identify the two standard rack units (2U) of space in the rack into which you want to install the support rails. Figure 21 shows two rack units with the front mounting holes identified.

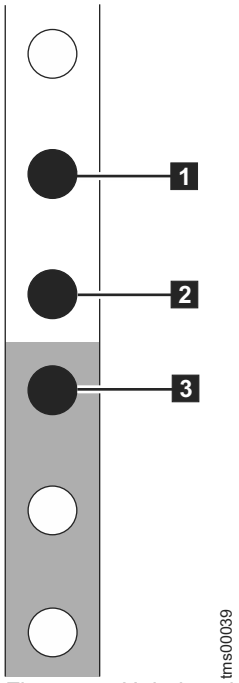


Figure 21. Hole locations in the front of the rack

1 Upper rail mounting bracket pin
2 Rack mounting screw hole
3 Lower rail mounting bracket pin

Note: Each rail comes with two medium bracket pins in the front bracket and two medium bracket pins in the rear bracket. The medium bracket pins are for installation in a 19-inch IBM rack cabinet. If you are installing the enclosure in a non-IBM rack cabinet, you might need to replace the set of medium bracket pins on the front and rear of the rail with either the small or large bracket pins that are included in the rail kit.

6. At each end of the rail, grasp the tab **1** and pull *firmly* to open the hinge bracket (see Figure 22).

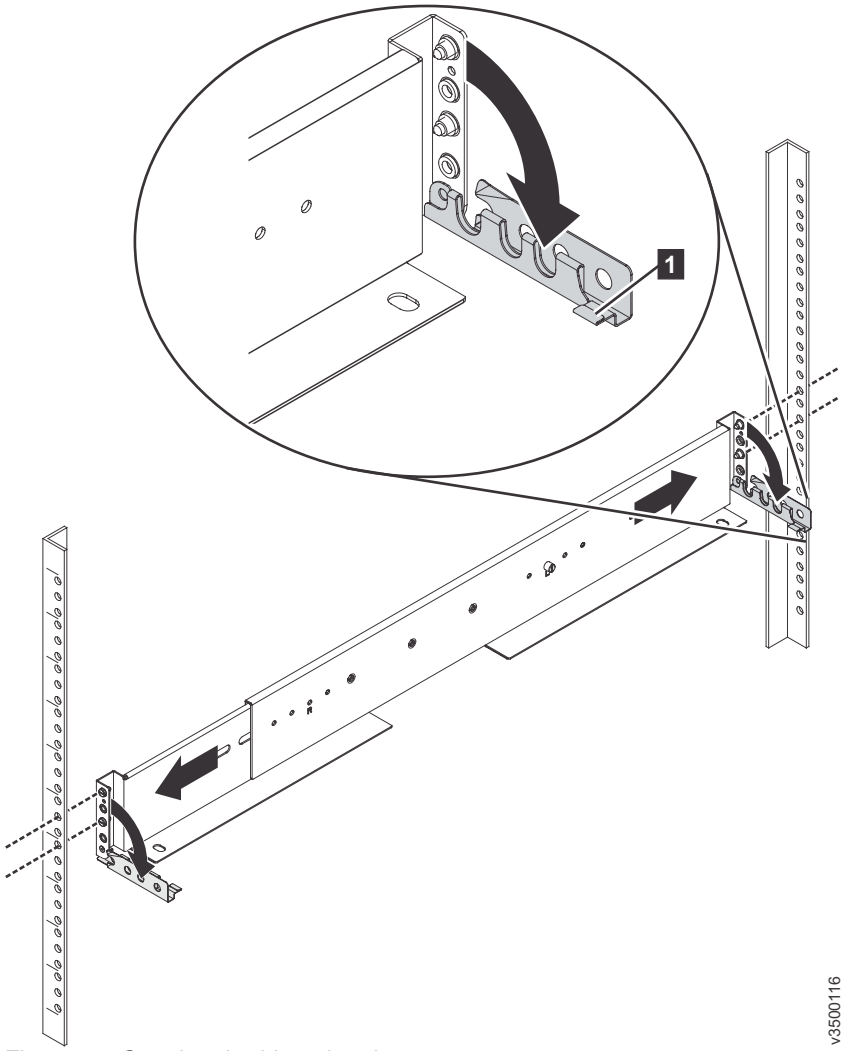


Figure 22. Opening the hinge brackets

7. Align the holes in the rail bracket with the holes on the front and rear rack cabinet flanges. Ensure that the rails are aligned on the inside of the rack cabinet.
8. On the rear of the rail, press the two bracket pins into the holes in the rack flanges and close the rear hinge bracket to secure the rail to the rack cabinet flange (see Figure 23 on page 55).

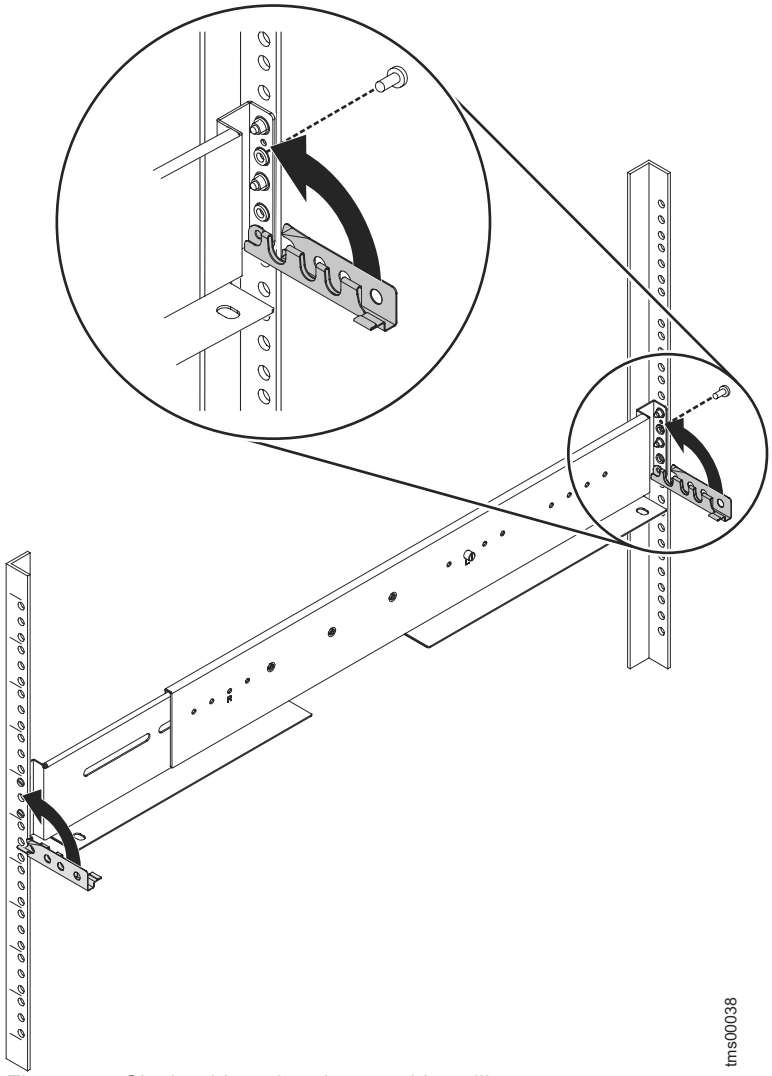


Figure 23. Closing hinge brackets and installing rear screw

9. On the front of the rail, press the two bracket pins into the holes in the rack flanges and close the front hinge bracket to secure the rail to the rack cabinet flange (see Figure 23).
10. Secure the rear of the rail to the rear rack flange by installing an M5 screw between the upper and lower mounting pins (see Figure 23).
11. Repeat steps 7 on page 54 through 10 to secure the opposite rail to the rack cabinet.

Replacing a canister

Contact IBM support for assistance in replacing a failed canister.

Replacing a CMOS battery in a canister

Learn how to replace the CMOS battery in a canister.

Before you begin

This product was designed 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 all safety instructions.

CAUTION:
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. (C045)

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

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 CMOS battery.

About this task

To replace the CMOS battery, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Disconnect all cables from the canister containing the CMOS battery to be replaced, making note of the cable connections to each interface card.
3. Remove the canister.
4. Remove the interface card located above the battery.
5. Remove the CMOS battery from the canister system board.
6. Install the new battery.
7. Reinstall the interface card.
8. Replace the canister in the enclosure.
9. Connect the cables to the interface cards in the canister, and connect the Ethernet management cable to the canister.

Replacing an interface card

Contact IBM support for assistance in replacing a failed interface card.

Replacing the front panel

Learn how to replace the enclosure front panel.

Before you begin

DANGER

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

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

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

  To disconnect:

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

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)**

About this task

To replace the front panel, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Shut down all host I/O to the system.
3. Power down the system using the CLI if possible, or remove power.
4. Wait for all LEDs to turn off, and then disconnect the two power cables.
5. Noting their locations for proper replacement, disconnect all interface card cables, and the two Ethernet management cables.
6. Remove the two battery modules.
7. Using two persons, remove the enclosure from the rack.
8. Remove the enclosure top cover by removing the 20 M3 Torx head screws from the top of the enclosure.

   Attention: Sharp edges, corners, and joints may be present on the sheet metal parts. Use care when handling to avoid cuts, scrapes, and pinching.
9. Disconnect the cable from the front panel.
10. Remove the two screws that secure the front panel to the enclosure, and remove the front panel.
11. Place the new front panel in the enclosure and secure it with the two screws.
12. Connect the cable that leads from the midplane to the front panel.
13. Replace the enclosure top cover, and secure it with the 20 M3 Torx head screws.
14. Install the enclosure in the rack.
15. Install the two battery modules.
16. Connect the cables to the interface cards in the enclosure, and connect the Ethernet management cables.
17. Connect the two power cables to the power supplies. The enclosure is now ready for host I/O.

What to do next

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

Replacing the power interposer board

Learn how to replace the power interposer board (PIB).

Before you begin

DANGER

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

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

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

  To disconnect:

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

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)**

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

About this task

To replace the power interposer board, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Shut down all host I/O to the system.
3. Power down the system by using the CLI if possible, or remove power.
4. Wait for all LEDs to turn off, and then disconnect the two power cables.
5. Noting their locations for proper replacement, disconnect all interface card cables, and the two Ethernet management cables.
6. Remove the two battery modules.
7. Using two persons, remove the enclosure from the rack.
8. Remove the enclosure top cover by removing the 20 M3 Torx head screws from the top of the enclosure.

   Attention: Sharp edges, corners, and joints may be present on the sheet metal parts. Use care when handling to avoid cuts, scrapes, and pinching.
9. Remove the power supplies from the enclosure.
10. To remove the PIB from the enclosure, complete the following steps:
    a. Lift the release handle on the top of the PIB, shown in Figure 24, away from the midplane.

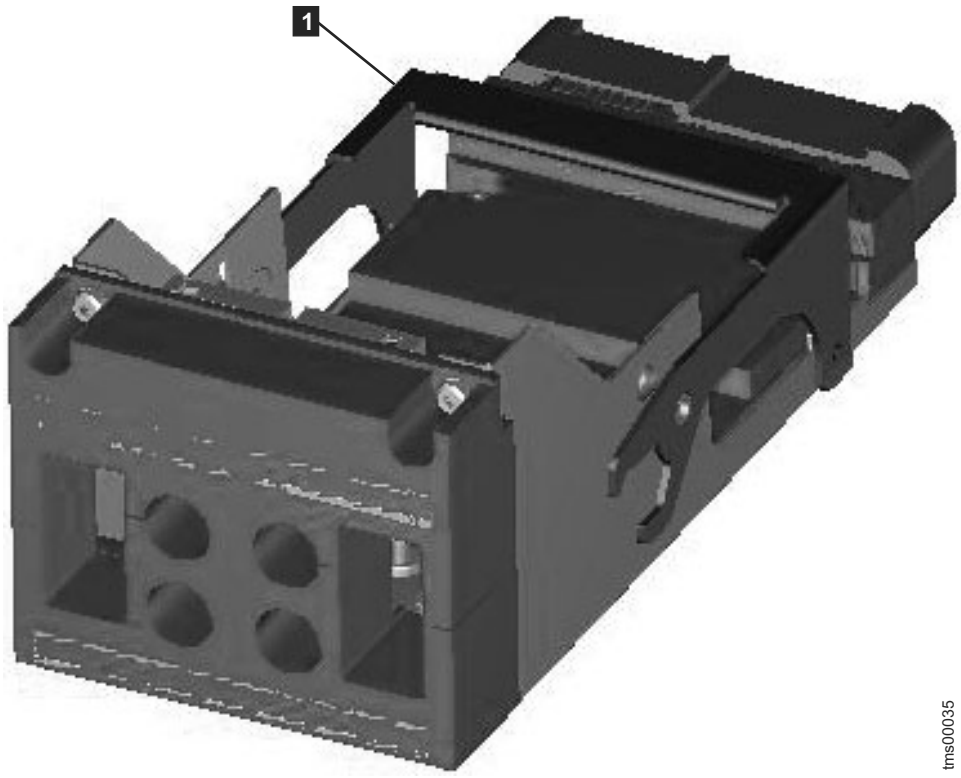


Figure 24. Power interposer board

1 Release handle

    b. Avoiding the connectors, lift the PIB straight up from the enclosure.

c. Align the new PIB with the guide pins on the floor of the enclosure.
d. Lower the PIB handle towards the midplane until the PIB locks into place.
e. Reinstall each power supply, making sure that the connector on the power supply aligns with its connector on the PIB.
f. Replace the enclosure top cover, and secure it with the 20 M3 Torx head screws.

11. Install the enclosure in the rack.
12. Install the two battery modules.
13. Connect the cables to the interface cards in the enclosure in their original locations, and connect the Ethernet management cables.
14. Connect the two power cables to the power supplies. The enclosure starts when power is connected.
15. After the boot process completes, connect one of the canisters to the service assistant.
16. Set the WWNN, MTM, and serial number based on the previously stored values by using the **satask chenclosurevpd** CLI commands (formerly **satask chenclosurevpd**). This action causes the nodes to warm start, so the CLI drops, the node re-reads the vpd and then comes back up.
17. Set the HIC configuration field by using the appropriate value:
    - If the enclosure is configured with FC4X8 (4 port 8 Gb Fibre Channel [FC]) adapters, run **satask chenclosurevpd -adapterconfig 1028**.
    - If the enclosure is configured with FC2X16 (2 port 16 GB FC) adapters, run **satask chenclosurevpd -adapterconfig 3598**.
    - If the enclosure is configured with four InfiniBand adapters, run **satask chenclosurevpd -adapterconfig 3341**.
    - If the enclosure is configured with ETH4x10 (4 port 10 GB FCoE) adapters, run **satask chenclosurevpd -adapterconfig 3855**.

    This action causes the nodes to warm start, so you may lose CLI/GUI access. The node re-reads the vpd then comes back up.
18. Validate that the HIC fields are set correctly by using **sainfo lsservicestatus** for each node canister
19. Reboot both nodes by using **satask stopnode -reboot** to incorporate the changes
20. The system is now ready for host I/O.

What to do next

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

Replacing the midplane

You should replace the midplane only if all normal troubleshooting measures for the other components in the system have been followed. Replacing the midplane is a disruptive process, as the system must be powered down and all components removed before the midplane is replaced.

Before you begin

DANGER

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

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

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

  To disconnect:

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

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)**

About this task

In particular, if there are connectivity issues with a particular redundant component, such as a canister, the component should be reseated, and replaced if

necessary before the midplane is replaced. If the enclosure VPD cannot be read, or the front panel is not detected, the issue could be due to a poor midplane connection.

To replace the midplane, complete the following steps:

Procedure

1. Read the safety precautions in the *IBM Systems Safety Notices*. These guidelines help you safely work with the system.
2. Shut down all host I/O to the system.
3. Power down the system by using the CLI if possible, or remove power.
4. Wait for all LEDs to turn off, and then disconnect the two power cables.
5. Noting their locations for proper replacement, disconnect all interface card cables, and the two Ethernet management cables.
6. Remove the two battery modules.
7. Using two persons, remove the enclosure from the rack.
8. Remove the enclosure top cover by removing the 20 M3 Torx head screws from the top of the enclosure.

   Attention: Sharp edges, corners, and joints may be present on the sheet metal parts. Use care when handling to avoid cuts, scrapes, and pinching.
9. Remove the two canisters partially from the enclosure.
10. Remove the flash modules partially from the enclosure.
11. Remove the power supplies from the enclosure.
12. Disconnect the cable that connects the front panel to the midplane.
13. Remove the power interface board (PIB). At this point, no components should be connected to the midplane.
14. Remove the screws that secure the midplane stiffener (carrier) to the enclosure.
15. Lift the midplane/stiffener assembly from the enclosure.
16. Remove the screws that secure the midplane to the stiffener.
17. Attach the new midplane to the stiffener.
18. Install the midplane/stiffener assembly in the enclosure.
19. Reconnect the cable that leads from the front panel to the midplane.
20. Install the power interface board (PIB).
21. Reseat the power supplies.
22. Reseat the flash modules.
23. Reseat the two canisters.
24. Replace the enclosure top cover, and secure it with the 20 M3 Torx head screws.
25. Install the enclosure in the rack.
26. Install the two battery modules.
27. Connect the cables to the interface cards in the enclosure in their original locations, and connect the Ethernet management cables.
28. Connect the two power cables to the power supplies. The enclosure starts when power is connected.
29. After the boot process completes, connect one of the canisters to the service assistant. The enclosure is now ready for host I/O.

What to do next

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

Appendix. Accessibility features for IBM FlashSystem 840

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

These are the major accessibility features for the IBM FlashSystem 840:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. PDF documents have been tested using Adobe Reader version 7.0. HTML documents have been tested using JAWS version 13.0.
- This product uses standard Windows navigation keys.
- Interfaces are commonly used by screen readers.
- Keys are discernible by touch, but do not activate just by touching them.
- Industry-standard devices, ports, and connectors.
- You can attach alternative input and output devices.

The system Information Center and its related publications are accessibility-enabled. .

Keyboard navigation

You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the Information Center from the keyboard by using the shortcut keys for your browser or screen-reader software. See your browser or screen-reader software Help for a list of shortcut keys that it supports.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Almaden Research
650 Harry Road
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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This explains the Federal Communications Commission's (FCC's) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2941
Email: lugi@de.ibm.com

Germany Electromagnetic Compatibility Directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

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 Mabnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk,New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Statement

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。

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。taiemi

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

Japan VCCI Council Class A statement

This explains the Japan Voluntary Control Council for Interference (VCCI) statement.

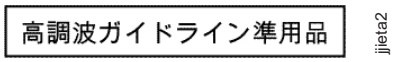
この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Japan Electronics and Information Technology Industries Association Statement

This explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for less than or equal to 20 A per phase.

高調波ガイドライン適合品

This explains the JEITA statement for greater than 20 A per phase.



Korean Communications Commission Class A Statement

This explains the Korean Communications Commission (KCC) statement.

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Russia Electromagnetic Interference Class A Statement

This statement explains the Russia Electromagnetic Interference (EMI) statement.

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Index

Numerics

A

B

C

D

E

F

G

H

T

U

V

W

Printed in USA

SC27-6297-00