IBM System Storage DS8870
Version 7 Release 0

Introduction and Planning Guide

GC27-4209-00

IBM System Storage DS8870
Version 7 Release 0

Introduction and Planning Guide

GC27-4209-00

Note:
Before using this information and the product it supports, read the information in the **Safety and environmental notices** and **Notices** sections.

This edition applies to version 7, release 0 of the IBM System Storage DS8870, and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Safety and Environmental notices

This section contains information about safety notices that are used in this guide and environmental notices for this product.

Safety notices

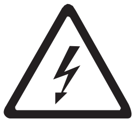
Observe the safety notices when using this product. These safety notices contain danger and caution notices. These notices are sometimes accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (Dxxx or Cxxx). Use the reference number to check the translation in the *IBM System Storage DS8000 Safety Notices*, P/N 98Y3994 on the documentation CD.

The sections that follow define each type of safety notice and give examples.

Danger notice

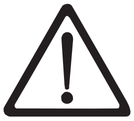
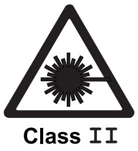
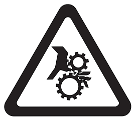
A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:

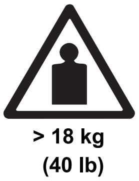


DANGER: An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. *(D004)*

Caution notice

A caution notice calls attention to 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. A caution notice can be accompanied by one of several symbols:

If the symbol is...	It means...
	A generally hazardous condition not represented by other safety symbols.
	This product contains a Class II laser. Do not stare into the beam. (*C029*) Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is...	It means...
	This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (*C008*)

Sample caution notices follow:

Caution

The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM® has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (*C007*)

Caution

The system contains circuit cards, assemblies, or both that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (*C014*)

Caution

When removing the Modular Refrigeration Unit (MRU), immediately remove any oil residue from the MRU support shelf, floor, and any other area to prevent injuries because of slips or falls. Do not use refrigerant lines or connectors to lift, move, or remove the MRU. Use handholds as instructed by service procedures. (*C016*)

Caution

Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre, ESCON®, FICON®) and an external public network . Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical fibre connectivity that does not pass through a public network.

Environmental notices

The environmental notices that apply to this product are provided in the *Environmental Notices and User Guide*, Z125-5823-*xx* manual. A copy of this manual is located on the publications CD provided in the ship group.

About this guide

The IBM System Storage® DS8870 Introduction and Planning Guide provides information about the IBM System Storage DS8870 storage unit.

This guide provides you with the following information:

- What you need to consider as you plan to use the DS8870 storage unit.
- How you can customize your DS8870 storage unit.

Who should use this guide

The IBM System Storage DS8870 Introduction and Planning Guide is for storage administrators, system programmers, and performance and capacity analysts.

Conventions used in this guide

The following typefaces are used to show emphasis:

boldface
Text in **boldface** represents menu items and lowercase or mixed-case command names.

italics Text in *italics* is used to emphasize a word. In command syntax, it is used for variables for which you supply actual values.

`monospace`
Text in `monospace` identifies the data or commands that you type, samples of command output, or examples of program code or messages from the system.

DS8000 library and related publications

Product manuals, other IBM publications, and websites contain information that relates to DS8000®.

DS8000 Information Center

The IBM System Storage DS8000 Information Center contains all of the information that is required to configure and manage the DS8000. The information center is updated between DS8000 product releases to provide the most current documentation. The information center is available at the following website: publib.boulder.ibm.com/infocenter/ds8000ic/index.jsp

DS8000 library

Table 1 on page xiv lists and describes the publications that make up the DS8000 library. Unless otherwise noted, these publications are available in Adobe portable document format (PDF). Go to the IBM Publications Center at www.ibm.com/shop/publications/order to obtain a publication.

Table 1. DS8000 library

Title	Description	Order Number
IBM System Storage DS: Command-Line Interface User's Guide	This guide describes the commands that you can use from the command-line interface (CLI) for managing your DS8000 configuration and Copy Services relationships. The CLI provides a set of commands that you can use to write customized scripts for a host system.	GC27-4212
IBM System Storage DS8000: Host Systems Attachment Guide	This guide provides information about attaching hosts to the DS8000 storage unit. The DS8000 provides a variety of host attachments so that you can consolidate storage capacity and workloads for open-systems hosts and System z® or S/390® hosts.	GC27-4210
IBM System Storage DS8000: Introduction and Planning Guide	This guide introduces the DS8000 product and lists the features you can order. It also provides guidelines for planning the installation and configuration of the storage unit.	GC27-4209
IBM System Storage Multipath Subsystem Device Driver User's Guide	This publication describes how to use the IBM Subsystem Device Driver (SDD) on open-systems hosts to enhance performance and availability on the DS8000. SDD creates single devices that consolidate redundant paths for logical unit numbers. SDD permits applications to run without interruption when path errors occur. It balances the workload across paths, and it transparently integrates with applications.	GC27-2122
IBM System Storage DS Application Programming Interface Reference	This publication provides reference information for the IBM System Storage DS application programming interface (API) and provides instructions for installing the Common Information Model Agent, which implements the API.	GC35-0516

Other IBM publications

Other IBM publications contain additional information that is related to the DS8000 product library. Table 2 is divided into categories to help you find publications that are related to specific topics.

Table 2. Other IBM publications

Title	Description	Order number
System Storage Productivity Center		
IBM System Storage Productivity Center Introduction and Planning Guide	This publication introduces the IBM System Storage Productivity Center hardware and software.	SC23-8824
Read This First: Installing the IBM System Storage Productivity Center	This publication provides quick instructions for installing the IBM System Storage Productivity Center hardware.	GI11-8938
IBM System Storage Productivity Center Software Installation and User's Guide	This publication describes how to install and use the IBM System Storage Productivity Center software.	SC23-8823

Table 2. Other IBM publications (continued)

Title	Description	Order number
IBM System Storage Productivity Center User's Guide	This publication describes how to use the IBM System Storage Productivity Center to manage the DS8000, IBM System Storage SAN Volume Controller clusters, and other components of your data storage infrastructure from a single interface.	SC27–2336
IBM Tivoli® Key Lifecycle Manager		
IBM Tivoli Key Lifecycle Manager Installation and Configuration Manager	This publication describes how to install and configure the Tivoli encryption key manager. The key server can be used to manage the encryption keys assigned to the IBM Full Disk Encryption disk drives in the DS8000.	SC23-9977
IBM System Management Pack for Microsoft		
IBM System Management Pack for Microsoft System Center Operations Manager User Guide	This publication describes how to install, configure, and use the IBM Storage Management Pack for Microsoft System Center Operations Manager (SCOM).	GC27-3909

IBM documentation and related websites

The following websites provide information about the DS8000 or related products or technologies:

Table 3. IBM documentation and related websites

Website	Link
IBM System Storage DS8000 series	www.ibm.com/servers/storage/disk/ds8000
Concurrent Copy for IBM System z and S/390 host systems	www.storage.ibm.com/software/sms/sdm
DS8000 command-line interface (DS CLI)	publib.boulder.ibm.com/infocenter/ds8000ic/index.jsp The information center has a complete command reference for the DS CLI.
Information about code bundles for DS8700, DS8800, and DS8870.	www.ibm.com/support/docview.wss?uid=ssg1S1003593 See **Section 3** for cross-reference links to SDD. www.ibm.com/support/docview.wss?uid=ssg1S1003740 www.ibm.com/support/docview.wss?uid=ssg1S1004204
IBM FlashCopy® for System z and S/390 host systems	www.storage.ibm.com/software/sms/sdm
IBM Flex System™ Information Center	publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp
Host system models, operating systems, adapters, and switches that the DS8000 series supports	www.ibm.com/systems/support/storage/config/ssic Click **New search**.

Table 3. IBM documentation and related websites (continued)

Website	Link
IBM Disk Storage Feature Activation (DSFA)	www.ibm.com/storage/dsfa
IBM version of the Java™ SE Runtime Environment (JRE) that is often required for IBM products	www.ibm.com/developerworks/java/jdk
Information about IBM Storage Easy Tier®	• www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101844 • www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101675 • www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102024
Remote Mirror and Copy (formerly Peer-to-Peer Remote Copy [PPRC]) for System z and S/390 host systems	www.storage.ibm.com/software/sms/sdm
SAN Fibre Channel switches	www.ibm.com/systems/storage/san
Subsystem Device Driver (SDD)	www.ibm.com/support/docview.wss?uid=ssg1S7000303
IBM Publications Center	www.ibm.com/shop/publications/order
IBM Redbooks® Publications	www.redbooks.ibm.com/

Related accessibility information

To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded for free from the Adobe website at: http://www.adobe.com/support/downloads/main.html

How to order IBM publications

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

The IBM Publications Center offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download at no charge. You can also order publications. You can access the IBM Publications Center at:

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

Send us your feedback

Your feedback is important in helping to provide the most accurate and high-quality information. If you have comments or suggestions for improving this publication, you can send us comments by e-mail to starpubs@us.ibm.com or use the Readers' Comments form at the back of this publication. Be sure to include the following information in your correspondence:

- Exact publication title
- Form number (for example, GA32–0689–00), part number, or EC level (located on the back cover)
- Page numbers to which you are referring

Note: For suggestions on operating enhancements or improvements, please contact your IBM Sales team.

Chapter 1. Introduction to IBM System Storage DS8000 series

IBM System Storage DS8000 series is a high-performance, high-capacity series of disk storage that supports continuous operations.

The latest and most advanced disk enterprise storage system in the DS8000 series is the IBM System Storage DS8870. It represents the latest in the series of high-performance and high-capacity disk storage systems. The DS8870 supports IBM POWER7® processor technology to help support higher performance.

The DS8000 series DS8870 supports functions such as point-in-time copy functions with IBM FlashCopy, FlashCopy Space Efficient, and Remote Mirror and Copy functions with Metro Mirror, Global Copy, Global Mirror, Metro/Global Mirror, IBM z/OS® Global Mirror, and z/OS Metro/Global Mirror. Easy Tier functions are supported on DS8870 storage units. I/O Priority Manager is also supported on the DS8870 units.

All DS8000 series models consist of a storage unit and one or two management consoles, two being the recommended configuration. The graphical user interface (GUI) or the command-line interface (CLI) provide the ability to logically partition storage and use the built-in Copy Services functions. For high-availability, the hardware components are redundant.

The Tivoli Key Lifecycle Manager (TKLM) software performs key management tasks for IBM encryption-enabled hardware, such as the DS8000 series by providing, protecting, storing, and maintaining encryption keys that are used to encrypt information being written to, and decrypt information being read from, encryption-enabled disks. TKLM operates on a variety of operating systems.

To learn additional information about the DS8000 series, you can view the e-Learning modules that are available from the IBM System Storage DS8000 Storage Manager Welcome page or the IBM System Storage DS8000 Information Center. The e-Learning modules provide animated presentations that describe the installation, configuration, management, and servicing of the DS8000 series.

DS8000 architecture

The architecture of the DS8000 is based on three major elements providing function specialization and three tiers of processing power.

Figure 1 on page 2 illustrates the elements:

- Host adapters (also known as front-end adapters) manage the I/O interfaces to other systems. They also manage the Fibre Channel path protocols for host I/Os and for replicating data to remote DS8000s.
- Device adapters (also known as back-end adapters) manage the internal storage devices. They also manage the SAS paths to drives, RAID protection, and drive sparing.
- A pair of high-performance redundant active-active Power servers, functionally positioned between the adapters and a key feature of the architecture.

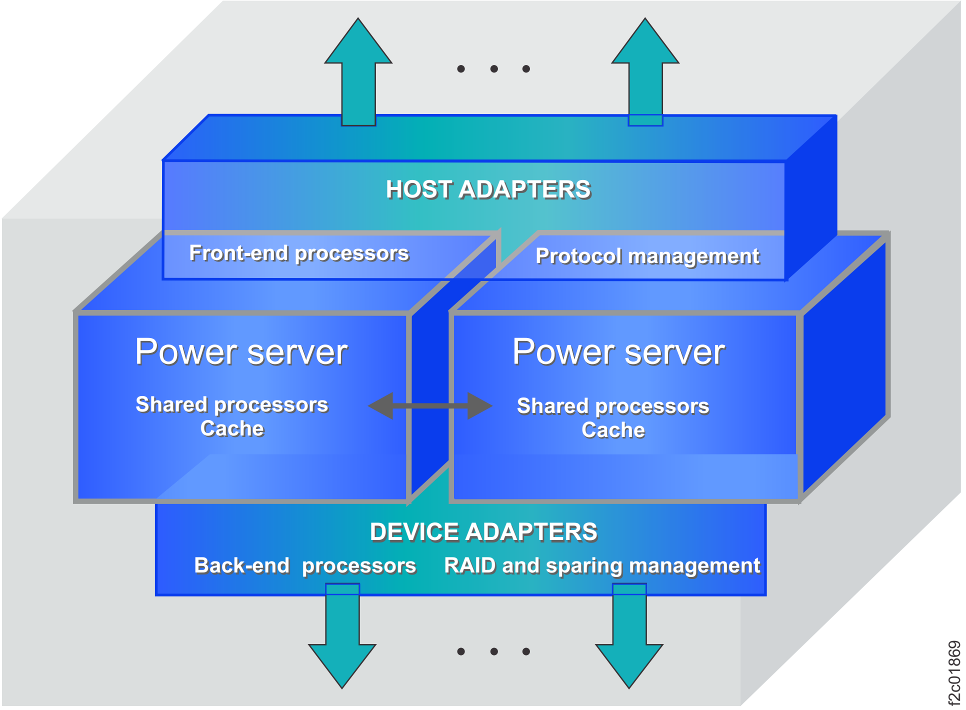


Figure 1. DS8000 architecture

The front-end and back-end adapters offload the bulk of the work to be done to the Power servers. Each Power server has multiple processor cores managed as a symmetric multiprocessing (SMP) pool of shared processing power to process the work done by that server. Each server runs an AIX® kernel that manages the processors, manages processor memory as a data cache, and more. For additional details on DS8000 architecture and design, see the latest IBM DS8000 Architecture and Implementation redbook.

Major benefits of the DS8000 architecture include:

Server foundation

- Promotes high availability and high performance through the use of field-proven Power servers
- Reduces custom components and design complexity
- Positions DS8000 to reap the benefits of server technology advances

Operating environment

- Promotes high availability and provides a high quality base for the system’s unique software through a field-proven AIX-based operating system kernel
- Provides an operating environment specifically optimized for Power servers (including performance and Reliability Availability Serviceability (RAS)
- Provides shared processor (SMP) efficiency
- Reduces custom code and design complexity

DS8870 overview

The DS8870 is the newest addition to the IBM System Storage DS8000 series. The DS8870 adds Model 961 (base frame) and 96E (expansion unit) to the 242x machine type family.

Features and functions of the DS8870

The following describes the features and functions of the DS8870.

High-density storage enclosure

The DS8000 series previously introduced the storage enclosure that supports 24 small form factor (SFF) 2.5” SAS drives in a 2U (height) factor. The DS8870 also supports a high-density and lower-cost-per-capacity large form factor (LFF) storage enclosure. This enclosure accepts 3.5" SAS drives, offering 12 drive slots. The LFF enclosure has a different appearance from the front than does the SFF enclosure, with its 12 drives slotting horizontally rather than vertically. For more information on storage enclosures, see “ DS8870 storage enclosure overview” on page 8.

High-density frame design

The DS8870 base model (961) supports up to 240 disks. Up to three additional expansion frames (Model 96E) can be added. The first expansion model supports up to 336 disks, the second expansion model supports up to 480 disks, and the third expansion model supports an additional 480 disks. The DS8870 can support a total of 1,536 drives (four frames) in a compact footprint, allowing high density and preserving valuable floor space in datacenter environments. Coupled with the DS8000 series cooling implementation, compact system footprint, and small form factor SAS-2 drives, a fully configured DS8870 consumes up to 37% less power than earlier generations of DS8000 storage units. For more information, see “ DS8870 (Models 961 and 96E)” on page 4.

IBM POWER7 technology

The DS8870 supports IBM POWER7 processor technology to help support high performance. It can be equipped with a 2-core, 4-core, 8-core, or 16-core processor complex for the highest performance requirements.

8 Gbps host and 8 Gbps device adapters

The DS8870 model offers host adapters that include high-function PCIe-attached four and eight-port Fibre Channel and IBM FICON host adapters. The DS8870 uses direct point-to-point high-speed PCIe connections to the I/O enclosures to communicate with the device and host adapters.

The DS8870 offers I/O enclosures that include up to 16 device adapters. The device adapters have four 8 Gbps Fibre Channel arbitrated loop (FC-AL) ports. The device adapters attach the storage enclosures to the DS8800.

Disk drive support

The DS8870 supports the following choice of disk drives:

- Solid state drives (SSDs) FDE:
  - 400 GB (FDE)
- Serial Attached SCSI (SAS) FDE drives:
  - 146 GB, 15K RPM
  - 300 GB, 15K RPM

  - 600 GB, 10K RPM
  - 900 GB, 10K RPM
  - 3 TB, 7.2K RPM
- SAS drives with Full Disk Encryption (FDE) and encryption Standby CoD:
  - 146 GB 15K RPM
  - 300 GB 15K RPM
  - 600 GB, 10K RPM
  - 900 GB 10K RPM
  - 3 TB 7.2K RPM

Business Class Feature

The DS8870 business class feature offers a streamlined, cost-competitive configuration with limited feature and function support. This model provides an upgrade path to the full enterprise class configuration and functions.

DS8870 (Models 961 and 96E)

The DS8870 includes Model 961 (base frame) and 96E (expansion model) offers higher performance than previous models in the DS8000 series.

Model 961 (base model)

Figure 2 on page 5 provides a high-level view of the front and back of the Model 961 base, which includes space for up to 15 disk drive sets (16 drives per disk drive set). In a maximum configuration, the base model can hold 240 disk drives (15 disk drive sets x 16 drives = 240 disk drives) **1** . The Model 961 is offered with a 2-core, 4-core, 8-core or 16-core processor complex. Expansion models (96E) can be added to the base model in an 8-core or 16-core system.

Note: You cannot add an expansion model to a DS8870 2-core or 4-core system.

The hardware management console (HMC) is stored below the drives **2** . Figure 3 on page 6 provides a detailed view of the HMC tray extended.

The DS8870 has an integrated rack power control (RPC) system that helps manage efficiency of power distribution. The POWER7 servers **3** contain the processor and memory that drive all functions within the DS8870. The power subsystem in the DS8870 is restriction of hazardous substances (RoHS) compliant. Other models in the IBM Storage DS8000 series contain primary power supply (PPS) units. The DS8870 uses direct current uninterruptible power supply (DC-UPS) units. The DC-UPS units improve energy efficiency. The DS8870 power subsystem also contains a faster processor with parity-protected memory.

The I/O enclosures provide connectivity between the adapters and the storage processors **4** . The adapters contained in the I/O enclosures can be either device adapters (DAs) or host adapters (HAs).

The base model contains DC-UPS power supplies **5** . The DC-UPS provides rectified ac power distribution and power switching for redundancy. The rack has two ac power cords. Each one feeding a DC-UPS. The DC-UPS distributes rectified line ac. If ac is not present at the input line, the output is switched to rectified ac from the partner DC-UPS. If neither ac input is active, the DC-UPS switches to 208V dc battery power for up to 50 seconds.

A redundant pair of RPC cards coordinate the power management within the storage facility 6 . The RPC cards are attached to the service processors in each complex allowing them to communicate with both the HMC and storage facility image logical partitions (LPARs). The RPC is also attached to the primary power system in each rack and on some models is indirectly connected to the fan-sense cards and to storage enclosures in each rack. The power system in each rack is either a primary power supply with associated batteries or an uninterruptible power supply (DC-UPS) with internal batteries.

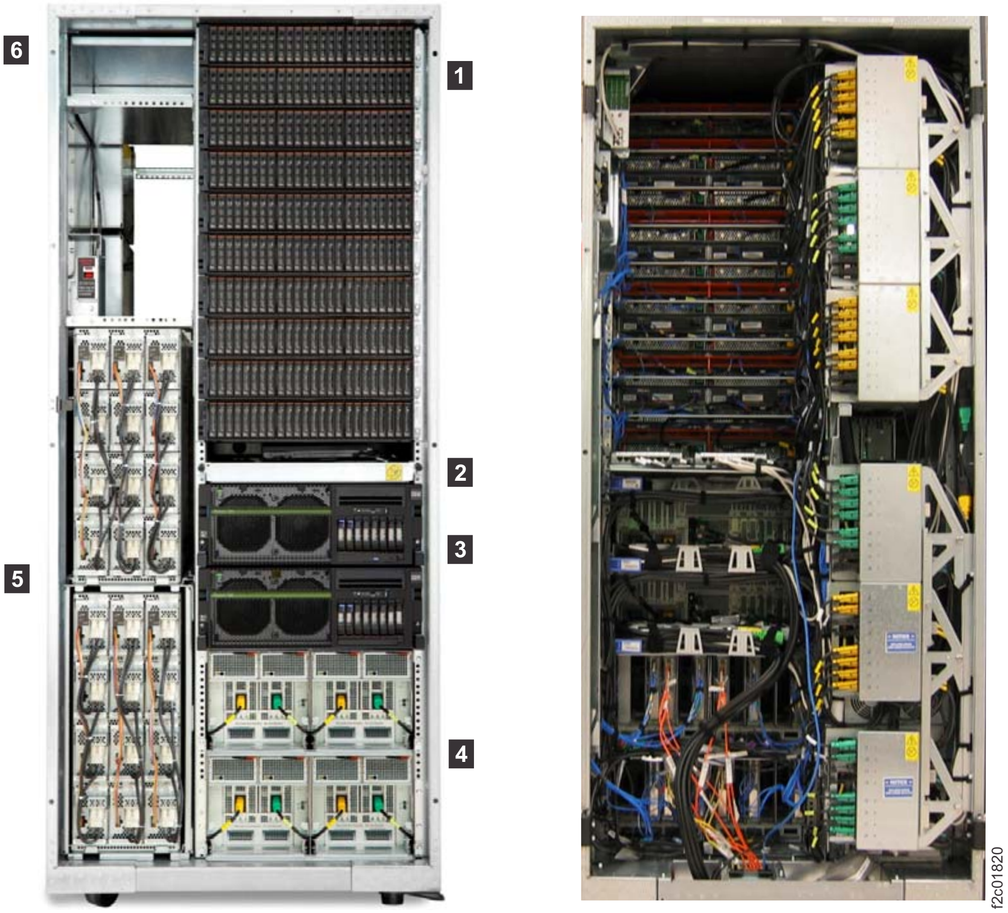


Figure 2. Base model (front and back views) of a Model 961 (4-core)

.

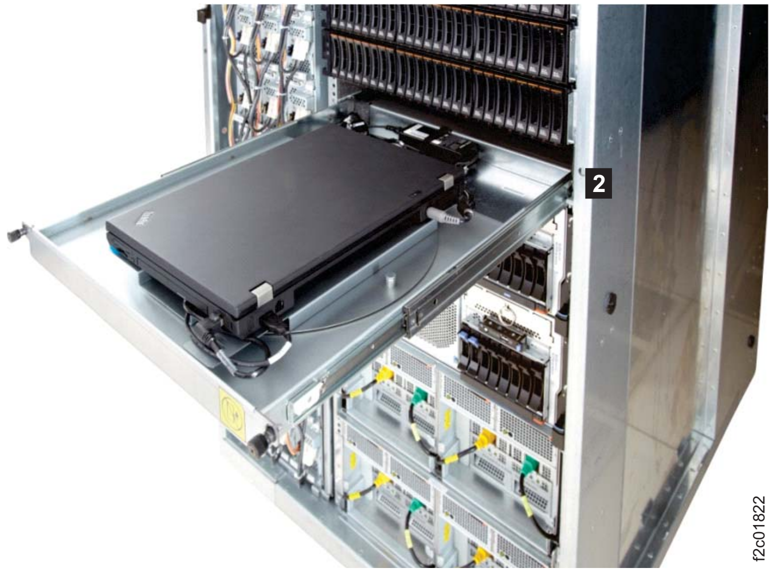


Figure 3. HMC location in a model 961 (4-core)

Model 96E (expansion model)

Figure 4 on page 7 shows the expansion model configuration of a Model 96E and the increased number of storage enclosures **1** that can be added. Up to three expansion models can be added to a base Model 961, for a total configuration of 1,536 drives.

The back side of the expansion model is the model power area. The expansion model contains two primary DC-UPS power supplies. As with the DC-UPS in base Model 961, they provide a redundant 208 V dc power distribution to the rack to convert the ac input into dc power.

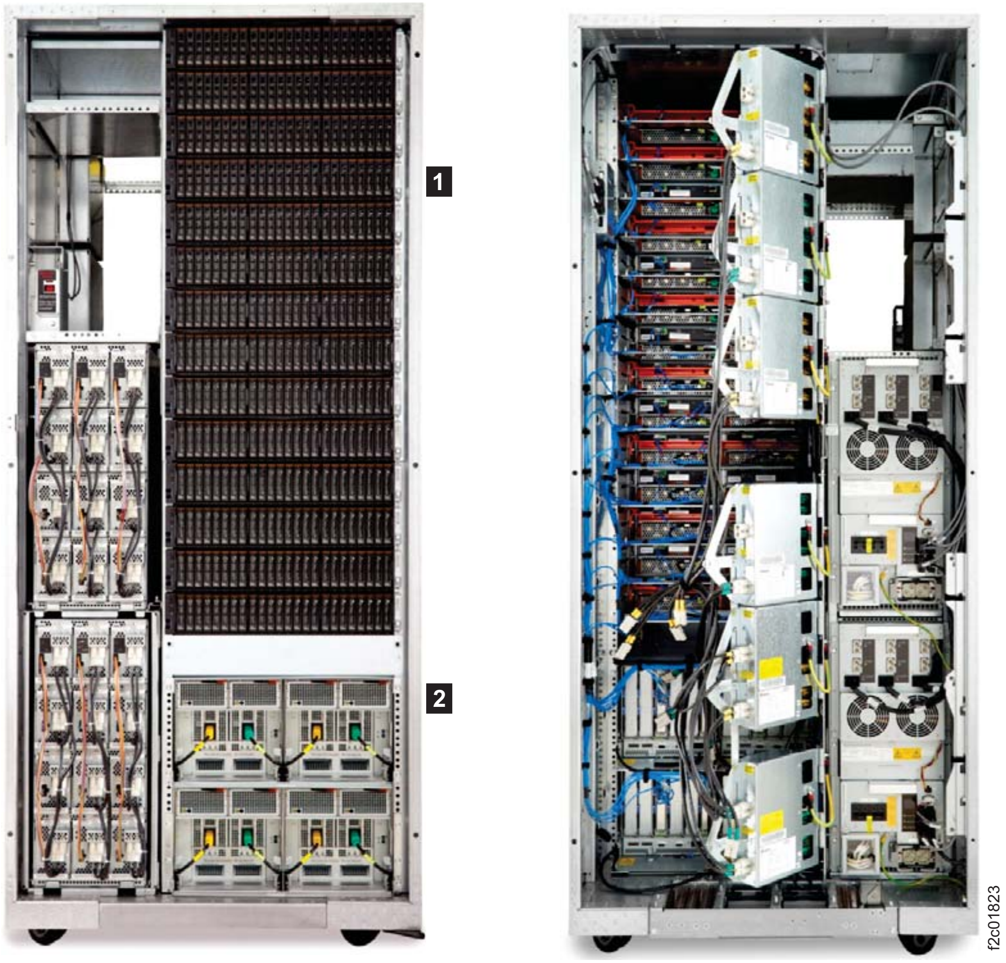


Figure 4. Expansion model (front and back views) of a Model 96E

Figure 5 on page 8 shows the detail of a DC-UPS at the back of the model.

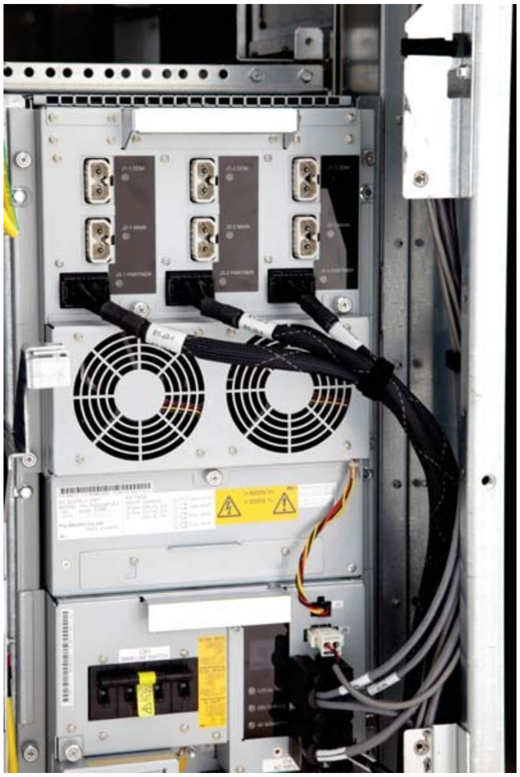


Figure 5. Expansion model (back view detail) of a Model 96E DC-UPS

For more information about Model 961 and 96E, see "Overview of physical configurations" on page 69.

DS8870 storage enclosure overview

The DS8870 includes two types of high-density storage enclosure, the 2.5" small form factor (SFF) enclosure and the new 3.5" large form factor (LFF) enclosure.

The DS8870 high-density storage enclosure is a small form factor (SFF) drive enclosure. The 3.5" enclosure is a large form factor (LFF) drive enclosure. Both enclosures have the following features:

- Fibre Channel (FC) cable connection
- A high performance 8 Gbps optical FC-AL fabric attachment from the device adapter to the storage expansion enclosure
- An enclosure control card providing an FC to SAS bridge, matching industry standards.
- Device adapter (DA) attachment, which supports dual-trunked Fibre Channel, allowing for higher bandwidth and an extra layer of redundancy

Figure 6 on page 9 shows front and back views of the storage enclosure. This supports 24 SFF, 2.5" SAS drives. The storage enclosure is 2U (EIA units) or 3.5" in height. The front of the enclosure contains slots for 24 drives, and also contains enclosure-level status indicators. The back of the enclosure contains:

- Two power supplies.
- Two interface controller (IC) cards for redundancy.

All power and signal cables exit from the back of the enclosure.

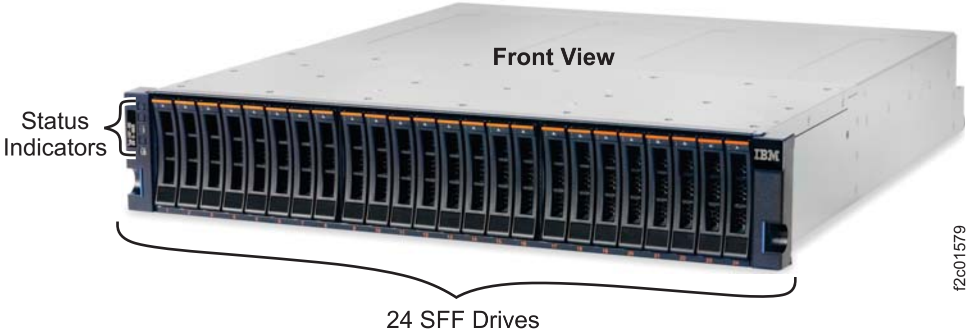


Figure 6. Front view of the storage expansion enclosure

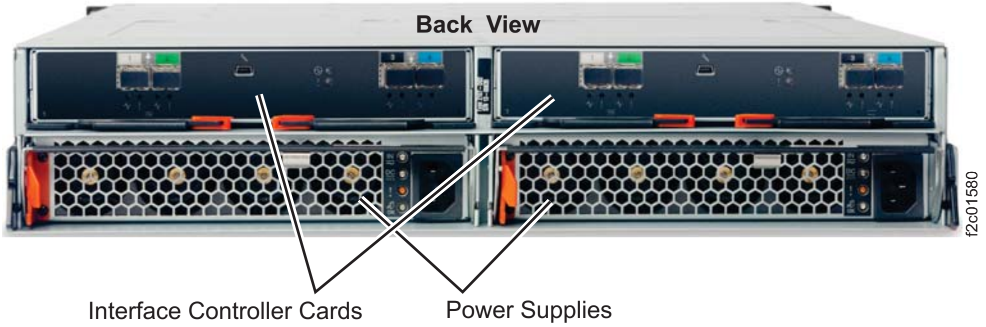


Figure 7. Back view of the storage expansion enclosure

The DS8870 supports a high-density and large form factor (LFF) storage enclosure. This enclosure accepts 3.5" drives, offering 12 drive slots. The SFF enclosure offers 24, 2.5" drive slots. The LFF enclosure has a different appearance from the front than does the SFF enclosure, with its 12 drives slotting horizontally rather than vertically.

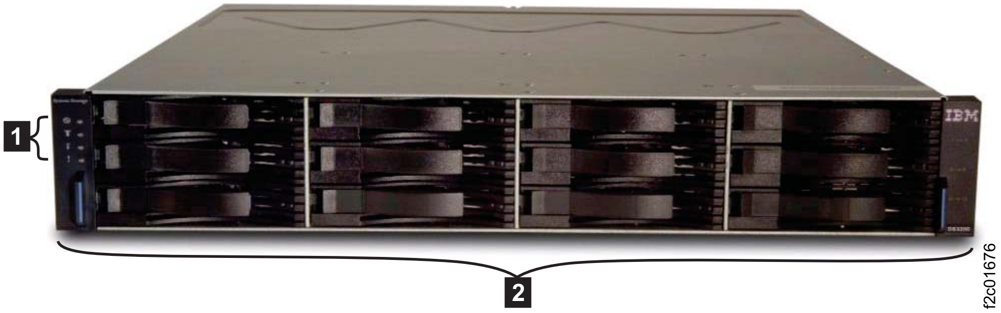


Figure 8. Front view of the LFF storage expansion enclosure

The following notes provide additional information about the labeled components in the Figure 8:

1. Status indicators for the enclosure
2. 12 LFF drives, 3.5"

Performance features

Features of the expansion storage enclosure include:

- Support for up to four enclosures per loop
- Redundant, integrated power and cooling
- 6 Gbps SAS data transfer rate to the disk drives
- Support for optical 8 Gbps FC-AL
- FC-AL to SAS protocol conversion

Power supply and cooling

Power supply features and requirements include:

- The subsystem in the DS8870 is restriction of hazardous substances (RoHS) compliant.
- The DS8870 supports IBM POWER7 processor technology to help support high performance. It can be equipped with a 2-core, 4-core, 8-core, or 16-core processor complex for the highest performance requirements.
- The power and cooling system are composed of two direct current uninterruptible power supply (DC-UPS) units, which improve energy efficiency and supply rectified ac.
- Each power supply contains fans for cooling.

Frame configuration notes

There are two types of frame configurations supported, which are commonly designated as A and B frames. An A frame is the base configuration (Model 961) and contains not just power and storage but also the I/O enclosures, Ethernet switch, Hardware Management Console (HMC), and I/O bays. If more storage is needed than the A frame (base Model 961) can provide, the next step is to add a B frame, or expansion (Model 96E). The 96E contains more storage and more I/O bays, increasing the number of device adapter cards you can select. Up to three expansion models can be added to the configuration.

DS8870 (Business Class feature)

The IBM System Storage DS8870 business class feature offers a streamlined, lower cost configuration than the standard configuration. The DS8870 business class feature for Model 961, reduces the number of installed device adapters and I/O enclosures while increasing the number of storage enclosures attached to the remaining device adapters. The business class option allows a system to be configured with more drives per device adapter, reducing configuration cost and increasing adapter usage.

The DS8870 Model 961 with business class has the following features:

- Dual two-core processor complex
- Up to 32 GB of processor memory on a two-core configuration

  Note: A 16 GB processor memory option is available with feature code 4311 for the two-core configuration, business class feature and a 32 GB processor memory option is available with feature code 4312.
- Up to 4 host adapters or up to 32 host ports, FCP (Fibre Channel protocol) or FICON

Note: Copy Services, SSD drives, and I/O priority manager are not supported on business class with 16 GB cache.

The DS8870 Model 961 business class feature supports up to 144 disk drives. For more information, including maximum storage capacities, see "Overview of physical configurations" on page 69. The cabling of the expansion frame remains the same for both the standard and business class.

DS8000 model conversion limitations

There are model conversion limitations for the DS8870, noted below.

DS8870 code cannot be installed in the DS8800 or older models.

Machine types overview

The DS8000 series include several machine types. Order a hardware machine type for the storage unit hardware and a corresponding function authorization machine type for the licensed functions that are planned for use.

Table 4 shows the available hardware machine types and their corresponding function authorization machine types.

Table 4. Available hardware and function authorization machine types

Hardware		Licensed functions	
Hardware machine type	**Available hardware models**	**Corresponding function authorization machine type**	**Available function authorization models**
Machine type 2421 (1-year warranty period)	Models 961 and 96E	Machine type 2396 (1-year warranty period)	Model LFA
Machine type 2422 (2-year warranty period)		Machine type 2397 (2-year warranty period)	
Machine type 2423 (3-year warranty period)		Machine type 2398 (3-year warranty period)	
Machine type 2424 (4-year warranty period)		Machine type 2399 (4-year warranty period)	

Because the 242x hardware machine types are built upon the 2107 machine type and microcode, some interfaces might display `2107`. This display is normal, and is no cause for alarm. The 242x machine type that you purchased is the valid machine type.

Features overview

The DS8870 storage units are designed to provide you with high-performance, connectivity, and reliability so that your workload can be easily consolidated into a single storage subsystem.

The following list provides an overview of some of the features that are associated with the DS8870.

Note: Additional specifications are provided at www.ibm.com/systems/storage/disk/ds8000/specifications.html.

Storage pool striping (rotate extents)

Storage pool striping is supported on the DS8000 series, providing improved performance. The storage pool striping function stripes new volumes across all ranks of an extent pool. The striped volume layout reduces workload skew in the system without requiring manual tuning by a storage administrator. This approach can increase performance with minimal operator effort. With storage pool striping support, the system automatically performs close to highest efficiency, which requires little or no administration. The effectiveness of performance management tools is also enhanced, because imbalances tend to occur as isolated problems. When performance administration is required, it is applied more precisely.

You can configure and manage storage pool striping using the DS Storage Manager, DS CLI, and DS Open API. The default of the extent allocation method (EAM) option that is applied to a logical volume is now rotate extents. The rotate extents option (storage pool striping) is designed to provide the best performance by striping volume extents across ranks in extent pool. Existing volumes can be re-configured nondisruptively by using manual volume migration and volume rebalance.

The storage pool striping function is provided with the DS8000 series at no additional charge.

DS8870 with POWER7 processor technology

The DS8870 is the newest addition to the IBM® System Storage® DS series. The DS8870 adds Models 961 (base frame) and 96E (expansion unit) to the 242x machine type family. The DS8870 supports IBM POWER7 processor technology to provide high performance. It can be equipped with a 2-core, 4-core, 8-core, or 16-core processor complex. The DS8870 offers up to three times higher performance than previous models in the DS8000® series for the highest performance requirements.

Rack power control system with DC-UPS

The DS8870 uses direct current uninterruptible power supply (DC-UPS) units for a higher level of resilience. The DC-UPS units also improve energy efficiency.

RoHS The power subsystem in the DS8870 meets restriction of hazardous substances (RoHS) requirements.

POWER7 processor technology

DS8870

The DS8870 supports IBM POWER7 processor technology to help support high performance. The DS8870 offers up to three times higher performance than the previous DS8000 series models. It can be equipped with a 2-core, 4-core, 8-core, or 16-core processor complex for the highest performance requirements.

Solid-state drives (SSDs)

The DS8000 series can accommodate fast solid-state drives, and traditional spinning disk drives, to support multitier environments. SSDs are the best choice for I/O intensive workload. They come in disk enclosures and have the same form factor as the traditional disks. FDE (Full Disk Encryption) SSDs are available for the DS8870 in a 400 GB capacity.

Industry standard disk drives

The DS8000 series models offer a selection of disk drives.

DS8870

Along with SSD drives, the DS8870 supports Serial Attached SCSI (SAS) FDE and encryption Standby CoD drives, available in the following capacities:

- 146 GB 15K drive set
- 300 GB 15K drive set
- 600 GB 10K drive set
- 900 GB 10K drive set
- 3 TB 7.2K drive set

Sign-on support using Lightweight Directory Access Protocol (LDAP)

The DS8000 provides support for both unified sign-on functions (available through the DS Storage Manager), and the ability to specify an existing Lightweight Directory Access Protocol (LDAP) server. The LDAP server can have existing users and user groups that can be used for authentication on the DS8000.

Setting up unified sign-on support for the DS8000 is achieved using the Tivoli Storage Productivity Center. See the Tivoli Storage Productivity Center Information Center for more information.

Note: Other supported user directory servers include IBM Directory Server and Microsoft Active Director.

Easy Tier

Easy Tier is designed to determine the appropriate tier of storage based on data access requirements and then automatically and nondisruptively move data, at the subvolume or sub-LUN level, to the appropriate tier on the DS8000. Easy Tier is an optional feature on the DS8870 that offers enhanced capabilities through features such as auto-rebalancing, hot spot management, rank depopulation, support for extent space-efficient (ESE) volumes, auto performance rebalance in both homogeneous and hybrid pools, and manual volume migration.

Multitenancy support (resource groups)

Resource groups functions provide additional policy-based limitations to DS8000 users, which in conjunction with the inherent volume addressing limitations support secure partitioning of copy services resources between user-defined partitions. The process of specifying the appropriate limitations is performed by an administrator using resource groups functions. DS Storage Manager (GUI) and DS CLI support is also available for resource groups functions.

It is feasible that multitenancy can be supported in certain environments without the use of resource groups provided the following constraints are met:

- Either copy services must be disabled on all DS8000 that share the same SAN (local and remote sites), or the landlord must configure the operating system environment on all hosts (or host LPARs) attached to a SAN which has one or more DS8000 units, so that no tenant can issue copy services commands.
- The zOS Distribute Data backup feature is disabled on all DS8000 units in the environment (local and remote sites).
- Thin provisioned volumes (ESE or TSE) are not used on any DS8000 unit in the environment (local and remote sites).

- On zSeries® systems there can be no more than one tenant running in a given LPAR, and the volume access must be controlled so that a CKD base volume or alias volume is only accessible by a single tenant's LPAR or LPARs.

I/O Priority Manager

The I/O Priority Manager can help you effectively manage quality of service levels for each application running on your system. This feature aligns distinct service levels to separate workloads in the system to help maintain the efficient performance of each DS8000 volume. The I/O Priority Manager detects when a higher-priority application is hindered by a lower-priority application that is competing for the same system resources. This might occur when multiple applications request data from the same disk drives. When I/O Priority Manager encounters this situation, it delays lower-priority I/O data to assist the more critical I/O data in meeting their performance targets.

Use this feature when you are looking to consolidate more workloads on your system and need to ensure that your system resources are aligned to match the priority of your applications. This feature is useful in multitenancy environments.

Note: The default setting for this feature is "disabled" and must be enabled for use.

Note: To enable monitoring, use DS CLI commands to set I/O Priority Manager to "Monitor" or to "MonitorSNMP," or use the DS Storage Manager to set I/O Priority Manager to "Monitor" on the Advanced tab of the Storage Image Properties page. The I/O Priority Manager feature can be set to "Managed" or "ManagedSNMP," but the I/O priority is not managed unless the I/O Priority Manager LIC key is activated.

Peripheral Component Interconnect Express® (PCIe) I/O enclosures

The DS8870 processor complexes use a PCIe infrastructure to access I/O enclosures. PCIe is a standard-based replacement to the general-purpose PCI expansion bus. PCIe is a full duplex serial I/O interconnect. Transfers are bi-directional, which means data can flow to and from a device simultaneously. The PCIe infrastructure uses a non-blocking switch so that more than one device can transfer data.

In addition, to improve I/O Operations Per Second (IOPS) and sequential read/write throughput, the I/O enclosures are directly connected to the internal servers through point-to-point PCIe cables. I/O enclosures no longer share common "loops," they connect directly to each server through separate cables and link cards, thus enabling a performance improvement over previous models.

Four- and eight-port 8 Gbps FCP and FICON adapters

The DS8870 includes high-function PCIe-attached 4-port, 8 Gbps FCP and FICON adapter. The device adapters attach the storage enclosureto the internal processors and cache via the PCIe.

The DS8870 supports four- and eight-port Fibre Channel/FICON host adapters. These 8 Gbps host adapters are offered in longwave and shortwave.
The DS8870 supports up to 16 host adapters maximum (up to 128 Fibre Channel Protocol/FICON ports) on a 8-core or 16-core configuration.

Note: The DS8870 supports connections from adapters and switches that are 8 Gbps, but auto-negotiates them to 4 Gbps or 2 Gbps, as needed.

High performance FICON

A high performance FICON feature is available that allows FICON extension (FCX) protocols to be used on fibre channel I/O ports that are enabled for the use of the FICON upper layer protocol. The use of FCX protocols provides a significant reduction in channel utilization. This reduction can allow more I/O input on a single channel and also for a reduction in the number of FICON channels required to support a given workload.

IBM Standby Capacity on Demand

Using the IBM Standby Capacity on Demand (Standby CoD) offering, you can install inactive disk drives that can be easily activated as business needs require. To activate, you logically configure the disk drives for use, nondisruptive activity that does not require intervention from IBM. Upon activation of any portion of the Standby CoD disk drive set, you must place an order with IBM to initiate billing for the activated set. At that time, you can also order replacement Standby CoD disk drive sets.

The offers up to six Standby CoD disk drive sets (96 disk drives) can be factory- or field-installed into your system.

Note: Solid-state drives are unavailable as Standby Capacity on Demand drives.

Host adapter usage statistics and additional counters

Customers can use usage statistics to monitor their I/O activity. For example, customers can monitor how busy the host adapters are and use that data to help manage their SAN. For more information on available commands, see the *IBM System Storage® DS8000 Command-Line Interface Guide*.

1 TB system cache support

POWER7 supports 1 TB of memory (the cache size is always less than 1 TB).

Online Information Center

The online Information Center is an information database that provides you with the opportunity to quickly familiarize yourself with the major aspects of the DS8000 series and to easily recognize the topics for which you might require more information. It provides information regarding user assistance for tasks, concepts, reference, user scenarios, tutorials, and other types of user information. Because the information is all in one place rather than across multiple publications, you can access the information that you need more efficiently and effectively.

For the latest version of the online Information Center, go to http://publib.boulder.ibm.com/infocenter/dsichelp/ds8000ic/index.jsp

Limitations

Known limitations exist for the DS8000 with regard to storage units, model conversion, and the DS Storage Manager interface.

The following list describes known limitations for DS8000 storage units:

- For the Dynamic Volume Expansion function, volumes cannot be in Copy Services relationships (point-in-time copy, FlashCopy SE, Metro Mirror, Global Mirror, Metro/Global Mirror, and z/OS Global Mirror) during expansion.
- The size limit for single volumes in a Copy Services relationship is 2 TB. This limit does not apply to extents (when part of multiple volumes).
- The amount of physical capacity within a 242x system that can be logically configured for use is enforced by the 242x Licensed Machine Code to maintain compliance with the extent of IBM authorization established for licensed functions activated on the machine.
- The deactivation of an activated licensed function, or a lateral change or reduction in the license scope, is a nondisruptive activity that occurs at the next machine IML. For example:
  - A lateral change is defined as changing the license scope from FB to CKD or from CKD to FB.
  - A reduction is defined as changing the license scope from ALL to FB or from ALL to CKD.
- The following activities are disruptive:
  - Addition of the Earthquake Resistance Kit feature 1906.
  - Removal of an expansion model from the base model. Data is not preserved during this activity.
- Some DS8000 series functions are unavailable or are not supported in all environments. Go to the *System Storage Interoperation Center* (SSIC) website at www.ibm.com/systems/support/storage/config/ssic for the most current information on supported hosts, operating systems, adapters, and switches.
- Plant configured systems with Encryption Drive Set support (feature number 1750) can support a field installation of encrypted drives. Encryption drive set deactivation support must be ordered using feature number 1754.
- SSD drive sets are not supported in RAID-6 or RAID-10 configurations.
- Nearline SAS drives are not supported on RAID-5 and RAID-10 configurations.
- In a tiered extent pool (with Enterprise and SSD drives), Extent Space Efficient (ESE) volumes cannot allocate extents to SSD ranks.
- Conversions between warranty machine types are not supported.
- Thin provisioning functions are not supported on System z/OS volumes.

DS Storage Manager limitations

It is important to note which Internet browsers are supported for the use of DS Storage Manager (GUI).

The DS Storage Manager (GUI) can be used on different versions of Internet browsers. Supported browsers include:

- Mozilla Firefox 10 ESR.
- Microsoft Internet Explorer 9 .

You must select appropriate browser security settings to open the DS Storage Manager with a browser. Additionally, if you access the DS Storage Manager through the Tivoli® Storage Productivity Center using Internet Explorer, you must configure Internet Explorer for that process. For instructions on how to perform these actions, visit the IBM System Storage DS8000 Information Center and select Installing > DS Storage Manager postinstallation instructions > Internet browser support.

DS8000 physical footprint

The physical footprint dimensions, caster locations, and cable openings for your storage unit help you plan your installation site.

Figure 9 shows the overall physical footprint of a DS8870.

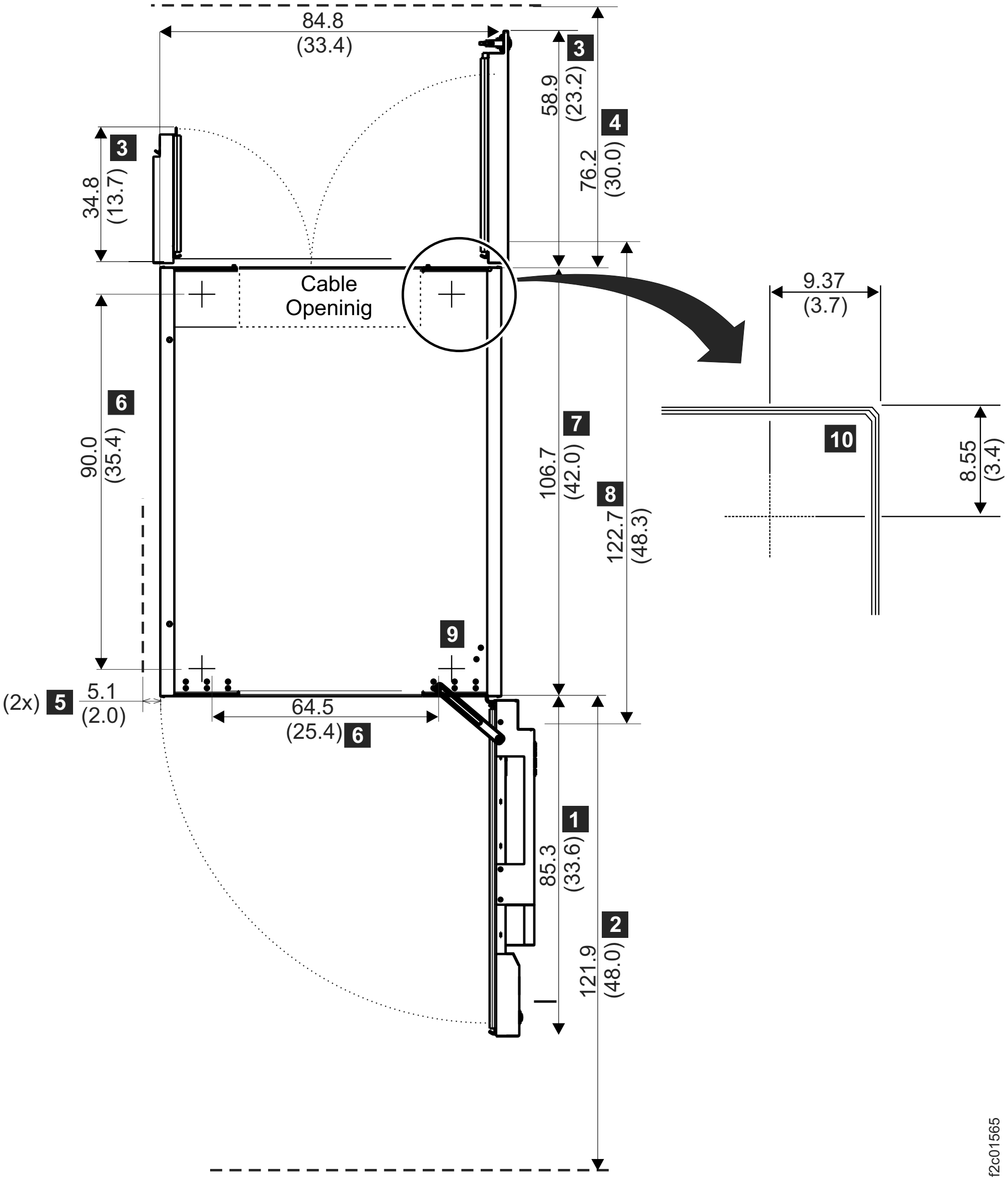


Figure 9. DS8000 physical footprint. Dimensions are in centimeters (inches).

The following dimensions are labeled on Figure 9:

1. Front cover width
2. Front service clearance
3. Back cover widths
4. Back service clearance
5. Clearance to allow front cover to open
6. Distance between casters

7. Depth of frame without covers
8. Depth of frame with covers
9. Minimum dimension between casters and outside edges of frames
10. Distance from the edge to the front of the open cover

Chapter 2. Hardware and features

This chapter helps you understand the hardware components and features available in the DS8000 series.

This chapter contains information about the hardware and the hardware features in your DS8000. It includes hardware topics such as the IBM System Storage Hardware Management Console, the storage complexes, available interfaces, device drivers, and storage disks. It also contains information on the features supported by the DS8000 hardware. Use the information in this chapter to assist you in planning, ordering, and in the management of your DS8000 hardware and its hardware features.

The Table 5 provides an example of some of the feature codes that are used to order features for the IBM System Storage DS8870, across Models 961 and 96E.

Table 5. Sample of feature codes for DS8870

Feature Code	Description	Notes
1051	Battery assembly	If zero EPLD is used, 1 battery assembly feature code is required. If 1 EPLD is used, 2 battery assembly feature codes are required.
1061	Single-phase power cord, 200-240V, 60A, 3-pin connector	HBL360C6W, Pin and Sleeve Connector, IEC 309, 2P3W HBL360R6W, AC Receptacle, IEC 60309, 2P3W
1068	Single-phase power cord, 200-240V, 63A, no connector	Inline Connector: not applicable Receptacle: not applicable
1081	Three-phase power cord, wye, 380V-415V, 32A, no connector	Inline Connector: not applicable Receptacle: not applicable
1082	Three-phase power cord, delta, 200-240V, 60A, 4-pin connector	HBL460C9W, Pin and Sleeve Connector, IEC 309, 3P4W HBL460R9W, AC Receptacle, IEC 60309, 3P4W
1083	Top exit three-phase power cord, wye, 380V-415V, 32A, no connector	Inline Connector: not applicable Receptacle: not applicable
1084	Top exit three-phase power cord, delta, 200-240V, 60A, 4-pin connector	HBL460C9W, Pin and Sleeve Connector, IEC 309, 3P4W HBL460R9W, AC Receptacle, IEC 60309, 3P4W
1731	DS8000 LMC V7.0	Microcode bundle
2999	Disk enclosure filler set	
4311	16 GB processor memory	961 Business Class (2-core)
4312	32 GB processor memory	961 Business Class (2-core)
4313	64 GB processor memory	961 (4-core)

Table 5. Sample of feature codes for DS8870 (continued)

Feature Code	Description	Notes
4314	128 GB processor memory	961 (8-core)
4315	256 GB processor memory	961 (8-core)
4316	512 GB processor memory	961 (16-core)
4317	1 TB processor memory	961 (16-core)
4401	2 Processor indicator	Requires 4311 and 4312
4402	4 Processor indicator	Requires 4313
4403	8 Processor indicator	Requires 4314 and 4315
4404	16 Processor indicator	Requires 4316 and 4317
5108	146 GB 15K FDE drive set	SAS
5308	300 GB 15K FDE drive set	SAS
5708	600 GB 10K FDE drive set	SAS
5758	900 GB 10K FDE drive set	SAS
5858	3 TB 7.2K FDE drive set	SAS
6158	400 GB FDE drive set	SSD
Note: Details for all of the available feature codes can be found throughout this DS8870 Introduction and Planning Guide, within their corresponding sections.		

Storage complexes

A storage complex is a set of storage units that are managed by management console units.

You can associate one or two management console units with a storage complex. Each storage complex must use at least one of the internal management console units in one of the storage units. You can add a second management console for redundancy. The second storage management console can be either one of the internal management console units in a storage unit or an external management console.

Hardware Management Console

The hardware management console (HMC) is the focal point for hardware installation, configuration, and maintenance activities.

The HMC is a dedicated notebook that is physically located (installed) inside your DS8000 storage unit, and can automatically monitor the state of your system, and notify you and IBM when service is required. The DS8000 Storage Manager is accessible from IBM System Storage Productivity Center (SSPC) through the IBM Tivoli Storage Productivity Center GUI. SSPC uses Tivoli Storage Productivity Center Basic Edition, which is the software that drives SSPC and provides the capability to manage storage devices and host resources from a single control point.

In addition to using Tivoli Storage Productivity Center, the GUI can also be accessed from any location that has network access using a web browser. Supported web browsers include:

- Mozilla Firefox 10 ESR.

- Microsoft Internet Explorer 9.

The first HMC in a storage complex is always internal to the 242x machine type, DS8870. To provide continuous availability of your access to the HMC functions, use a second HMC, especially for storage environments that use encryption. For more information, see “Best practices for encrypting storage environments” on page 167.

This second HMC can be provided in two ways:

- **External** (outside the 242x machine type, Model 961). This console is installed in the customer-provided rack. It uses the same hardware as the internal HMC.

  Note: The external HMC should be within 50 feet of the base model.
- **Internal** The internal HMC from each of two separate storage facilities can be "cross-coupled". Plan for this configuration to be accomplished during the initial installation of the two storage facilities to avoid additional power cycling. (Combining two previously installed storage facilities into the cross-coupled configuration at a later date, requires a power cycle of the second storage facility.) Ensure that you maintain the same machine code level for all storage facilities in the cross-coupled configuration.

RAID implementation

RAID implementation improves data storage reliability and performance.

Redundant array of independent disks (RAID) is a method of configuring multiple disk drives in a storage subsystem for high availability and high performance. The collection of two or more disk drives presents the image of a single disk drive to the system. If a single device failure occurs, data can be read or regenerated from the other disk drives in the array.

RAID implementation provides fault-tolerant data storage by storing the data in different places on multiple disk drive modules (DDMs). By placing data on multiple disks, I/O operations can overlap in a balanced way to improve the basic reliability and performance of the attached storage devices.

Physical capacity can be configured as RAID 5, RAID 6 (only on the DS8000 series), RAID 10, or a combination of RAID 5 and RAID 10. RAID 5 can offer excellent performance for most applications, while RAID 10 can offer better performance for selected applications, in particular, high random, write content applications in the open systems environment. RAID 6 increases data protection by adding an extra layer of parity over the RAID 5 implementation.

You can reconfigure RAID 5 disk groups as RAID 10 disk groups or vice versa.

RAID 5 overview

RAID 5 is a method of spreading volume data across multiple disk drives. The DS8000 series supports RAID 5 arrays.

RAID 5 increases performance by supporting concurrent accesses to the multiple DDMs within each logical volume. Data protection is provided by parity, which is stored throughout the drives in the array. If a drive fails, the data on that drive can be restored using all the other drives in the array along with the parity bits that were created when the data was stored.

RAID 6 overview

RAID 6 is a method of increasing the data protection of arrays with volume data spread across multiple disk drives. The DS8000 series supports RAID 6 arrays.

RAID 6 increases data protection by adding an extra layer of parity over the RAID 5 implementation. By adding this protection, RAID 6 can restore data from an array with up to two failed drives. The calculation and storage of extra parity slightly reduces the capacity and performance compared to a RAID 5 array. RAID 6 is suitable for storage using archive class DDMs.

RAID 10 overview

RAID 10 provides high availability by combining features of RAID 0 and RAID 1. The DS8000 series supports RAID 10 arrays.

RAID 0 increases performance by striping volume data across multiple disk drives. RAID 1 provides disk mirroring, which duplicates data between two disk drives. By combining the features of RAID 0 and RAID 1, RAID 10 provides a second optimization for fault tolerance.

RAID 10 implementation provides data mirroring from one DDM to another DDM. RAID 10 stripes data across half of the disk drives in the RAID 10 configuration. The other half of the array mirrors the first set of disk drives. Access to data is preserved if one disk in each mirrored pair remains available. In some cases, RAID 10 offers faster data reads and writes than RAID 5 because it is not required to manage parity. However, with half of the DDMs in the group used for data and the other half used to mirror that data, RAID 10 disk groups have less capacity than RAID 5 disk groups.

DS8000 interfaces

You can use a variety of IBM interfaces to enhance the management of your DS8000 storage unit. These IBM interfaces include DS Storage Manager, the DS Command-line interface (CLI), the DS Open application programming interface, Tivoli Storage Productivity Center, and Tivoli Storage Productivity for Replication Manager.

Note: For DS8000, you can have a maximum of 256 interfaces of any type connected at one time.

System Storage DS® Storage Manager

The DS Storage Manager is an interface that is used to perform logical configurations and Copy Services management functions.

The DS Storage Manager can be accessed through the Tivoli Storage Productivity Center Element Manager from any network-connected workstation with a supported browser. The DS Storage Manager is installed as a GUI for the Windows and Linux operating systems. It can be accessed from any location that has network access using a web browser.

Note: Supported browsers include:

- Mozilla Firefox 10 ESR.
- Microsoft Internet Explorer 9.

Access the GUI from a browser using the IP_address:P_port on your DS8000 HMC.

DS command-line interface

The IBM System Storage DS CLI can be used to create, delete, modify, and view Copy Services functions and the logical configuration of a storage unit. These tasks can be performed either interactively, in batch processes (operating system shell scripts), or in DS CLI script files. A DS CLI script file is a text file that contains one or more DS CLI commands and can be issued as a single command. DS CLI can be used to manage logical configuration, Copy Services configuration, and other functions for a storage unit, including managing security settings, querying point-in-time performance information or status of physical resources, and exporting audit logs.

The DS CLI provides a full-function set of commands to manage logical configurations and Copy Services configurations. The DS CLI can be installed on and is supported in many different environments, including:

- AIX® 5.1, 5.2, 5.3, 6.1
- HP-UX 11.0, 11i, v1, v2, v3

  Note: The DS CLI supports HP-UX 11iv3 only when the Legacy mode is enabled.
- HP Tru64 UNIX version 5.1, 5.1A
- Linux RedHat 3.0 Advanced Server (AS) and Enterprise Server (ES)
- Red Hat Enterprise Linux (RHEL) 4 and RHEL 5
- SuSE 8, SuSE 9, SuSE Linux Enterprise Server (SLES) 8, SLES 9, and SLES 10
- VMware ESX v3.0.1 Console
- Novell NetWare 6.5
- IBM System i® i5/OS® 5.3
- OpenVMS 7.3-1 (or newer)
- Sun Solaris 7, 8, and 9
- Microsoft Windows 2000, Windows Datacenter, Windows 2003, Windows Vista, Windows Server 2008, Windows XP, and Windows 7

DS Open Application Programming Interface

The DS Open Application Programming Interface (API) is a nonproprietary storage management client application that supports routine LUN management activities, such as LUN creation, mapping and masking, and the creation or deletion of RAID 5, RAID 6, and RAID 10 volume spaces.

The DS Open API supports these activities through the use of the Storage Management Initiative Specification (SMI-S), as defined by the Storage Networking Industry Association (SNIA).

The DS Open API helps integrate configuration management support into storage resource management (SRM) applications, which help you to use existing SRM applications and infrastructures. The DS Open API can also be used to automate configuration management through customer-written applications. Either way, the DS Open API presents another option for managing storage units by complementing the use of the IBM System Storage DS Storage Manager Web-based interface and the DS command-line interface.

Note: The DS Open API supports the IBM System Storage DS8000 series and is an embedded component.

You can implement the DS Open API without using a separate middleware application, like the IBM System Storage Common Information Model (CIM) agent, which provides a CIM-compliant interface. The DS Open API uses the CIM technology to manage proprietary devices as open system devices through storage management applications. The DS Open API is used by storage management applications to communicate with a storage unit.

Tivoli Storage Productivity Center

The Tivoli Storage Productivity Center is an integrated software solution that can help you improve and centralize the management of your storage environment through the integration of products. With the Tivoli Storage Productivity Center (TPC), it is possible to manage and fully configure multiple DS8000 storage systems from a single point of control.

Note: System Storage Productivity Center (SSPC) uses Tivoli Storage Productivity Center Basic Edition to manage storage devices.

The DS Storage Manager is installed as a GUI for the Windows and Linux operating systems. In addition to using TPC, it can also be accessed from any location that has network access using a web browser. Supported web browsers include:

- Mozilla Firefox 10 ESR.
- Microsoft Internet Explorer 9.

Tivoli Storage Productivity Center simplifies storage management by providing the following benefits:

- Centralizing the management of heterogeneous storage network resources with IBM storage management software
- Providing greater synergy between storage management software and IBM storage devices
- Reducing the number of servers that are required to manage your software infrastructure
- Migrating from basic device management to storage management applications that provide higher-level functions

With the help of agents, Tivoli Storage Productivity Center discovers the devices to which it is configured. It then can start an element manager that is specific to each discovered device, and gather events and data for reports about storage management.

Tivoli Storage Productivity Center for Replication

Tivoli Storage Productivity Center for Replication facilitates the use and management of Copy Services functions such as the remote mirror and copy functions (Metro Mirror and Global Mirror) and the point-in-time function (FlashCopy).

Tivoli Storage Productivity Center for Replication provides a graphical interface that you can use for configuring and managing Copy Services functions across the

DS8000 and Enterprise Storage Server® (ESS) storage units. These data-copy services maintain consistent copies of data on source volumes that are managed by Replication Manager.

Tivoli Storage Productivity Center for Replication for FlashCopy, Metro Mirror, and Global Mirror support provides automation of administration and configuration of these services, operational control (starting, suspending, resuming), Copy Services tasks, and monitoring and managing of copy sessions.

Tivoli Storage Productivity Center for Replication is an option of the Tivoli Storage Productivity Center for Replication software program. If you are licensed for Copy Services functions, you can use Tivoli Storage Productivity Center for Replication to manage your data copy environment.

Notes:

1. Tivoli Storage Productivity Center for Replication operations can now be performed using the DS8000 hardware management console (HMC).
2. The use of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) are both supported through the HMC ports.

For more information, visit the IBM Publications website using the following web address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp

DS8000 hardware specifics

The DS8000 models offer a high degree of availability and performance through the use of redundant components that can be replaced while the system is operating. You can use the DS8000 models with a mix of different operating systems and clustered and nonclustered variants of the same operating systems.

Contributing to the high degree of availability and reliability are the structure of the DS8000 storage unit, the host systems it supports, and its processor memory and processor speeds.

Storage unit structure

The design of the storage unit, which contains the base model and the expansion models, contributes to the high degree of availability that is associated with the DS8000 series. The primary components that support high availability within the storage unit are the storage server, the processor complex, and the rack power control card.

Storage unit

The storage unit contains a storage server and one or more storage (disk) enclosures that are packaged in one or more racks with associated power supplies, batteries, and cooling.

Storage server

The storage server consists of two processor complexes, two or more I/O enclosures, and a pair of rack power control cards.

Processor complex

A processor complex controls and manages the storage unit to perform the function of the storage server. The two processor complexes form a redundant pair such that if either processor complex fails, the remaining processor complex performs all storage server functions.

Rack power control card

A redundant pair of rack power control (RPC) cards coordinate the power management within the storage unit. The RPC cards are attached to the service processors in each processor complex, the primary power supplies in each rack, and indirectly to the fan/sense cards and storage enclosures in each rack.

All DS8000 models include the IBM System Storage Multi-path Subsystem Device Driver (SDD). The SDD provides load balancing and enhanced data availability capability in configurations with more than one I/O path between the host server and the DS8000 series storage unit. Load balancing can reduce or eliminate I/O bottlenecks that occur when many I/O operations are directed to common devices using the same I/O path. The SDD can eliminate the single point of failure by automatically rerouting I/O operations when a path failure occurs.

Disk drives

The DS8870 provides you with the following choice of disk drives.

DS8870

The following drives are available in a 2.5" form factor.

SAS drive types with Full Disk Encryption (FDE):

- 146 GB, 15K RPM
- 300 GB, 15K RPM
- 600 GB, 10K RPM
- 900 GB, 10K RPM

2.5" SSD:

- 400 GB (FDE)

The following is available in a 3.5" form factor.
SAS drive set:

- 3 TB 7.2K RPM (includes FDE and FDE Standby CoD)

Host attachment overview

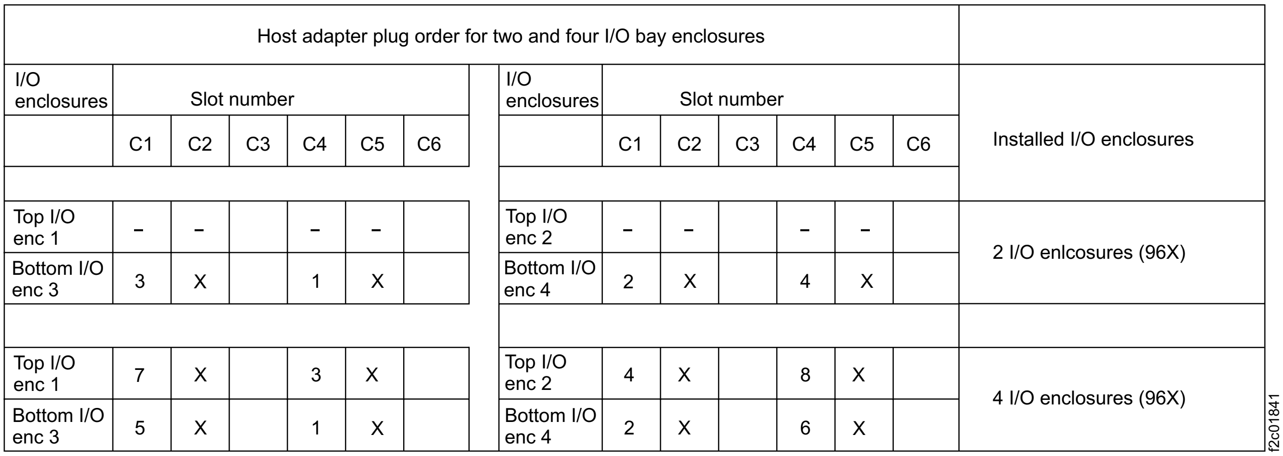
The DS8000 series provides various host attachments so that you can consolidate storage capacity and workloads for open-systems hosts and System z.

The DS8000 series provides extensive connectivity using Fibre Channel adapters across a broad range of server environments.

Host adapter intermix support

Both 4-port and 8-port host adapters (HAs) are available in the DS8870, but like the DS8800, it can use the same 8 Gbps, 4-port HA for improved performance.

Figure 10 on page 27 also shows the adapter plug order for the DS8870 using a 4-port or 8-port HA configuration.



Host adapter plug order for two and four I/O bay enclosures														
I/O enclosures	Slot number						I/O enclosures	Slot number						Installed I/O enclosures
	C1	C2	C3	C4	C5	C6		C1	C2	C3	C4	C5	C6	
Top I/O enc 1	–	–		–	–		Top I/O enc 2	–	–		–	–		2 I/O enlcosures (96X)
Bottom I/O enc 3	3	X		1	X		Bottom I/O enc 4	2	X		4	X		
Top I/O enc 1	7	X		3	X		Top I/O enc 2	4	X		8	X		4 I/O enclosures (96X)
Bottom I/O enc 3	5	X		1	X		Bottom I/O enc 4	2	X		6	X		

Figure 10. Plug order for 4- and 8-port HA slots (8 GB) for two and four DS8870 I/O enclosures

Open-systems host attachment with Fibre Channel adapters

You can attach a DS8000 series to an open-systems host with Fibre Channel adapters.

Fibre Channel is a 2 Gbps, 4 Gbps or 8 Gbps, full-duplex, serial communications technology to interconnect I/O devices and host systems that are separated by tens of kilometers.

The IBM System Storage DS8000 series supports SAN connections of up to 2 Gbps with 2 Gbps host adapters, up to 4 Gbps with 4 Gbps host adapters, and up to 8 Gbps with 8 Gbps host adapters. The DS8000 series negotiates automatically, determining whether it is best to run at a 2 Gbps, 4 Gbps, or 8 Gbps link speed. The IBM System Storage DS8000 series detects and operates at the greatest available link speed that is shared by both sides of the system.

Fibre Channel technology transfers information between the sources and the users of the information. This information can include commands, controls, files, graphics, video, and sound. Fibre Channel connections are established between Fibre Channel ports that reside in I/O devices, host systems, and the network that interconnects them. The network consists of elements like switches, bridges, and repeaters that are used to interconnect the Fibre Channel ports.

FICON attached System z hosts overview

This section describes how you can attach the DS8000 storage unit to FICON attached System z hosts.

Each storage unit Fibre Channel adapter has four ports. Each port has a unique worldwide port name (WWPN). You can configure the port to operate with the FICON upper-layer protocol. For FICON, the Fibre Channel port supports connections to a maximum of 509 FICON hosts. On FICON, the Fibre Channel adapter can operate with fabric or point-to-point topologies.

With Fibre Channel adapters that are configured for FICON, the storage unit provides the following configurations:

- Either fabric or point-to-point topologies
- A maximum of eight 8-port host adapters on the DS8870 Model 961 (4-core), which equates to 64 host adapter ports. With the first expansion model, 96E,

another eight host adapters are available, which equates to an additional 64 ports (a maximum of 128 host adapter ports). Any DS8000 fibre channel I/O port an be configured for either SCSI/PPRC or FICON.

- A maximum of 509 N-Port logins per Fibre Channel port
- A maximum of 8192 process logins (SCSI Initiator to DS8000 port) per storage image over all Fibre Channel ports configured for SCSI/PPRC.
- A maximum of 1280FICON logical paths on each Fibre Channel port configured for FICON
- Access to all 255 control-unit images (8000 CKD devices) over each FICON port
- A maximum of 512 logical paths per control unit image over all Fibre channel ports configured for FICON.

Note: FICON host channels limit the number of devices per channel to 16 384. To fully access 65 280 devices on a storage unit, it is necessary to connect a minimum of four FICON host channels to the storage unit. You can access the devices through a switch to a single storage unit FICON port. With this method, you can expose 64 control-unit images (16 384 devices) to each host channel.

The storage unit supports the following operating systems for System z and S/390 hosts:

- Linux
- Transaction Processing Facility (TPF)
- Virtual Storage Extended/Enterprise Storage Architecture (VSE/ESA)
- z/OS
- z/VM®
- z/VSE®

For the most current information on supported hosts, operating systems, adapters and switches, go to the *System Storage Interoperation Center* (SSIC) website at www.ibm.com/systems/support/storage/config/ssic.

Processor memory

The DS8000 series offers a number of configuration options for processor memory.

DS8870

The DS8870 two-core business class configuration offers up to 32 GB of processor memory.

The business-class feature, Model 961 two-core configuration, offers 16 GB of processor memory with feature code 4311, and a 32 GB processor memory option is available with feature code 4312. 4-core offers 64 GB with feature code 4313, 8-core offers up to 256 GB with feature codes 4314 and 4315, and 16-core offers up to 1 TB with features codes 4316 and 4317.

The nonvolatile storage (NVS) scales with the selected processor memory size, which can also help optimize performance. The NVS is typically 1/32 of the installed memory.

Note: The minimum NVS is 1 GB.

For more information, see “Overview of physical configurations” on page 69.

Subsystem device driver for open-systems

The IBM System Storage Multipath Subsystem Device Driver (SDD) supports open-systems hosts.

The Subsystem Device Driver (SDD) is enclosed in the host server with the native disk device driver for the storage unit. It uses redundant connections between the host server and disk storage in the DS8000 series to provide enhanced performance and data availability.

I/O load balancing

You can maximize the performance of an application by spreading the I/O load across clusters, arrays, and device adapters in the storage unit.

During an attempt to balance the load within the storage unit, placement of application data is the determining factor. The following resources are the most important to balance, roughly in order of importance:

- Activity to the RAID disk groups. Use as many RAID disk groups as possible for the critical applications. Most performance bottlenecks occur because a few disks are overloaded. Spreading an application across multiple RAID disk groups ensures that as many disk drives as possible are available. This is extremely important for open-system environments where cache-hit ratios are usually low.
- Activity to the clusters. When selecting RAID disk groups for a critical application, spread them across separate clusters. Because each cluster has separate memory buses and cache memory, this maximizes the use of those resources.
- Activity to the device adapters. When selecting RAID disk groups within a cluster for a critical application, spread them across separate device adapters.
- Activity to the SCSI or Fibre Channel ports. Use the IBM System Storage Multipath Subsystem Device Driver (SDD) or similar software for other platforms to balance I/O activity across SCSI or Fibre Channel ports.

Note: For information about SDD, see *IBM System Storage Multipath Subsystem Device Driver User's Guide*. This document also describes the product engineering tool, the ESSUTIL tool, which is supported in the pcmpath commands and the datapath commands.

Storage consolidation

When you use a storage unit, you can consolidate data and workloads from different types of independent hosts into a single shared resource.

You might mix production and test servers in an open systems environment or mix open systems, System z and S/390 hosts. In this type of environment, servers rarely, if ever, contend for the same resource.

Although sharing resources in the storage unit has advantages for storage administration and resource sharing, there are additional implications for workload planning. The benefit of sharing is that a larger resource pool (for example, disk drives or cache) is available for critical applications. However, you must ensure that uncontrolled or unpredictable applications do not interfere with critical work. This requires the same kind of workload planning that you use when you mix various types of work on a server.

If your workload is critical, consider isolating it from other workloads. To isolate the workloads, place the data as follows:

- On separate RAID disk groups. Data for open systems, System z or S/390 hosts are automatically placed on separate arrays, which reduces the contention for disk use.
- On separate device adapters.
- In separate storage unit clusters, which isolates use of memory buses, microprocessors, and cache resources. Before you make this decision, verify that the isolation of your data to a single cluster provides adequate data access performance for your application.

Count key data

In count-key-data (CKD) disk data architecture, the data field stores the user data.

Because data records can be variable in length, in CKD they all have an associated count field that indicates the user data record size. The key field enables a hardware search on a key. The commands used in the CKD architecture for managing the data and the storage devices are called channel command words.

Fixed block

In fixed block (FB) architecture, the data (the logical volumes) are mapped over fixed-size blocks or sectors.

With an FB architecture, the location of any block can be calculated to retrieve that block. This architecture uses tracks and cylinders. A physical disk contains multiple blocks per track, and a cylinder is the group of tracks that exists under the disk heads at one point in time without performing a seek operation.

T10 DIF support

American National Standards Institute (ANSI) T10 Data Integrity Field (DIF) standard is supported on System z for SCSI end-to-end data protection on fixed block (FB) LUN volumes. This support applies to the IBM Storage DS8870 unit (models 961 and 96E). System z support applies to FCP channels only.

System z provides added end-to-end data protection between the operating system and the DS8870 unit. This support adds protection information consisting of CRC (Cyclic Redundancy Checking), LBA (Logical Block Address), and host application tags to each sector of FB data on a logical volume.

Data protection using the T10 Data Integrity Field (DIF) on FB volumes includes the following features:

- Ability to convert logical volume formats between standard and protected formats supported through PPRC between standard and protected volumes
- Support for earlier versions of T10-protected volumes on the DS8870 with non T10 DIF-capable hosts
- Allows end-to-end checking at the application level of data stored on FB disks
- Additional metadata stored by the storage facility image (SFI) allows host adapter-level end-to-end checking data to be stored on FB disks independently of whether the host uses the DIF format.

Notes:

- This feature requires changes in the I/O stack to take advantage of all the capabilities the protection offers.
- T10 DIF volumes can be used by any type of Open host with the exception of iSeries, but active protection is supported only for Linux on System z. The protection can only be active if the host server is Linux on System z-enabled.
- T10 DIF volumes can accept SCSI I/O of either T10 DIF or standard type, but if the FB volume type is standard, then only standard SCSI I/O is accepted.

Logical volumes

A logical volume is the storage medium that is associated with a logical disk. It typically resides on two or more hard disk drives.

For the storage unit, the logical volumes are defined at logical configuration time. For count-key-data (CKD) servers, the logical volume size is defined by the device emulation mode and model. For fixed block (FB) hosts, you can define each FB volume (LUN) with a minimum size of a single block (512 bytes) to a maximum size of 2^{32} blocks or 16 TB.

A logical device that has nonremovable media has one and only one associated logical volume. A logical volume is composed of one or more extents. Each extent is associated with a contiguous range of addressable data units on the logical volume.

Allocation, deletion, and modification of volumes

Extent allocation methods (namely, rotate volumes and pool striping) determine the means by which actions are completed on DS8000 volumes.

All extents of the ranks assigned to an extent pool are independently available for allocation to logical volumes. The extents for a LUN or volume are logically ordered, but they do not have to come from one rank and the extents do not have to be contiguous on a rank. This construction method of using fixed extents to form a logical volume in the DS8000 allows flexibility in the management of the logical volumes. You can delete volumes, resize volumes, and reuse the extents of those volumes to create other volumes, different sizes. One logical volume can be deleted without affecting the other logical volumes defined on the same extent pool.

Because the extents are cleaned after you delete a volume, it can take some time until these extents are available for reallocation. The reformatting of the extents is a background process.

There are two extent allocation methods used by the DS8000: rotate volumes and storage pool striping (rotate extents).

Storage pool striping: extent rotation

The default storage allocation method is storage pool striping. The extents of a volume can be striped across several ranks. The DS8000 keeps a sequence of ranks. The first rank in the list is randomly picked at each power on of the storage subsystem. The DS8000 tracks the rank in which the last allocation started. The allocation of a first extent for the next volume starts from the next rank in that sequence. The next extent for that volume is taken from the next rank in sequence, and so on. The system rotates the extents across the ranks.

If you migrate an existing non-striped volume to the same extent pool with a rotate extents allocation method, then the volume is "reorganized." If you add more ranks to an existing extent pool, then the "reorganizing" existing striped volumes spreads them across both existing and new ranks.

You can configure and manage storage pool striping using the DS Storage Manager, DS CLI, and DS Open API. The default of the extent allocation method (EAM) option that is allocated to a logical volume is now rotate extents. The rotate extents option is designed to provide the best performance by striping volume extents across ranks in extent pool.

Managed EAM

Once a volume is managed by Easy Tier, the EAM of the volume is changed to managed EAM, which can result in placement of the extents differing from the rotate volume and rotate extent rules. The EAM only changes when a volume is manually migrated to a non-managed pool.

Rotate volumes allocation method

Extents can be allocated sequentially. In this case, all extents are taken from the same rank until there are enough extents for the requested volume size or the rank is full, in which case the allocation continues with the next rank in the extent pool.

If more than one volume is created in one operation, the allocation for each volume starts in another rank. When allocating several volumes, rotate through the ranks. You might want to consider this allocation method when you prefer to manage performance manually. The workload of one volume is going to one rank. This method makes the identification of performance bottlenecks easier; however, by putting all the volumes data onto just one rank, you might introduce a bottleneck, depending on your actual workload.

LUN calculation

The DS8000 series uses a volume capacity algorithm (calculation) to provide a logical unit number (LUN).

In the DS8000 family, physical storage capacities such as DDMs are expressed in powers of 10. Logical or effective storage capacities (logical volumes, ranks, extent pools) and processor memory capacities are expressed in powers of 2. Both of these conventions are used for logical volume effective storage capacities.

On open volumes with 512 byte blocks (including T10-protected volumes), you can specify an exact block count to create a LUN. You can specify a DS8000 standard LUN size (which is expressed as an exact number of binary GBs (2^30)) or you can specify an ESS volume size (which is expressed in decimal GBs (10^9) accurate to 0.1 GB). The unit of storage allocation unit for open volumes is fixed block one extent. The extent size for open volumes is exactly 1 GB (2^30). Any logical volume that is not an exact multiple of 1 GB does not use all the capacity in the last extent that is allocated to the logical volume. Supported block counts are from 1 to 4 194 304 blocks (2 binary TB) in increments of one block. Supported DS8000 sizes are from 1 to 2048 GB (2 binary TB) in increments of 1 GB. The supported ESS LUN sizes are limited to the exact sizes that are specified from 0.1 to 982.2 GB (decimal) in increments of 0.1 GB and are rounded up to the next larger 32 K byte boundary. The ESS LUN sizes do not result in DS8000 standard LUN sizes. Therefore, they can waste capacity. However, the unused capacity is less than one full extent. ESS LUN sizes are typically used on DS8000 when volumes must be copied between DS8000 and ESS.

On open volumes with 520 byte blocks, you can select one of the supported LUN sizes that are used on System i® processors to create a LUN. The operating system uses 8 of the bytes in each block. This leaves 512 bytes per block for your data. The selected sizes are specified in decimal GB (10^9) or are specified to the exact block count that is shown in Table 6. System i LUNs are defined as protected or unprotected. If the open volume is defined as unprotected, the AS/400® operating system performs software mirroring on the LUN with another non-protected internal or external LUN. If the open volume is defined as protected, the AS/400 operating system does not perform software mirroring on the LUN. The selection of protected or unprotected does not affect the RAID protection that is used by DS8000 on the open volume. In either case, the volume remains protected by RAID.

On CKD volumes, you can specify an exact cylinder count or a DS8000 standard volume size to create a LUN. The DS8000 standard volume size is expressed as an exact number of Mod 1 equivalents (which is 1113 cylinders). The unit of storage allocation for CKD volumes is one CKD extent. The extent size for CKD volume is exactly a Mod 1 equivalent (which is 1113 cylinders). Any logical volume that is not an exact multiple of 1113 cylinders (1 extent) does not use all the capacity in the last extent that is allocated to the logical volume. For CKD volumes that are created with 3380 track formats, the number of cylinders (or extents) is limited to either 2226 (1 extent) or 3339 (2 extents). For CKD volumes that are created with 3390 track formats, you can specify the number of cylinders in the range of 1 - 65520 (x'0001' - x'FFF0') in increments of one cylinder, or as an integral multiple of 1113 cylinders between 65,667 - 262,668 (x'10083' - x'4020C') cylinders (59 - 236 Mod1 equivalents). Alternatively, for 3390 track formats, you can specify Mod 1 equivalents in the range of 1-236.

Note: On IBM i, the supported logical volume sizes for load source units (LSUs) are 17.54 GB, 35.16 GB, 70.56 GB, and 141.1 GB. Logical volume sizes of 8.59 and 282.2 GB are not supported.

Table 6 provides models of storage capacity and disk volumes for System i.

Table 6. Capacity and models of disk volumes for System i

Model Number (Unprotected)	Model Number (Protected)	Capacity	Expected Number of LBAs	OS Version Support
A81	A01	8.59 GB	16 777 216 (0x01000000)	Version 5 Release 2 and Version 5 Release 3
A82	A02	17.55 GB	34 275 328 (0x020B0000)	Version 5 Release 2 and Version 5 Release 3
A85	A05	35.17 GB	68 681 728 (0x04180000)	Version 5 Release 2 and Version 5 Release 3
A84	A04	70.56 GB	137 822 208 (0x08370000)	Version 5 Release 2 and Version 5 Release 3
A86	A06	141.12 GB	275 644 416 (0x106E0000)	Version 5 Release 3 and later

Table 6. Capacity and models of disk volumes for System i (continued)

Model Number (Unprotected)	Model Number (Protected)	Capacity	Expected Number of LBAs	OS Version Support
A87	A07	282.25 GB	551 288 832 (0x20DC0000)	Version 5 Release 3 and later

Extended address volumes for CKD

Count key data (CKD) volumes now support the additional capacity of 1 TB. The 1 TB capacity is an increase in volume size from the previous 223 GB.

This increased volume capacity is referred to as extended address volumes (EAV) and is supported by the 3390 Model A. Use a maximum size volume of up to 1,182,006 cylinders for the IBM zOS. This support is available to you for the z/OS version 12.1, and later.

You can create a 1 TB IBM System z CKD volume on the DS8870.

A System z CKD volume is composed of one or more extents from a CKD extent pool. CKD extents are 1113 cylinders in size. When you define a System z CKD volume, you must specify the number of cylinders that you want for the volume. The DS8000 and the zOS have limits for the CKD EAV sizes. You can define CKD volumes with up to 1,182,006 cylinders, about 1 TB on the DS8870.

If the number of cylinders that you specify is not an exact multiple of 1113 cylinders, then some space in the last allocated extent is wasted. For example, if you define 1114 or 3340 cylinders, 1112 cylinders are wasted. For maximum storage efficiency, consider allocating volumes that are exact multiples of 1113 cylinders. In fact, multiples of 3339 cylinders should be considered for future compatibility. If you want to use the maximum number of cylinders for a volume (that is 1,182,006 cylinders), you are not wasting cylinders, because it is an exact multiple of 1113 (1,182,006 divided by 1113 is exactly 1062). This size is also an even multiple (354) of 3339, a model 3 size.

Quick initialization

The quick initialization function initializes the data logical tracks or blocks within a specified extent range on a logical volume with the appropriate initialization pattern for the host.

Normal read and write access to the logical volume is allowed during the initialization process. Therefore, the extent metadata must be allocated and initialized before the quick initialization function is started. Depending on the operation, the quick initialization can be started for the entire logical volume or for an extent range on the logical volume.

The quick initialization function is started for the following operations:

- Standard logical volume creation
- Standard logical volume expansion
- Standard logical volume reinitialization
- Extent space-efficient (ESE) logical volume expansion
- ESE logical volume reinitialization

- ESE logical volume extent conversion
- Track space-efficient (TSE) or compressed TSE logical volume expansion
- TSE or compressed TSE logical volume reinitialization

Chapter 3. Data management features

The DS8000 storage unit is designed with many management features that allow you to securely process and access your data according to your business needs, even if it is 24 hours a day and 7 days a week.

This chapter contains information about the data management features in your DS8000. Use the information in this chapter to assist you in planning, ordering licenses, and in the management of your DS8000 data management features.

FlashCopy SE feature

The FlashCopy SE feature allocates storage space on an as-needed basis by using space on a target volume only when it actually copies tracks from the source volume to the target volume.

Without track space-efficient (TSE) volumes, the FlashCopy function requires that all the space on a target volume be allocated and available even if no data is copied there. With space-efficient volumes, FlashCopy uses only the number of tracks that are required to write the data that is changed during the lifetime of the FlashCopy relationship, so the allocation of space is on an as-needed basis. Because it does not require a target volume that is the exact size of the source volume, the FlashCopy SE feature increases the potential for a more effective use of system storage capacity.

FlashCopy SE is intended for temporary copies. Unless the source data has little write activity, copy duration does not last longer than 24 hours. The best use of FlashCopy SE is when less than 20% of the source volume is updated over the life of the relationship. Also, if performance on the source or target volumes is important, standard FlashCopy is strongly recommended.

You can define the space-efficiency attribute for the target volumes during the volume creation process. A space-efficient volume can be created from any extent pool that has space-efficient storage already created in it. Both the source and target volumes of any FlashCopy SE relationship must be on the same server cluster.

If the space-efficient source and target volumes have been created and are available, they can be selected when you create the FlashCopy relationship.

Important: Space-efficient volumes are currently supported as FlashCopy target volumes only.

After a space-efficient volume is specified as a FlashCopy target, the FlashCopy relationship becomes space-efficient. FlashCopy works the same way with a space-efficient volume as it does with a fully provisioned volume. All existing copy functions work with a space-efficient volume except for the Background Copy function (not permitted with a space-efficient target) and the Dataset Level FlashCopy function. A miscalculation of the amount of copied data can cause the space-efficient repository to run out of space, and the FlashCopy relationship fails (that is, reads or writes to the target are prevented). You can withdraw the FlashCopy relationship to release the space.

Dynamic volume expansion

The DS8000 series supports dynamic volume expansion.

Dynamic volume expansion increases the capacity of open systems and System z volumes, while the volume remains connected to a host system. This capability simplifies data growth by providing volume expansion without taking volumes offline.

Since some operating systems do not support a change in volume size, a host action is required to detect the change after the volume capacity is increased.

The following maximum volume sizes are supported:

- Open Systems FB volumes - 16 TB
- System z CKD volume types 3390 model 9, and custom is 65520 cylinders
- System z CKD volume type 3390 model 3 is 3339 cylinders
- System z CKD volume types 3390 model A, up to 1,182,006 cylinders

Count key data and fixed block volume deletion prevention

The DS CLI and DS Storage Manager have been enhanced to include a force option that is designed to prevent deleting count key data (CKD) and fixed block (FB) volumes that are in use or online.

If the force option is enabled, the DS8000 checks whether the volumes are online or in use before they are deleted. (For CKD volumes, a volume is online if it is participating in a Copy Services relationship or if it is online to a System z host. For FB volumes, a volume is online if it is participating in a Copy Services relationship or is part of a volume group.) If you specify the force option when you delete a volume, online checking is suppressed and the DS8000 deletes the volume regardless if it is online or in use.

IBM System Storage Easy Tier

Easy Tier is an optional, no charge feature on the DS8870. It offers capabilities such as manual volume capacity rebalance, auto performance rebalancing in both homogenous and hybrid pools, hot spot management, rank depopulation, manual volume migration, and thin provisioning support (ESE volumes only) for Easy Tier features. Easy Tier determines the appropriate tier of storage based on data access requirements and then automatically and nondisruptively moves data, at the subvolume or sub-LUN level, to the appropriate tier on the DS8000.

Use Easy Tier to dynamically move your data to the appropriate drive tier in your system with its automatic performance monitoring algorithms. You can use this feature to increase the efficiency of your SSDs and the efficiency of all the tiers in your DS8000 system.

You can use the features of Easy Tier between three tiers of storage within your system on the DS8870 storage unit.

With the latest Easy Tier you can distribute your entire workload among the ranks in your storage pool using three tiers, more efficiently distributing bandwidth across tiers in addition to IOPS.

You can also use Easy Tier in automatic mode to assist in the management of your ESE thin provisioning on fixed block (FB) volumes.

Easy Tier features help you to effectively manage your system health, storage performance, and storage capacity automatically. Easy Tier uses system configuration and workload analysis with warm demotion to achieve effective overall system health. Simultaneously, data promotion and auto-rebalancing address performance while cold demotion works to address capacity. This maximizes performance while minimizing cost. See "Easy Tier: automatic mode" on page 40 for more information.

An additional feature provides the capability for you to use Easy Tier in manual mode for thin provisioning. Rank depopulation is supported on ranks with ESE volumes allocated (extent space-efficient) or auxiliary volumes. See "Easy Tier: manual mode" on page 44 for more information.

Note: Use Easy Tier in manual mode to depopulate ranks containing TSE auxiliary volumes.

Use the capabilities of Easy Tier to support:

- Three tiers - Using three tiers and efficient algorithms improves system performance and cost effectiveness.
- Cold demotion - Cold data (or extents) stored on a higher-performance tier is demoted to a more appropriate tier. Easy Tier is available with two-tier HDD pools as well as with three-tier pools. Sequential bandwidth is moved to the lower tier to increase the efficient use of your tiers. For more information on cold demote functions, see "Easy Tier: automatic mode" on page 40.
- Warm demotion - Active data that has larger bandwidth is demoted from either tier one (SSD) or tier two (Enterprise) to SAS Enterprise or Nearline SAS. Warm demotion is triggered whenever the higher tier is over its bandwidth capacity. Selected warm extents are demoted to allow the higher tier to operate at its optimal load. Warm demotes do not follow a predetermined schedule. For more information on warm demote functions, see "Easy Tier: automatic mode" on page 40.
- Manual volume or pool rebalance - Volume rebalancing relocates the smallest number of extents of a volume and restripes those extents on all available ranks of the extent pool.
- Auto-rebalancing - Automatically balances the workload of the same storage tier within both the homogeneous and the hybrid pool based on usage to improve system performance and resource use. Use the auto-rebalancing functions of Easy Tier to manage a combination of homogenous and hybrid pools, including relocating hot spots on ranks. With homogenous pools, systems with only one tier can use Easy Tier technology to optimize their RAID array utilization.
- Rank depopulations - Allows ranks that have extents (data) allocated to them to be unassigned from an extent pool by using extent migration to move extents from the specified ranks to other ranks within the pool.
- Thin provisioning - Support for the use of thin provisioning is available on ESE (FB) and standard volumes. The use of TSE volumes (FB and CKD) is not supported.

Easy Tier provides a performance monitoring capability, regardless of whether the Easy Tier license feature is activated. Easy Tier uses the monitoring process to determine what data to move and when to move it when using automatic mode. You can enable monitoring independently (with or without the Easy Tier license feature activated) for information about the behavior and benefits that can be expected if automatic mode were enabled. For more information, see"Volume data monitoring" on page 47.

Data from the monitoring process is included in a summary report that you can download to your Windows system. Use the IBM System Storage DS8000 Storage Tier Advisor Tool application to view the data when you point your browser to that file. For more information, see "IBM System Storage DS8000 Storage Tier Advisor Tool" on page 48.

Prerequisites

The following conditions must be met to enable Easy Tier:

- The Easy Tier license feature is enabled (required for both manual and automatic mode, except when monitoring is set to All Volumes).
- For automatic mode to be active, the following conditions must be met:
  - Easy Tier automatic mode monitoring is set to either All or Auto mode.
  - For Easy Tier to manage pools, the Auto Mode Volumes must be set to either Tiered Pools or All Pools.

Table 7 contains drive combinations you can use with your three-tier configuration, and with the migration of your ESE volumes.

Table 7. Drive combinations to use with three-tiers

Models	Drive combinations: three tiers
DS8870	SSD, SAS Enterprise, Nearline SAS
Notes: 1. Easy Tier features include extendable support in automatic mode for FC (enterprise class) and SATA storage tiers. 2. SATA drives are not available in SAS 2.5" form factor.	

Easy Tier: automatic mode

Use of the automatic mode of Easy Tier requires the Easy Tier license feature.

In Easy Tier, both IOPS and bandwidth algorithms determine when to migrate your data. This process can help you improve performance.

Use automatic mode to have Easy Tier relocate your extents to their most appropriate storage tier in a hybrid pool, based on usage. Because workloads typically concentrate I/O operations (data access) on only a subset of the extents within a volume or LUN, automatic mode identifies the subset of your frequently accessed extents and relocates them to the higher-performance storage tier.

Subvolume or sub-LUN data movement is an important option to consider in volume movement because not all data at the volume or LUN level becomes hot data. For any given workload, there is a distribution of data considered either hot or cold. This can result in significant overhead associated with moving entire volumes between tiers. For example, if a volume is 1 TB, you do not want to move the entire 1 TB volume when the generated heat map indicates that only 10 GB is considered hot. This capability makes use of your higher performance tiers while reducing the number of drives that you need to optimize performance.

Using automatic mode, you can use high performance storage tiers with a much smaller cost. This means that you invest a small portion of storage in the high-performance storage tier. You can use automatic mode for relocation and tuning without the need for your intervention, using automatic mode to help generate cost-savings while optimizing your storage performance.

Three-tier automatic mode is supported with the following Easy Tier functions:

- Support for ESE volumes with the thin provisioning of your FB volumes.
- Support for a matrix of device (DDM) and adapter types
- Monitoring of both bandwidth and IOPS limitations
- Data demotion between tiers
- Automatic mode hot spot rebalancing, which applies to the following auto performance rebalance situations:
  - Redistribution within a tier after a new rank is added into a managed pool
  - Redistribution within a tier after a rank is removed from a managed pool
  - Redistribution when the workload is imbalanced on the ranks within a tier of a managed pool.

To help manage and improve performance, Easy Tier is designed to identify hot data at the subvolume or sub-LUN (extent) level, based on ongoing performance monitoring, and then automatically relocate that data to an appropriate storage device in an extent pool that is managed by Easy Tier. Easy Tier uses an algorithm to assign heat values to each extent in a storage device. These heat values determine on what tier the data would best reside, and migration takes place automatically. Data movement is dynamic and transparent to the host server and to applications using the data.

By default, automatic mode is enabled (through the DS CLI and DS Storage Manager) when the Easy Tier license feature is activated. You can temporarily disable automatic mode.

Easy Tier provides capabilities to support the automatic functions of auto-rebalance, warm demotion, and cold demotion. This includes support for extent pools with three tiers (SSD, SAS Enterprise, or Near-line SAS).

With Easy Tier you can use automatic mode to help you manage the thin provisioning of your ESE FB volumes.

Functions and features of Easy Tier: automatic mode

Rebalance and demotion are functions of Easy Tier in automatic mode.

Auto-rebalance

Rebalance is a function of Easy Tier automatic mode to balance the extents in the same tier based on usage. Auto-rebalance supports single managed pools as well as hybrid pools. You can use the Storage Facility Image (SFI) control to enable or disable the auto-rebalance function on all pools of an SFI. When you enable auto-rebalance, every standard and ESE volume is placed under Easy Tier management for auto-rebalancing procedures. Using auto-rebalance gives you the advantage of these automatic functions:

- Easy Tier operates within a tier, inside a managed storage pool.

- Easy Tier automatically detects performance skew and rebalances extents within the same tier.

In any tier, placing highly active (hot) data on the same physical rank can cause the hot rank or the associated device adapter (DA) to become a performance bottleneck. Likewise, over time skews can appear within a single tier that cannot be addressed by migrating data to a faster tier alone, and require some degree of workload rebalancing within the same tier. Auto-rebalance addresses these issues within a tier in both hybrid and homogenous pools. It also helps the system respond in a more timely and appropriate manner to overloading, skews, and any under-utilization that can occur from the addition or deletion of hardware, migration of extents between tiers, changes in the underlying volume configurations, and variations in the workload. Auto-rebalance adjusts the system to continuously provide optimal performance by balancing the load on the ranks and on DA pairs.

The latest version of Easy Tier provides support for auto-rebalancing within homogenous pools. If you set the Easy Tier Automatic Mode Migration control to Manage All Extent Pools, extent pools with a single-tier can perform intra-tier rank rebalancing. If Easy Tier is turned off, then no volumes are managed. If Easy Tier is on, it manages all the volumes it supports, standard or ESE. TSE volumes are not supported with auto-rebalancing.

Notes:

- Standard and ESE volumes are supported.
- Merging pools are restricted to allow repository auxiliary volumes only in a single pool.
- If Easy Tier's Automatic Mode Migration control is set to Manage All Extent Pools, then single-tier extent pools are also managed to perform intra-tier rank rebalancing.

Warm demotion

Warm demotion operation demotes warm (or mostly sequential-accessed) extents in SSD to HDD, or from Enterprise SAS to NearLine SAS drives to protect the drive performance on the system. The ranks being demoted to are selected randomly. This function is triggered when bandwidth thresholds are exceeded. This means that extents are warm-demoted from one rank to another rank among tiers when extents have high bandwidth but low IOPS.

It is helpful to understand that warm demotion is different from auto-rebalancing. While both warm demotion and auto-rebalancing can be event-based, rebalancing movement takes place within the same tier while warm demotion takes place among more than one tier. Auto-rebalance can initiate when the rank configuration changes. It also performs periodic checking for workload that is not balanced across ranks. Warm demotion initiates when an overloaded rank is detected.

Cold demotion

Cold demotion recognizes and demotes cold or semi-cold extents to an appropriate lower-cost tier. Cold extents are demoted in a storage pool to a lower tier as long as that storage pool is not idle.

Cold demotion occurs when Easy Tier detects any of the following scenarios:

- Extents in a storage pool become inactive over time, while other data remains active. This is the most typical use for cold demotion, where inactive data is demoted to the SATA tier. This action frees up extents on the enterprise tier before the extents on the SATA tier become hot, helping the system be more responsive to new, hot data.
- All the extents in a storage pool become inactive simultaneously due to either a planned or unplanned outage. Disabling cold demotion assists the user in scheduling extended outages or experiencing outages without effecting the extent placement.
- All extents in a storage pool are active. In addition to cold demote using the capacity in the lowest tier, an extent is selected which has close to zero activity, but with high sequential bandwidth and low random IOPS for the demotion. Bandwidth available on the lowest tier is also used.
- All extents in a storage pool become inactive due to a planned non use event, such as an application reaching its end of life. In this situation, cold demotion is disabled and the user may select one of three options:
  - Allocate new volumes in the storage pool and plan on those volumes becoming active. Over time, Easy Tier replaces the inactive extents on the enterprise tier with active extents on the SATA tier.
  - Depopulate all of the enterprise HDD ranks. When all enterprise HDD ranks are depopulated, all extents in the pool are on the SATA HDD ranks. Store the extents on the SATA HDD ranks until they need to be deleted or archived to tape. Once the enterprise HDD ranks are depopulated, move them to a storage pool.
  - Leave the extents in their current locations and reactivate them at a later time.

Figure 11 on page 44 illustrates all of the migration types supported by the latest Easy Tier enhancements in a three-tier configuration. The auto-performance rebalance might also include additional swap operations.

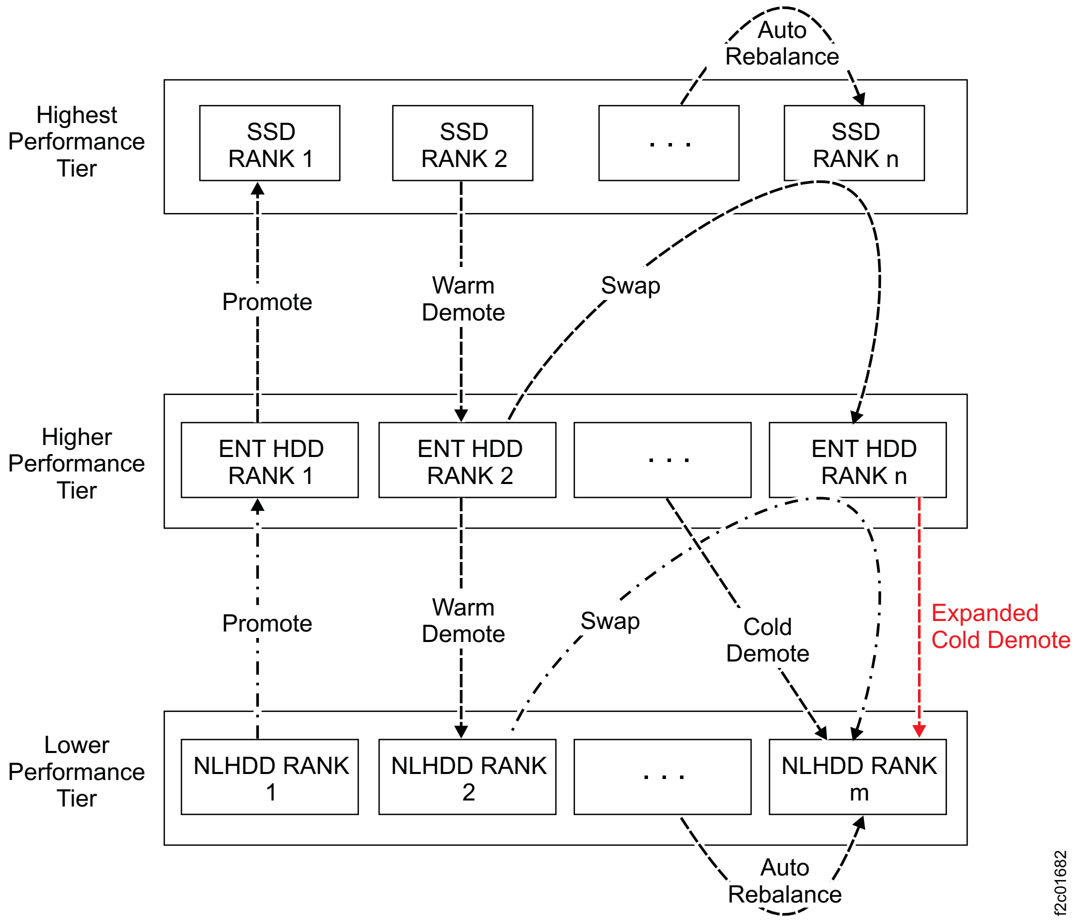


Figure 11. Three-tier migration types and their processes

Easy Tier: manual mode

Easy Tier in manual mode provides the capability to migrate volumes and merge extent pools, under the same DS8870 system, concurrently with I/O operations.

In Easy Tier manual mode, you can dynamically relocate a logical volume between extent pools or within an extent pool to change the extent allocation method of the volume or to redistribute the volume across new ranks that have been added. This capability is referred to as *dynamic volume relocation*. You can also merge two existing pools into one without affecting the data on the logical volumes associated with the extent pools.

Enhanced functions of Easy Tier manual mode offer additional capabilities. You can use manual mode to relocate your extents, or to relocate an entire volume from one pool to another pool. Later, you might also need to change your storage media or configurations. Upgrading to a new disk drive technology, rearranging the storage space, or changing storage distribution within a given workload are typical operations that you can perform with volume relocations. Use manual mode to achieve these operations with minimal performance impact and to increase the options you have in managing your storage.

Functions and features of Easy Tier: manual mode

This section descries the functions and features of Easy Tier in manual mode.

Volume migration

Volume migration for restriping can be achieved by:

- Restriping - Relocating a subset of extents within the volume for volume migrations within the same pool.
- Rebalancing - Redistributing the volume across available ranks. This feature focuses on providing pure striping, without requiring preallocation of all the extents. This means that you can use rebalancing when only a few extents are available.

You can select which logical volumes to migrate, based on performance considerations or storage management concerns. For example, you can:

- Migrate volumes from one extent pool to another. You might want to migrate volumes to a different extent pool that has more suitable performance characteristics, such as different disk drives or RAID ranks. For example, a volume that was configured to stripe data across a single RAID can be changed to stripe data across multiple arrays for better performance. Also, as different RAID configurations become available, you might want to move a logical volume to a different extent pool with different characteristics, which changes the characteristics of your storage. You might also want to redistribute the available disk capacity between extent pools.

  Notes:

  - When you initiate a volume migration, ensure that all ranks are in the configuration state of Normal in the target extent pool.
  - Volume migration is supported for standard and ESE volumes. There is no direct support to migrate auxiliary volumes. However, you can migrate extents of auxiliary volumes as part of ESE migration or rank depopulation.
  - Ensure that you understand your data usage characteristics before you initiate a volume migration.
  - The overhead that is associated with volume migration is comparable to a FlashCopy operation running as a background copy.
- Change the extent allocation method that is assigned to a volume. You can relocate a volume within the same extent pool but with a different extent allocation method. For example, you might want to change the extent allocation method to help spread I/O activity more evenly across ranks. If you configured logical volumes in an extent pool with fewer ranks than now exist in the extent pool, you can use Easy Tier to manually redistribute the volumes across new ranks that have been added.

  Note: If you specify a different extent allocation method for a volume, the new extent allocation method takes effect immediately.

Manual volume rebalance using volume migration

Volume and pool rebalancing are designed to redistribute the extents of volumes within a non managed pool. This means skew is less likely to occur on the ranks.

Notes:

- Manual rebalancing is not allowed in hybrid or managed pools.
- Manual rebalancing is allowed in homogeneous pools.
- You cannot mix fixed block (FB) and count key data (CKD) drives.

Volume rebalance can be achieved by initiating a manual volume migration. Use volume migration to achieve manual rebalance when a rank is added to a pool, or when a large volume with rotate volumes EAM is deleted. Manual rebalance is often referred to as capacity rebalance because it balances the distribution of extents without factoring in extent usage. When a volume migration is targeted to the same pool and the target EAM is rotate extent, the volume migration acts internally as a volume rebalance.

Use volume rebalance to relocate the smallest number of extents of a volume and restripe the extents of that volume on all available ranks of the pool where it is located. The behavior of volume migration, which differs from volume rebalance, continues to operate as it did in the previous version of Easy Tier.

Notes: Use the latest enhancements to Easy Tier to:

- Migrate ESE logical volumes
- Perform pool rebalancing by submitting a volume migration for every standard and ESE volume in a pool
- Merge extent pools with virtual rank auxiliary volumes in both the source and destination extent pool

Extent pools

You can manually combine two existing extent pools with homogeneous or hybrid disks into a single extent pool with SSD drives to use auto mode. However, when merged pools are managed by Easy Tier, extents from SSD, SAS Enterprise, and Nearline SAS are managed as a three-tier storage hierarchy.

An extent pool with any mix of SSD, SAS Enterprise, and Nearline SAS drive classes are managed by Easy Tier in automatic mode, for situations in which:

- There are three tiers composed of SSD, SAS Enterprise or Nearline SAS in a DS8870.

Rank depopulation

Easy Tier provides an enhanced method of rank depopulation, which can be used to replace old drive technology, reconfigure pools and tear down hybrid pools. This method increases efficiency and performance when replacing or relocating whole ranks. Use the latest enhancements to Easy Tier to perform rank depopulation on any ranks in the various volume types (ESE logical, virtual rank auxiliary, TSE repository auxiliary, SE repository auxiliary, and non SE repository auxiliary).

Use rank depopulation to concurrently stop using one or more ranks in a pool. You can use rank depopulation to perform any of the following functions:

- Swap out old drive technology
- Reconfigure pools
- Tear down hybrid pools
- Change RAID types

Note: Rank depopulation is supported on ranks that have extent space efficient (ESE) extents.

Volume data monitoring

The IBM Storage Tier Advisory Tool collects and reports volume data. It provides performance monitoring data even if the license feature is not activated.

The monitoring capability of the DS8000 enables it to monitor the usage of storage at the volume extent level. Monitoring statistics are gathered and analyzed every 24 hours. In an Easy Tier managed extent pool, the analysis is used to form an extent relocation plan for the extent pool, which provides a recommendation, based on your current plan, for relocating extents on a volume to the most appropriate storage device. The results of this data are summarized in a report that you can download. For more information, see “IBM System Storage DS8000 Storage Tier Advisor Tool” on page 48.

Table 8 describes monitor settings and mirrors the monitor settings in the DS CLI and DS Storage Manager.

Table 8. DS CLI and DS Storage Manager settings for monitoring

	Easy Tier license feature	
Monitor Setting	**Not installed**	**Installed**
All Volumes	All volumes are monitored.	All volumes are monitored.
Auto Mode Volumes	No volumes are monitored.	Volumes in extent pools managed by Easy Tier are monitored.
No Volumes	No volumes are monitored.	No volumes are monitored.

The default monitoring setting for Easy Tier **Auto Mode** is On. Volumes in managed extent pools are monitored when the Easy Tier license feature is activated. Volumes are not monitored if the Easy Tier license feature is not activated.

You can determine whether volumes are monitored and also disable the monitoring process temporarily, using either the DS CLI or DS Storage Manager.

Migration process management

You can initiate volume migrations and pause, resume, or cancel a migration process that is in progress.

Volumes that are eligible for migration are dependent on the state and access of the volumes. Table 9 shows the states required to allow migration with Easy Tier.

Table 9. Volume states required for migration with Easy Tier

Volume state	**Is migration allowed with Easy Tier?**
Access state	
Online	Yes
Fenced	No
Data state	
Normal	Yes
Pinned	No

Table 9. Volume states required for migration with Easy Tier (continued)

Volume state	Is migration allowed with Easy Tier?
Read only	Yes
Inaccessible	No
Indeterminate data loss	No
Extent fault	No

Initiating volume migration

With Easy Tier, you can migrate volumes from one extent pool to another. The time to complete the migration process might vary, depending on what I/O operations are occurring on your storage unit.

If an error is detected during the migration process, the storage facility image (SFI) retries the extent migration after a short time. If an extent cannot be successfully migrated, the migration is stopped, and the configuration state of the logical volume is set to migration error.

Pausing and resuming migration

You can pause volumes that were in the process of being migrated. You can also resume the migration process on the volumes that were paused.

Canceling migration

You can cancel the migration of logical volumes that were in the process of being migrated. The volume migration process pre-allocates all extents for the logical volume when you initiate a volume migration. All pre-allocated extents on the logical volume that have not migrated are released when you cancel a volume migration. The state of the logical volumes changes to migration-canceled and the target extent pool that you specify on a subsequent volume migration is limited to either the source extent pool or target extent pool of the original volume migration.

Note: If you initiate a volume migration but the migration was queued and not in progress, then the cancel process returns the volume to normal state and not migration-canceled.

IBM System Storage DS8000 Storage Tier Advisor Tool

The DS8000 offers a reporting tool called IBM System Storage DS8000 Storage Tier Advisor Tool.

The Storage Tier Advisor Tool is a Windows application that provides a graphical representation of performance data that is collected by Easy Tier over a 24-hour operational cycle. It is the application that allows you to view the data when you point your browser to the file. The Storage Tier Advisor Tool supports the enhancements provided with Easy Tier, including support for SSD, SAS Enterprise, and Nearline SAS for DS8870 and the auto performance rebalance feature. Download the Storage Tier Advisor Tool for the DS8870 at the Customer Download Files Storage Tier Advisor Tool FTP page.

To extract the summary performance data generated by the Storage Tier Advisor Tool, you can use either the DS CLI or DS Storage Manager. When you extract summary data, two files are provided, one for each server in the storage facility image (SFI server). The download operation initiates a long running task to collect performance data from both selected storage facility images. This information can be provided to IBM if performance analysis or problem determination is required.

You can view information to analyze workload statistics and evaluate which logical volumes might be candidates for Easy Tier management. If you have not installed and enabled the Easy Tier feature, you can use the performance statistics gathered by the monitoring process to help you determine whether to use Easy Tier to enable potential performance improvements in your storage environment.

Easy Tier considerations and limitations

When planning for volume migration, it is important to consider how Easy Tier functions with storage configurations, and recognize its limitations.

Migration considerations

The following information might be helpful in using Easy Tier with the DS8000:

- You cannot initiate a volume migration on a volume that is in the process of being migrated. The first migration must complete first.
- You cannot initiate, pause, resume, or cancel migration on selected volumes that are aliases or virtual volumes.
- You cannot migrate volumes from one extent pool to another or change the extent allocation method unless the Easy Tier feature is installed on the DS8000.
- There are likely to be a limited number of SSD arrays due to their cost. If there are volumes that require static extent allocations on SSD arrays, one or more homogeneous extent pools must be configured with one or more SSD ranks. If there are volumes that require Easy Tier automatic mode, one or more heterogeneous extent pools must be configured with one or more SSD ranks. There is no way to share SSD ranks between storage pools. Therefore, a hybrid pool and a non-hybrid pool cannot share space on an SSD rank.
- Volume migration is supported for standard, auxiliary, and ESE volumes.
- If you specify a different extent allocation method for a volume, the new extent allocation method takes effect immediately.
- A volume that is being migrated cannot be expanded and a volume that is being expanded cannot be migrated.
- When a volume is migrated out of an extent pool that is managed with Easy Tier, or when Easy Tier is no longer installed, the DS8870 disables Easy Tier and no longer automatically relocates high activity I/O data on that volume between storage devices.

Limitations

The following limitations apply to the use of Easy Tier for DS8870:

- TSE logical volumes do not support extent migration. This means these entities do not support Easy Tier manual mode or Easy Tier automatic mode.
- You cannot merge two extent pools:
  - If both extent pools contain TSE volumes.
  - If there are TSE volumes on the SSD ranks.
  - If you have selected an extent pool that contains volumes that are being migrated.
- It might be helpful to know that some basic characteristics of Easy Tier might limit the applicability for your generalized workloads. The granularity of the

extent that can be relocated within the hierarchy is large (1 GB). Additionally, the time period over which the monitoring is analyzed is continuous, and long (24 hours). Therefore, some workloads may have hot spots, but when considered over the range of the relocation size, they will not appear, on average, to be hot. Also, some workloads may have hot spots for short periods of time, but when considered over the duration of Easy Tier's analysis window, the hot spots will not appear, on average, to be hot.

Performance for System z

The DS8000 series supports the following IBM performance enhancements for System z environments.

- Parallel access volumes (PAVs)
- Multiple allegiance
- z/OS Distributed Data Backup
- z/HPF extended distance capability

Parallel access volumes

A PAV capability represents a significant performance improvement by the storage unit over traditional I/O processing. With PAVs, your system can access a single volume from a single host with multiple concurrent requests.

You must configure both your storage unit and operating system to use PAVs. You can use the logical configuration definition to define PAV-bases, PAV-aliases, and their relationship in the storage unit hardware. This unit address relationship creates a single logical volume, allowing concurrent I/O operations.

Static PAV associates the PAV-base address and its PAV aliases in a predefined and fixed method. That is, the PAV-aliases of a PAV-base address remain unchanged. Dynamic PAV, on the other hand, dynamically associates the PAV-base address and its PAV aliases. The device number types (PAV-alias or PAV-base) must match the unit address types as defined in the storage unit hardware.

You can further enhance PAV by adding the IBM HyperPAV feature. IBM HyperPAV associates the volumes with either an alias address or a specified base logical volume number. When a host system requests IBM HyperPAV processing and the processing is enabled, aliases on the logical subsystem are placed in an IBM HyperPAV alias access state on all logical paths with a given path group ID. IBM HyperPAV is only supported on FICON channel paths.

PAV can improve the performance of large volumes. You get better performance with one base and two aliases on a 3390 Model 9 than from three 3390 Model 3 volumes with no PAV support. With one base, it also reduces storage management costs that are associated with maintaining large numbers of volumes. The alias provides an alternate path to the base device. For example, a 3380 or a 3390 with one alias has only one device to write to, but can use two paths.

The storage unit supports concurrent or parallel data transfer operations to or from the same volume from the same system or system image for System z or S/390 hosts. PAV software support enables multiple users and jobs to simultaneously access a logical volume. Read and write operations can be accessed simultaneously to different domains. (The domain of an I/O operation is the specified extents to which the I/O operation applies.)

Multiple allegiance

With multiple allegiance, the storage unit can execute concurrent, multiple requests from multiple hosts.

Traditionally, IBM storage subsystems allow only one channel program to be active to a disk volume at a time. This means that, once the subsystem accepts an I/O request for a particular unit address, this unit address appears "busy" to subsequent I/O requests. This single allegiance capability ensures that additional requesting channel programs cannot alter data that is already being accessed.

By contrast, the storage unit is capable of multiple allegiance (or the concurrent execution of multiple requests from multiple hosts). That is, the storage unit can queue and concurrently execute multiple requests for the same unit address, if no extent conflict occurs. A conflict refers to either the inclusion of a Reserve request by a channel program or a Write request to an extent that is in use.

z/OS Distributed Data Backup

z/OS Distributed Data Backup (zDDB) is an optional licensed feature that allows hosts, attached through a FICON or ESCON interface, to access data on fixed block (FB) volumes through a device address on FICON or ESCON interfaces.

If the zDDB LIC feature key is installed and enabled and a volume group type specifies either FICON or ESCON interfaces, this volume group has implicit access to all FB logical volumes that are configured in addition to all CKD volumes specified in the volume group. In addition, this optional feature enables data backup of open systems from distributed server platforms through a System z host. The feature helps you manage multiple data protection environments and consolidate those into one environment managed by System z. For more information, see "z/OS Distributed Data Backup" on page 107.

z/HPF extended distance

z/HPF extended distance reduces the impact associated with supported commands on current adapter hardware, improving FICON throughput on the DS8000 I/O ports. The DS8000 also supports the new zHPF I/O commands for multitrack I/O operations.

Copy Services

Copy Services functions can help you implement storage solutions to keep your business running 24 hours a day, 7 days a week. Copy Services include a set of disaster recovery, data migration, and data duplication functions.

The DS8000 series supports Copy Service functions that contribute to the protection of your data. These functions are also supported on the IBM TotalStorage Enterprise Storage Server.

Notes:

- If you are creating paths between an older release of the DS8000 (Release 5.1 or earlier), which supports only 4-port host adaptors, and a newer release of the DS8000 (Release 6.0 or later), which supports 8-port host adaptors, the paths should connect only to the lower four ports on the newer storage unit.

- The maximum number of FlashCopy relationships allowed on a volume is 65534. If that number is exceeded, the FlashCopy operation fails.
- The size limit for volumes or extents in a Copy Service relationship is 2 TB.
- Thin provisioning functions in open-system environments are supported for the following Copy Services functions:
  - FlashCopy relationships
  - Global Mirror relationships provided that the Global Copy A and B volumes are Extent Space Efficient (ESE) volumes. The FlashCopy target volume (Volume C) in the Global Mirror relationship can be a ESE volume, Target Space Efficient (TSE) volume, or standard volume.
- PPRC supports any intermix of T10-protected or standard volumes. FlashCopy does not support intermix.

The following Copy Services functions are available as optional features:

- Point-in-time copy, which includes IBM System Storage FlashCopy and Space-Efficient FlashCopy

  The FlashCopy function enables you to make point-in-time, full volume copies of data, so that the copies are immediately available for read or write access. In System z environments, you can also use the FlashCopy function to perform data set level copies of your data.
- Remote mirror and copy, which includes the following functions:
  - IBM System Storage Metro Mirror (previously known as Synchronous PPRC)

    Metro Mirror provides real-time mirroring of logical volumes between two DS8000 storage units that can be located up to 300 km from each other. It is a synchronous copy solution where write operations are completed on both copies (local and remote site) before they are considered to be done.
  - IBM System Storage Global Copy (previously known as PPRC Extended Distance)

    Global Copy is a nonsynchronous long-distance copy function where incremental updates are sent from the local to the remote site on a periodic basis.
  - IBM System Storage Global Mirror (previously known as Asynchronous PPRC)

    Global Mirror is a long-distance remote copy function across two sites using asynchronous technology. Global Mirror processing is designed to provide support for virtually unlimited distance between the local and remote sites, with the distance typically limited only by the capabilities of the network and the channel extension technology.
  - IBM System Storage Metro/Global Mirror (a combination of Metro Mirror and Global Mirror)

    Metro/Global Mirror is a three-site remote copy solution, which uses synchronous replication to mirror data between a local site and an intermediate site, and asynchronous replication to mirror data from an intermediate site to a remote site.
- Remote mirror and copy for System z environments, which includes z/OS Global Mirror

Note: When Flashcopy is used on FB (open) volumes, the source and the target volumes must have the same protection type of either T10 DIF or standard.

The point-in-time and remote mirror and copy features are supported across various IBM server environments such as IBM i, System p®, and System z, as well as servers from Sun and Hewlett-Packard.

You can manage these functions through a command-line interface called the DS CLI and a Web-based interface called the DS Storage Manager. The DS Storage Manager allows you to set up and manage the following types of data-copy functions from any point where network access is available:

Point-in-time copy (FlashCopy)

The FlashCopy function enables you to make point-in-time, full volume copies of data, with the copies immediately available for read or write access. In System z environments, you can also use the FlashCopy function to perform data set level copies of your data. You can use the copy with standard backup tools that are available in your environment to create backup copies on tape.

FlashCopy is an optional function. To use it, you must purchase one of the point-in-time 242x indicator feature and 239x function authorization features.

The FlashCopy function creates a copy of a source volume on the target volume. This copy is called a point-in-time copy. When you initiate a FlashCopy operation, a FlashCopy relationship is created between a source volume and target volume. A FlashCopy relationship is a *mapping* of the FlashCopy source volume and a FlashCopy target volume. This mapping allows a point-in-time copy of that source volume to be copied to the associated target volume. The FlashCopy relationship exists between this volume pair from the time that you initiate a FlashCopy operation until the storage unit copies all data from the source volume to the target volume or you delete the FlashCopy relationship, if it is a persistent FlashCopy.

One of the main benefits of the FlashCopy function is that the point-in-time copy is immediately available for creating a backup of production data. The target volume is available for read and write processing so it can be used for testing or backup purposes. Data is physically copied from the source volume to the target volume using a background process. (A FlashCopy operation without a background copy is also possible, which allows only data that is modified on the source to be copied to the target volume.) The amount of time that it takes to complete the background copy depends on the following criteria:

- The amount of data being copied
- The number of background copy processes that are occurring
- The other activities that are occurring on the storage units

The FlashCopy function supports the following copy options:

Consistency groups

Creates a consistent point-in-time copy of multiple volumes, with negligible host impact. You can enable FlashCopy consistency groups from the DS CLI.

Change recording

Activates the change recording function on the volume pair that is participating in a FlashCopy relationship. This enables a subsequent refresh to the target volume.

Establish FlashCopy on existing Metro Mirror source

Allows you to establish a FlashCopy relationship where the target volume is also the source of an existing remote mirror and copy source volume. This enables you to create full or incremental point-in-time copies at a local site and then use remote mirroring commands to copy the data to the remote site.

Fast reverse
Reverses the FlashCopy relationship without waiting for the finish of the background copy of the previous FlashCopy. This option applies to the Global Mirror mode.

Inhibit writes to target
Ensures that write operations are inhibited on the target volume until a refresh FlashCopy operation is complete.

Multiple Relationship FlashCopy
Allows a source volume to have multiple (up to 12) target volumes at the same time.

Persistent FlashCopy
Allows the FlashCopy relationship to remain even after the FlashCopy operation completes. You must explicitly delete the relationship.

Refresh target volume
Provides the ability to refresh a FlashCopy relationship, without recopying all tracks from the source volume to the target volume.

Resynchronizing FlashCopy volume pairs
Provides the ability to update an initial point-in-time copy of a source volume without having to recopy your entire volume.

Reverse restore
Reverses the FlashCopy relationship and copies data from the target volume to the source volume.

Remote Pair FlashCopy

Figure 12 on page 55 illustrates how Remote Pair FlashCopy works. If Remote Pair FlashCopy is used to copy data from Local A to Local B, an equivalent operation is also performed from Remote A to Remote B. FlashCopy can be performed as described for a Full Volume FlashCopy, Incremental FlashCopy, and Dataset Level FlashCopy.

The Remote Pair FlashCopy function prevents the Metro Mirror relationship from changing states and the resulting momentary period where Remote A is out of synchronization with Remote B. This feature provides a solution for data replication, data migration, remote copy, and disaster recovery tasks.

Without Remote Pair FlashCopy, when you established a FlashCopy relationship from Local A to Local B, using a Metro Mirror primary volume as the target of that FlashCopy relationship, the corresponding Metro Mirror volume pair went from "full duplex" state to "duplex pending" state as long as the FlashCopy data was being transferred to the Local B. The time it took to complete the copy of the FlashCopy data, until all Metro Mirror volumes were synchronous again, depended on the amount of data being transferred. During this time, the Local B would be inconsistent if a disaster were to have occurred.

Note: Previously, if you created a FlashCopy relationship with the "Preserve Mirror, Required" option, using a Metro Mirror primary volume as the target of that FlashCopy relationship, and if the status of the Metro Mirror volume pair was not in a "full duplex" state, the FlashCopy relationship failed. That restriction is now removed. The Remote Pair FlashCopy relationship will complete successfully with the "Preserve Mirror, Required" option, even if the status of the Metro Mirror volume pair is either in a suspended or duplex pending state.

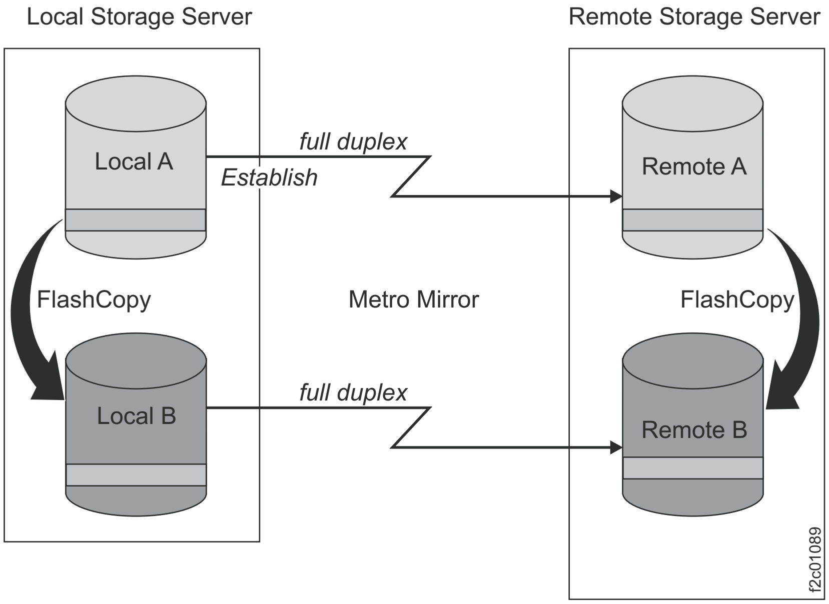


Figure 12. Remote Pair FlashCopy

Remote mirror and copy

The remote mirror and copy feature is a flexible data mirroring technology that allows replication between a source volume and a target volume on one or two disk storage units. You can also issue remote mirror and copy operations to a group of source volumes on one logical subsystem (LSS) and a group of target volumes on another LSS. (An LSS is a logical grouping of up to 256 logical volumes for which the volumes must have the same disk format, either count key data or fixed block.)

Remote mirror and copy is an optional feature that provides data backup and disaster recovery. To use it, you must purchase at least one of the remote mirror and copy 242x indicator feature and 239x function authorization features.

The remote mirror and copy feature provides synchronous (Metro Mirror) and asynchronous (Global Copy) data mirroring. The main difference is that the Global Copy feature can operate at very long distances, even continental distances, with minimal impact on applications. Distance is limited only by the network and channel extenders technology capabilities. The maximum supported distance for Metro Mirror is 300 km.

With Metro Mirror, application write performance is dependent on the available bandwidth. Global Copy allows you to better use your available bandwidth capacity, therefore allowing you to include more of your data to be protected.

The enhancement to Global Copy is Global Mirror, which uses Global Copy and the benefits of FlashCopy to form consistency groups. (A consistency group is a set of volumes that contain consistent and current data to provide a true data backup at a remote site.) Global Mirror uses a master storage unit (along with optional subordinate storage units) to internally, without external automation software, manage data consistency across volumes using consistency groups.

Consistency groups can also be created using the freeze and run functions of Metro Mirror. The freeze and run functions, when used with external automation software, provide data consistency for multiple Metro Mirror volume pairs.

The following sections describe the remote mirror and copy functions.

Synchronous mirroring (Metro Mirror)

Provides real-time mirroring of logical volumes (a source and a target) between two storage units that can be located up to 300 km from each other. With Metro Mirror copying, the source and target volumes can be on the same storage unit or on separate storage units. You can locate the storage unit at another site, some distance away.

Metro Mirror is a synchronous copy feature where write operations are completed on both copies (local and remote site) before they are considered to be complete. Synchronous mirroring means that a storage server constantly updates a secondary copy of a volume to match changes made to a source volume.

The advantage of synchronous mirroring is that there is minimal host impact for performing the copy. The disadvantage is that since the copy operation is synchronous, there can be an impact to application performance because the application I/O operation is not acknowledged as complete until the write to the target volume is also complete. The longer the distance between primary and secondary storage units, the greater this impact to application I/O, and therefore, application performance.

Asynchronous mirroring (Global Copy)

Copies data nonsynchronously and over longer distances than is possible with the Metro Mirror feature. When operating in Global Copy mode, the source volume sends a periodic, incremental copy of updated tracks to the target volume instead of a constant stream of updates. This causes less impact to application writes for source volumes and less demand for bandwidth resources, while allowing a more flexible use of the available bandwidth.

The updates are tracked and periodically copied to the target volumes. As a consequence, there is no guarantee that data is transferred in the same sequence that was applied to the source volume. To get a consistent copy of your data at your remote site, you must periodically switch from Global Copy to Metro Mirror mode, then either stop the application I/O or freeze data to the source volumes using a manual process with freeze and run commands. The freeze and run functions can be used with external automation software such as Geographically Dispersed Parallel Sysplex™ (GDPS®), which is available for System z environments, to ensure data consistency to multiple Metro Mirror volume pairs in a specified logical subsystem.

Common options for Metro Mirror and Global Copy include the following modes:

Suspend and resume

If you schedule a planned outage to perform maintenance at your remote site, you can suspend Metro Mirror or Global Copy processing on specific volume pairs during the duration of the outage. During this time, data is no longer copied to the target volumes. Because the primary storage unit keeps track of all changed data on the source volume, you can resume operations at a later time to synchronize the data between the volumes.

Copy out-of-synchronous data

You can specify that only data that was updated on the source volume while the volume pair was suspended be copied to its associated target volume.

Copy an entire volume or not copy the volume

You can copy an entire source volume to its associated target volume to guarantee that the source and target volume contain the same data. When you establish volume pairs and choose not to copy a volume, a relationship is established between the volumes but no data is sent from the source volume to the target volume. In this case, it is assumed that the volumes contain exactly the same data and are consistent, so copying the entire volume is not necessary or required. Only new updates are copied from the source to target volumes.

Global Mirror

Provides a long-distance remote copy across two sites using asynchronous technology. Global Mirror processing is most often associated with disaster recovery or disaster recovery testing. However, it can also be used for everyday processing and data migration.

The Global Mirror function mirrors data between volume pairs of two storage units over greater distances without affecting overall performance. It also provides application-consistent data at a recovery (or remote) site in case of a disaster at the local site. By creating a set of remote volumes every few seconds, the data at the remote site is maintained to be a point-in-time consistent copy of the data at the local site.

Global Mirror operations periodically invoke point-in-time FlashCopy operations at the recovery site, at regular intervals, without disrupting the I/O to the source volume, thus giving a continuous, near up-to-date data backup. By grouping many volumes into a session, which is managed by the master storage unit, you can copy multiple volumes to the recovery site simultaneously while maintaining point-in-time consistency across those volumes. (A session contains a group of source volumes that are mirrored asynchronously to provide a consistent copy of data at the remote site. Sessions are associated with Global Mirror relationships and are defined with an identifier [session ID] that is unique across the enterprise. The ID identifies the group of volumes in a session that are related and that can participate in the Global Mirror consistency group.)

Global Mirror has been enhanced to support up to 32 Global Mirror sessions per storage facility image. Previously, only one session was supported per storage facility image.

Multiple Global Mirror sessions allow you to failover only data that is assigned to one host or application instead of forcing you to failover all data if one host or application fails. This provides increased flexibility to control the scope of a failover operation and to assign different options and attributes to each session.

The DS CLI and DS Storage Manager have been enhanced to display information about the sessions, including the copy state of the sessions.

Metro/Global Mirror

Provides a three-site, long distance disaster recovery replication that combines Metro Mirror with Global Mirror replication for both System z and open systems data. Metro/Global Mirror uses synchronous replication to mirror data between a local site and an intermediate site, and asynchronous replication to mirror data from an intermediate site to a remote site.

In a three-site, Metro/Global Mirror, should an outage occur, a backup site is maintained regardless of which one of the sites is lost. Suppose an outage occurs at the local site, Global Mirror continues to mirror updates between the intermediate and remote sites, maintaining the recovery capability at the remote site. If an outage occurs at the intermediate site, data at the local storage unit is not affected. If an outage occurs at the remote site, data at the local and intermediate sites is not affected. Applications continue to run normally in either case.

With the incremental resynchronization function enabled on a Metro/Global Mirror configuration, should the intermediate site be lost, the local and remote sites can be connected, and only a subset of changed data is copied between the volumes at the two sites. This reduces the amount of data that needs to be copied from the local site to the remote site and the time it takes to do the copy.

z/OS Global Mirror

In the event of workload peaks, which might temporarily overload the bandwidth of the Global Mirror configuration, the enhanced z/OS Global Mirror function initiates a Global Mirror suspension that preserves primary site application performance. If you are installing new high-performance z/OS Global Mirror primary storage subsystems, this function provides improved capacity and application performance during heavy write activity. This enhancement can also allow Global Mirror to be configured to tolerate longer periods of communication loss with the primary storage subsystems. This enables the Global Mirror to stay active despite transient channel path recovery events. In addition, this enhancement can provide fail-safe protection against application system impact related to unexpected data mover system events.

The z/OS Global Mirror function is an optional function. To use it, you must purchase the remote mirror for z/OS 242x indicator feature and 239x function authorization feature.

z/OS Metro/Global Mirror Incremental Resync

z/OS Metro/Global Mirror Incremental Resync is an enhancement for z/OS Metro/Global Mirror. z/OS Metro/Global Mirror Incremental Resync can eliminate the need for a full copy after a HyperSwap® situation in 3-site z/OS Metro/Global Mirror configurations. The DS8000 series supports z/OS Metro/Global Mirror which is a 3-site mirroring solution that utilizes IBM System Storage Metro Mirror and z/OS Global Mirror (XRC). The z/OS Metro/Global Mirror Incremental Resync capability is intended to enhance this solution by enabling resynchronization of data between sites using only the changed data from the Metro Mirror target to the z/OS Global Mirror target after a GDPS HyperSwap.

z/OS Global Mirror Multiple Reader (enhanced readers)

z/OS Global Mirror Multiple Reader provides multiple Storage Device Manager readers allowing improved throughput for remote mirroring configurations in System z environments. z/OS Global Mirror Multiple Reader helps maintain constant data consistency between mirrored sites and promotes efficient recovery. This function is supported on the DS8000 series running in a System z environment with version 1.7 or later at no additional charge.

Interoperability with existing and previous generations of the DS8000 series

All of the remote mirroring solutions documented in the sections above use Fibre Channel as the communications link between the primary and secondary storage units. The Fibre Channel ports used for remote mirror and copy can be configured as either a dedicated remote mirror link or as a shared port between remote mirroring and Fibre Channel Protocol (FCP) data traffic.

The remote mirror and copy solutions are optional capabilities of the DS8800 Model 951 and are compatible with previous generations of DS8000. They are available as follows:

- Metro Mirror indicator feature numbers 75xx and 0744 and corresponding DS8000 series function authorization (2396-LFA MM feature numbers 75xx)
- Global Mirror indicator feature numbers 75xx and 0746 and corresponding DS8000 series function authorization (2396-LFA GM feature numbers 75xx).

The DS8000 series systems can also participate in Global Copy solutions with the IBM TotalStorage ESS Model 750, IBM TotalStorage ESS Model 800, and IBM System Storage DS6000™ series systems for data migration. For more information on data migration and migration services, contact IBM or a Business Partner representative.

Global Copy is a non-synchronous long distance copy option for data migration and backup, and is available under Metro Mirror and Global Mirror licenses or Remote Mirror and Copy license on older DS8000, ESS, or DS6000 systems.

Disaster recovery using Copy Services

One of the main reasons for using Copy Services functions is to prepare for a possible disaster by backing up, copying, and mirroring your data both at the local (production) and remote sites.

Having a disaster recovery plan can ensure that critical data is recoverable at the time of a disaster. Because most disasters are unplanned, your disaster recovery plan must provide a way that allows you to recover your applications quickly, and more importantly, to access your data. Consistent data to the same point-in-time across all storage units is vital before you can recover your data at a backup (normally your remote) site.

Most users use a combination of remote mirror and copy and point-in-time copy (FlashCopy) features to form a comprehensive enterprise solution for disaster recovery. In an event of a planned event or unplanned disaster, you can use failover and failback modes as part of your recovery solution. Failover and failback modes help to reduce the time that is required to synchronize remote mirror and copy volumes after you switch between the local (or production) and the intermediate or remote sites during planned and unplanned outages. Although failover transmits no data, it changes the status of a device, and the status of the secondary volume changes to a suspended primary volume. The Failback command transmits data and can go in either direction depending on which device the Failback command is issued to.

Recovery procedures that include failover and failback modes use remote mirror and copy functions, such as Metro Mirror, Global Copy, Global Mirror, Metro/Global Mirror, and FlashCopy.

Note: See the *IBM System Storage DS8000 Command-Line Interface User's Guide* for specific disaster recovery tasks.

Data consistency can be achieved using the following methods:

Manually using external software (without Global Mirror)

If you use Metro Mirror, Global Copy, and FlashCopy functions to create a consistent and restartable copy at your recovery site, you must do a manual and periodic suspend operation at your local site. This means using *freeze and run* commands together with external automated software and then using the FlashCopy function to make a consistent copy of your target volume for backup or recovery purposes. (Automation software is not provided with the storage unit; it must be supplied by the user.)

Note: Freezing of the data is done at the same point-in-time across all links and all storage units.

Automatically (with Global Mirror and FlashCopy)

If you use a two-site Global Mirror or a three-site Metro/Global Mirror configuration, the process to create a consistent and restartable copy at your intermediate or remote site is done using an automated process, with minimal or no interruption to your applications. Global Mirror operations automate the process of continually forming consistency groups. It combines Global Copy and FlashCopy operations to provide consistent data at the remote site. A master storage unit (along with subordinate storage units) internally manages data consistency using consistency groups within a Global Mirror configuration. Consistency groups can be created many times per hour to increase the currency of data that is captured in the consistency groups at the remote site.

Note: A consistency group is a collection of volumes (grouped in a session) across multiple storage units that are managed together in a session during the creation of consistent copies of data. The formation of these consistency groups is coordinated by the master storage unit, which sends commands over remote mirror and copy links to its subordinate storage units.

In a two-site Global Mirror configuration, if you have a disaster at your local site and have to start production at your remote site, you can use the consistent point-in-time data from the consistency group at your remote site to recover when the local site is operational.

In a three-site Metro/Global Mirror configuration, if you have a disaster at your local site and you must start production at either your intermediate or remote site, you can use the consistent point-in-time data from the consistency group at your remote site to recover when the local site is operational.

Resource groups for Copy Services scope limiting

Resource groups are used to define a collection of resources and associate a set of policies relative to how the resources are configured and managed. You can define a network user account so that it has authority to manage a specific set of resources groups.

Copy Services scope limiting overview

Copy services scope limiting is the ability to specify policy-based limitations on Copy Services requests. With the combination of policy-based limitations and other inherent volume-addressing limitations, you can control which volumes can be in a Copy Services relationship, which network users or host LPARs issue Copy Services requests on which resources, and other Copy Services operations.

Use these capabilities to separate and protect volumes in a Copy Services relationship from each other. This can assist you with multi-tenancy support by assigning specific resources to specific tenants, limiting Copy Services relationships so that they exist only between resources within each tenant's scope of resources, and limiting a tenant's Copy Services operators to an "operator only" role.

When managing a single-tenant installation, the partitioning capability of resource groups can be used to isolate various subsets of an environment as if they were separate tenants. For example, to separate mainframes from distributed system servers, Windows from UNIX, or accounting departments from telemarketing.

Using resource groups to limit Copy Service operations

Figure 13 on page 62 illustrates one possible implementation of an exemplary environment that uses resource groups to limit Copy Services operations. Figure 13 on page 62 shows two tenants (Client A and Client B) that are concurrently operating on shared hosts and storage systems.

Each tenant has its own assigned LPARs on these hosts and its own assigned volumes on the storage systems. For example, a user cannot copy a Client A volume to a Client B volume.

Resource groups are configured to ensure that one tenant cannot cause any Copy Services relationships to be initiated between its volumes and the volumes of another tenant. These controls must be set by an administrator as part of the configuration of the user accounts or access settings for the storage unit.

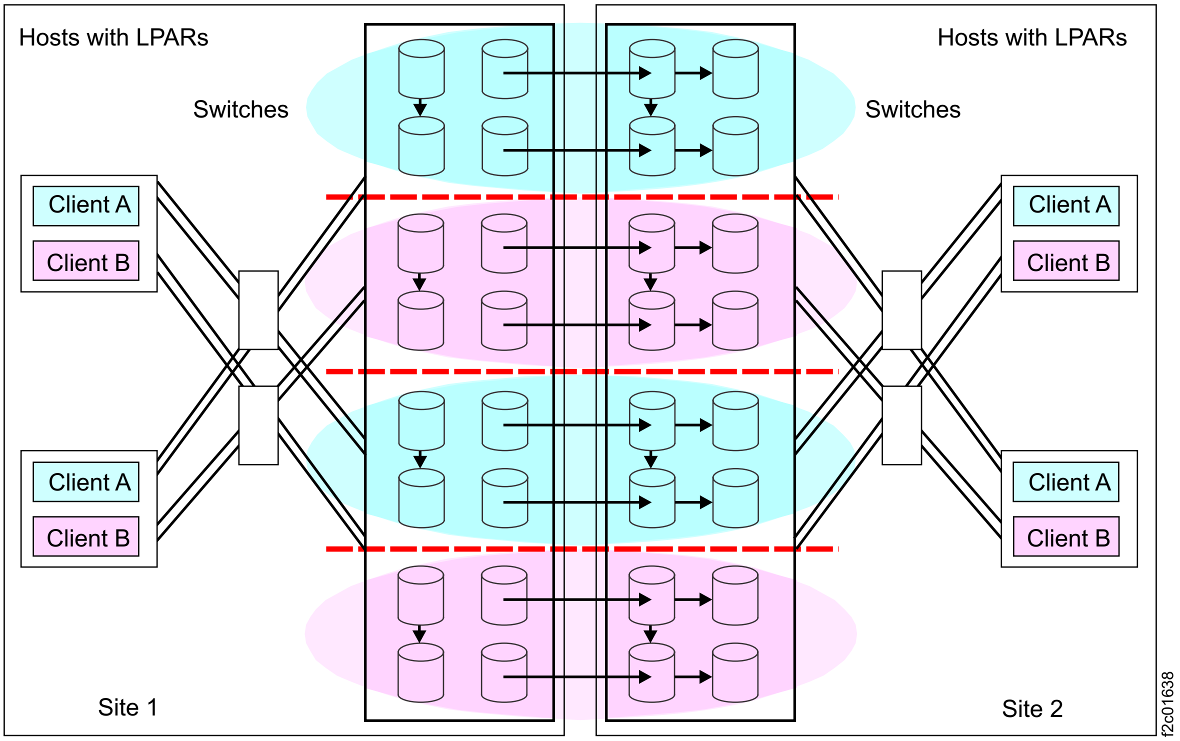


Figure 13. Implementation of multiple-client volume administration

Resource groups functions provide additional policy-based limitations to DS8000 users, which in conjunction with the inherent volume addressing limitations support secure partitioning of Copy Services resources between user-defined partitions. The process of specifying the appropriate limitations is performed by an administrator using resource groups functions.

Note: User and administrator roles for resource groups are the same user and administrator roles used for accessing the DS8000. For example, those roles include storage administrator, Copy Services operator, and physical operator.

The process of planning and designing the use of resource groups for Copy Services scope limiting can be complex. For more information on the rules and policies that must be considered in implementing resource groups, visit the IBM System Storage DS8000 Information Center, and select **Overview** > **Resource Groups** to display topics which provide more detail. For specific DS CLI commands used to implement resource groups, see the *IBM System Storage DS8000 Command-Line Interface User's Guide*.

Comparison of licensed functions

A key decision that you must make in planning for a disaster is deciding which licensed functions to use to best suit your environment.

Table 10 on page 63 provides a brief summary of the characteristics of the Copy Services features that are available for the storage unit.

Table 10. Comparison of licensed functions

Licensed function	Description	Advantages	Considerations
Metro/Global Mirror	Three-site, long distance disaster recovery replication	A backup site is maintained regardless of which one of the sites is lost.	Recovery point objective (RPO) might grow if bandwidth capability is exceeded.
Metro Mirror	Synchronous data copy at a distance	No data loss, rapid recovery time for distances up to 300 km.	Slight performance impact.
Global Copy	Continuous copy without data consistency	Nearly unlimited distance, suitable for data migration, only limited by network and channel extenders capabilities.	Copy is normally fuzzy but can be made consistent through synchronization.
Global Mirror	Asynchronous copy	Nearly unlimited distance, scalable, and low RPO. The RPO is the time needed to recover from a disaster; that is, the total system downtime.	RPO might grow when link bandwidth capability is exceeded.
z/OS Global Mirror	Asynchronous copy controlled by System z host software	Nearly unlimited distance, highly scalable, and very low RPO.	Additional host server hardware and software is required. The RPO might grow if bandwidth capability is exceeded or host performance might be impacted.

Logical configuration overview

Before you configure your DS8000, it is important to understand IBM terminology for storage concepts and the storage hierarchy.

In the storage hierarchy, you begin with a physical disk. Logical groupings of eight disks form an array site. Logical groupings of one array site form an array. After you define your array storage type as CKD or fixed block, you can create a rank. A rank is divided into a number of fixed-size extents. If you work with an open-systems host, an extent is 1 GB. If you work in an IBM System z environment, an extent is the size of an IBM 3390 Mod 1 disk drive.

After you create ranks, your physical storage can be considered virtualized. Virtualization dissociates your physical storage configuration from your logical configuration, so that volume sizes are no longer constrained by the physical size of your arrays.

The available space on each rank is divided into extents. The extents are the building blocks of the logical volumes. An extent is striped across all disks of an array.

Extents of the same storage type are grouped together to form an extent pool. Multiple extent pools can create storage classes that provide greater flexibility in storage allocation through a combination of RAID types, DDM size, DDM speed, and DDM technology. This allows a differentiation of logical volumes by assigning them to the appropriate extent pool for the needed characteristics. Different extent sizes for the same device type (for example, count-key-data or fixed block) can be supported on the same storage unit, but these different extent types must be in different extent pools.

A logical volume is composed of one or more extents. A volume group specifies a set of logical volumes. By identifying different volume groups for different uses or functions (for example, SCSI target, FICON/ESCON control unit, remote mirror and copy secondary volumes, FlashCopy targets, and Copy Services), access to the set of logical volumes that are identified by the volume group can be controlled. Volume groups map hosts to volumes. Figure 14 on page 65 shows a graphic representation of the logical configuration sequence.

When volumes are created, you must initialize logical tracks from the host before the host is allowed read and write access to the logical tracks on the volumes. With the Quick Initialization feature for open system on CKD TSE and FB ESE or TSE volumes, an internal volume initialization process allows quicker access to logical volumes that are used as host volumes and source volumes in Copy Services relationships, such as FlashCopy or Remote Mirror and Copy relationships. This process dynamically initializes logical volumes when they are created or expanded, allowing them to be configured and placed online more quickly.

You can now specify LUN ID numbers through the graphical user interface (GUI) for volumes in a map-type volume group. Do this when you create a new volume group, add volumes to an existing volume group, or add a volume group to a new or existing host. Previously, gaps or holes in LUN ID numbers could result in a "map error" status. The Status field is eliminated from the Volume Groups main page in the GUI and the Volume Groups accessed table on the Manage Host Connections page. You can also assign host connection nicknames and host port nicknames. Host connection nicknames can be up to 28 characters, which is expanded from the previous maximum of 12. Host port nicknames can be 32 characters, which is expanded from the previous maximum of 16.

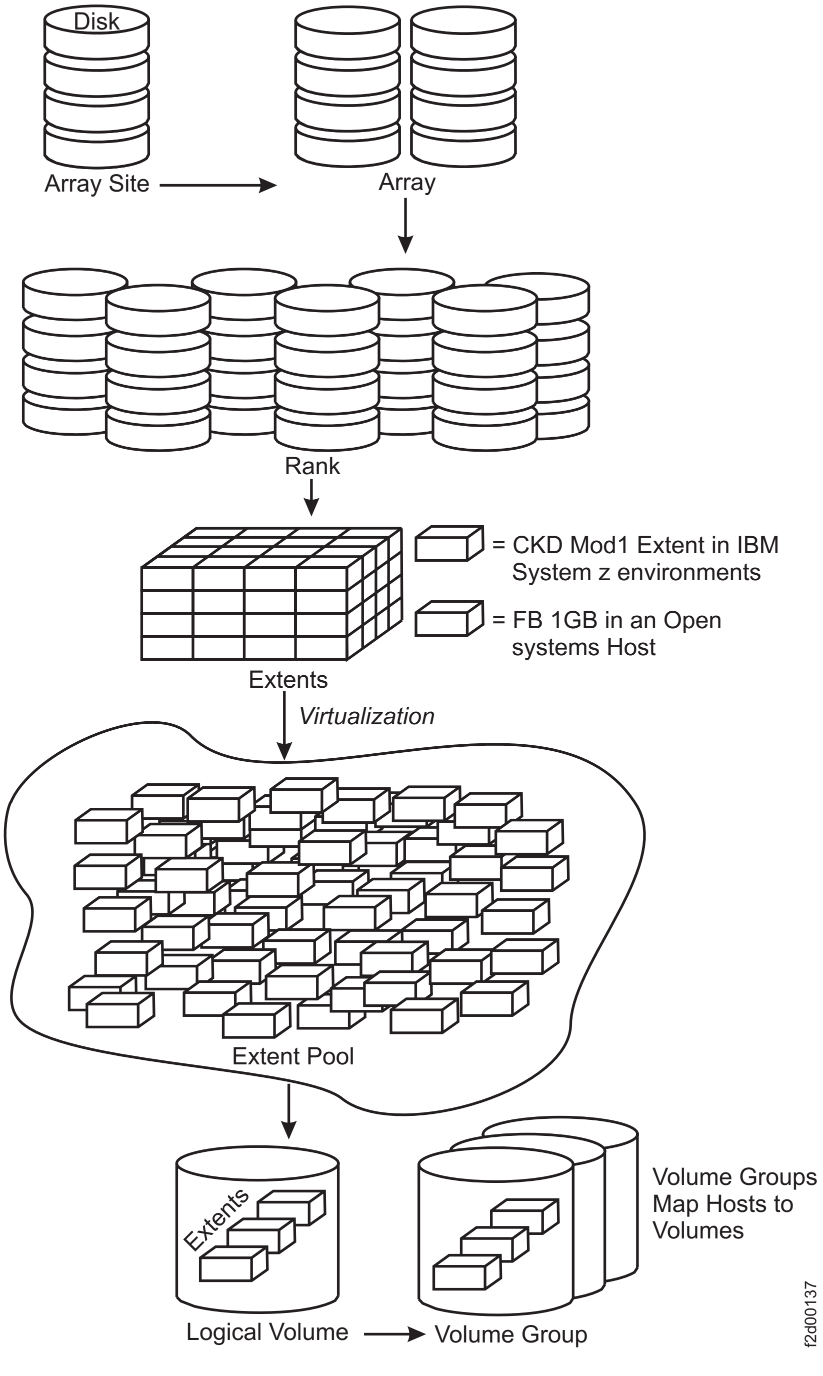

Disk
Array Site
Array
Rank
= CKD Mod1 Extent in IBM System z environments
= FB 1GB in an Open systems Host
Extents
Virtualization
Extent Pool
Extents
Logical Volume
Volume Group
Volume Groups Map Hosts to Volumes
f2d00137

Figure 14. Logical configuration sequence

The storage management software can be used in real-time mode. When you are connected to storage devices over your network, you can use the Real-time Manager to manage your hardware or configure your storage.

I/O Priority Manager

The performance group attribute associates the logical volume with a performance group object. Each performance group has an associated performance policy which determines how the I/O Priority Manager processes I/O operations for the logical volume.

Note: The default setting for this feature is "disabled" and must be enabled for use.

The I/O Priority Manager maintains statistics for the set of logical volumes in each performance group that can be queried. If management is performed for the performance policy, the I/O Priority Manager controls the I/O operations of all managed performance groups to achieve the goals of the associated performance policies. The performance group defaults to 0 if not specified. Table 11 lists performance groups that are predefined and have the associated performance policies:

Table 11. Performance groups and policies

Performance group	Performance policy	Performance policy description
0	0	No management
1-5	1	Fixed block high priority
6-10	2	Fixed block medium priority
11-15	3	Fixed block low priority
16-18	0	No management
19	19	CKD high priority 1
20	20	CKD high priority 2
21	21	CKD high priority 3
22	22	CKD medium priority 1
23	23	CKD medium priority 2
24	24	CKD medium priority 3
25	25	CKD medium priority 4
26	26	CKD low priority 1
27	27	CKD low priority 2
28	28	CKD low priority 3
29	29	CKD low priority 4
30	30	CKD low priority 5
31	31	CKD low priority 6
Note: Performance group settings can be managed using DS CLI or the DS Storage Manager.		

Encryption

The DS8000 series supports data encryption through the use of the IBM Full Disk Encryption (FDE) feature and IBM Tivoli Key Lifecycle Manager.

Encryption technology has a number of considerations that are critical to understand to maintain the security and accessibility of encrypted data. For example, encryption must be enabled by feature code and configured to protect data in your environment. It is not automatic because FDE drives are present. For a list of FDE drives, see “Disk drives” on page 26. For more information, see "Appendix B. Encryption."

Virtual private network

A virtual private network (VPN) is a private network that securely connects corporate networks across the Internet to remote offices and users.

A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. A VPN provides user authentication, data encryption, and data integrity to ensure the security of the data while in transit across private networks and the Internet.

VPNs securely convey information across the Internet by connecting remote users, branch offices, and business partners into an extended corporate network. Many companies are replacing their existing telecommunications infrastructure with VPNs, by implementing secure IP tunnels across the Internet between corporate sites as well as to business partners and remote users.

Because security is a critical issue for companies worldwide, VPN connections provide a secure infrastructure that require systems to work together to mitigate the risk of malicious activity from both external and internal sources. Any connection from your network to the public Internet raises some of the following security concerns:

- Infection by viruses
- Intrusion by hackers
- Accessibility of your data from a remote support site
- Authorization of remote users to access your machine when a remote connection is opened

IBM VPN connections, along with the security features that are built into the DS8000 storage unit, make it possible to access IBM service representatives who can assist you in resolving complex problems without the risks that are associated with a connection to an external network. For information about the IBM VPN implementation including technical details, go to the www.ibm.com/support/docview.wss?uid=ssg1S1002693.

In addition, your IBM representative can inform you about other remote connectivity options, including modem-less operation of the DS8000.

Chapter 4. Planning the physical configuration

This chapter helps you plan the physical configuration of your DS8000 storage unit.

Physical configuration planning is your responsibility. Your disk marketing specialist can help you plan and select the DS8000 physical configuration and features.

This chapter includes the following information:

- Explanations of each feature that you can order to complete the physical configuration for each DS8000 model you order.
- Feature codes to use when you order each feature.
- Configuration rules and guidelines

Overview of physical configurations

When you order your DS8000 models, you can use the DS8000 feature codes to customize the physical configuration of your model.

You must follow established configuration rules to create a valid configuration—not just for the model itself, but also for the storage unit of which the model is a part. A storage unit can consist of a stand-alone base model or it can contain the base model plus expansion models.

Table 12 provides the storage unit configuration ranges for the DS8870 base model.

Table 12. Storage unit configuration values

Description	DS8870 (2-core) business class[1, 2]	DS8870 (4-core)	DS8870 (8-core) [3]	DS8870 (16-core)
Processor memory (min)	16 GB	64 GB	128 GB	512 GB
Processor memory (max)	32 GB	64 GB	256 GB	1024 GB
NVS	0.512	1	2-4	8-16
8 Gbps host adapter; 8 port	2–4	2–8	2–16	2–16
8 Gbps host adapter; 4 port	2–4	2–8	2–16	2–16
Device adapters pairs	1–2	1–4	1–8	1–8
Storage capacity 2.5" drives Storage capacity 3.5" drives	2.3–129 TB 24 - 216 TB	2.3–216 TB 24 - 360 TB	2.3 - 1.4 PB 24 - 2.3 PB	2.3 - 1.4 PB 24 - 2.3 PB

Notes:

1. The DS8870 supports a three-phase and single-phase power configuration.
2. The DS8870 (2-core) business class does not support SSDs.
3. A DS8870 8-core configuration with 128 GB memory can only support up to a second expansion frame.

Configuration controls

DS8000 models ship with indicator features that control the physical configuration at the storage unit level.

These indicator features are for administrative use only. They help ensure that each storage unit (the base model plus any expansion models) has a valid configuration. There is no charge for these features.

DS8000 models can include the following indicators:

- **Expansion model position indicators**

  Expansion model position indicators flag base models that have attached expansion models. They also flag the position of each expansion model within the storage unit. For example, a position 1 indicator flags the expansion model as the first expansion model within the storage unit.
- **Standby CoD indicators**

  Each base model contains a Standby CoD indicator that indicates whether the storage unit takes advantage of the Standby Capacity on Demand (Standby CoD) offering.
- **Other indicators**

  If applicable, models also include other indicators. These include operating system indicators, which indicate that the model is for use in a particular IBM eServer or Linux environment.

Determining physical configuration features

You must consider several guidelines for determining and then ordering the features that you require to customize your storage unit. Determine the feature codes for the optional features you select and use those to complete your configuration.

1. Calculate your overall storage needs. Consider the licensed functions, such as FlashCopy and Remote Mirror and Copy functions, that you must use to ensure continuous data availability and to implement the necessary disaster recover recovery requirements set by your management.

   Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.
2. Determine the DS8000 models of which your storage unit is to be comprised. Consider both base and expansion models.
3. Determine the management console configuration that supports the storage unit using the following steps:
   a. Order one internal management console for each storage unit. The internal management console feature code must be ordered for the base model within the storage unit.
   b. Decide whether an external management console is to be installed for the storage unit. Adding an external management console helps to ensure that you maintain a highly available environment.
4. For each base and expansion model, determine the disk storage features that you need.
   a. Select the disk drive set feature codes and determine the amount of each feature code that you must order for each model.

   b. Select the disk enclosure feature codes and determine the amount that you must order to enclose the disk drive sets that you are ordering.
   c. Select the disk cable feature codes and determine the amount that you need of each.
5. Determine the I/O adapter features that you need for your storage unit.
   a. Select the device and host adapters feature codes to order and choose a model to contain the adapters. Remember that all base models can contain adapters, but only the first attached expansion model can contain adapters.
   b. For each model chosen to contain adapters, determine the number of each I/O enclosure feature codes that you must order.
   c. Select the cables that you require to support the adapters.
6. Based on the disk storage and adapters that the base model and expansion models support, determine the appropriate processor memory feature code that is needed by each base model.
7. Decide which power features that you must order to support each model.
8. Review the other optional features and determine which feature codes to order.

Management console features

Management consoles are required features for your storage unit configuration.

Customize your management consoles by specifying the following different features:

- An external management console as well as the required internal management console
- Management console external line cords

Internal and external management consoles

The management console is the focal point for configuration, Copy Services functions, remote support, and maintenance of DS8000 storage units.

The hardware management console (HMC) is a dedicated appliance that is physically located inside your storage unit and it can proactively monitor the state of your system, notifying you and IBM when service is required. It also can be connected to your network for centralized management of your system using the IBM System Storage DS Command Line Interface (CLI) or storage management software through the IBM System Storage DS Open API. (The DS Storage Manager cannot be launched from the HMC.)

You can also use the DS CLI to control the access of your service and support personnel to the HMC remotely.

An external management console is available as an optional feature and as a redundant management console for environments with high-availability requirements. If you use Copy Services, a redundant management console configuration is especially important.

The internal management console is included with every primary base model and is mounted in a pull-out tray for convenience and security. The external management console must be installed in an external 19-inch system rack. This rack can be an IBM rack or a non-IBM rack. The rack must conform to the required specifications. When you order an external management console, the hardware that you require to install the management console into the rack is included with it.

Tip: To ensure that your IBM service representative can quickly and easily access an external management console, place the external management console rack within 15.2 m (50 ft) of the storage units that are connected to it.

Notes:

1. To help preserve console function, the external and the internal management console units are unavailable as a general-purpose computing resource.
2. The external management console satisfies all applicable requirements of Section 508 of the Rehabilitation Act, as long as assistive technology properly inter-operates with it.

Feature codes for internal and external management consoles

Use the management console feature codes to order up to two management consoles for each storage unit.

Table 13 lists the management console feature codes.

Table 13. Management console feature codes

Feature Code	Description	Comments
1120	Management Console - laptop internal	To be installed in an internal IBM rack. (Model 961
1130	Management Console - laptop external	To be installed in an external IBM or a non-IBM rack. (Model 961).

Management console external power cord

If using an external management console, you must select an external power cord that is specific to your country, voltage, and amperage needs.

The power cord supplies external power to the external management console.

Feature codes for management console external power cords

Use the management console external power cord feature codes to specify a power cord when using an external management console.

Table 14 lists the external power cord feature codes.

Table 14. Management console external power cord feature codes

Feature Code	Description (V = volts, A = amperes)	Country or region
1170	MC power cord standard rack	All
1171	MC power cord group 1	United States, Canada, Bahamas, Barbados, Bermuda, Bolivia, Brazil, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Jamaica, Japan, Japan (PDS), Mexico, Netherlands Antilles, Panama, Philippines, Saudi Arabia, Suriname, Taiwan, Trinidad, Venezuela
1172	MC power cord group 2 (250 V, 15 A)	Brazil

Configuration rules for management consoles

The management console is a dedicated appliance located in your storage unit that can proactively monitor the state of your system. You must order an internal management console each time you order a base model.

You can also order a second management console for the storage unit. The second management console must be an external management console.

You must specify one keyboard feature with each management console that you order. Keyboard features specify the language and whether the keyboard is installed on an internal or external management console.

When you order an internal or external management console, the necessary Ethernet cables that attach it to the storage unit are included.

Storage features

You must select the storage features that you want on your DS8000 storage units.

The storage features are separated into the following categories:

- Disk drive set features and disk enclosure features
- Standby Capacity on Demand features
- Disk enclosure filler features
- Device adapter features
- Disk drive cable features

Disk drives and disk enclosures

Disk drives and disk enclosures are required parts of your DS8000 storage unit configuration.

Each disk enclosure feature contains a pair (2) of disk enclosures. Each disk drive set feature contains 16 disk drives. Each half drive set feature contains 8 disk drives. When installed, each disk drive set feature is installed with 8 drives in each enclosure, and each half drive set feature is installed with 4 drives in each enclosure.

Note: Half Drive sets apply to SSDs only.

The DS8870 LFF (3.5") storage enclosure slots are numbered left to right, and then top to bottom, so that the top row of drives is D01-D04, the second row is D05-D08, the third row is D09-D12. The DS8870 SFF (2.5") storage enclosure slots are numbered from left to right as slots D01-D24. For full SFF (2.5") drive sets, the first installation group populates as D01-D08 for both enclosures of the pair. The second installation group is D09-D16, and for the DS8870, the third installation group populates as D17-D24. For half drive sets, the first installation group populates as D01-D04 of both enclosures in the pair and the second installation group populates as D05-D08 of both enclosures, and so on.

Note: Keep in mind that DS8870 storage features are installed from the bottom up within a unit.

Table 15. Disk drive set feature placement - full drive sets

Storage enclosure type	Set 1	Set 2	Set 3
DS8870 LFF (3.5")	n/a D01-D04	n/a D05-D08	n/a D09-D12
DS8870 SFF (2.5")	D01-D08	D09-D16	D17-D24

Table 16. Disk drive set feature placement - half drive sets

Storage enclosure type	Set 1	Set 2	Set 3	Set 4	Set 5	Set 6
DS8870 LFF (3.5")	D01-D04 (row 1)	D05-D08 (row 2)	D09-D12 (row 3)	n/a	n/a	n/a
DS8870 SFF (2.5")	D01-D04	D05-D08	D09-D12	D13-D16	D17-D20	D21-D24

Feature codes for IBM Full Disk Encryption disk drive sets

Use the IBM Full Disk Encryption (FDE) disk drive feature codes to order the encryption disk drive sets for your storage unit.

Each IBM Full Disk Encryption disk drive set provides 16 disk drives. Table 17 provides the various encryption disk drive sets that you can order (based on disk size and RPM), and the feature codes to use.

Table 17. Feature codes for IBM Full Disk Encryption disk drive sets. An intermix of encryption and nonencryption disk drives is not supported.

Feature Code	Size and description	Disk speed in RPM (K = 1000)	DS8000 Models
5108	146 GB FDE Drive Set	15K	961 and 96E
5308	300 GB FDE Drive Set	15K	961 and 96E
5708	600 GB FDE Drive Set	10K	961 and 96E
5758	900 GB FDE Drive Set	10K	961 and 96E
5858	3 TB FDE Drive Set	7.2K	961 and 96E
6156	400 GB SSD FDE Half Drive Set	n/a	961 and 96E
6158	400 GB SSD FDE Drive Set	n/a	961 and 96E

Notes:

- An intermix of encryption and nonencryption disk drives is not supported.
- The maximum number of features allowed for 6158 is 12.
- The maximum number of features allowed for 6156 is 1.
- In a DS8870, 8 drives are the minimum number of SSDs (RAID-5 only) that are supported.
- The POWER7 subsystem supports 1 TB of system cache.

Feature codes for disk enclosures

Use disk enclosure feature codes to order the disk enclosures for your storage unit.

Table 18 on page 75 describes the feature codes.

Table 18. Disk enclosure feature code

Feature Code	Description	Models
1241	Disk enclosure pair **Note:** The disk enclosure feature contains two disk enclosure filler features in the disk enclosure. The enclosure pair supports the installation of one to three disk features.	961 and 96E
1242	HD STD enclosure indicator	
1244	3.5" disk drive enclosure indicator	
1245	HD SSD enclosure indicator for 400 GB disk drives	

Standby CoD disk sets

You can use the IBM Standby Capacity On Demand (Standby CoD) offering by ordering Standby CoD disk sets.

A Standby CoD disk set contains 8 or 16 disk drives of the same capacity and 7 200, 10 000, or 15 000 RPM.

When you initially order Standby CoD disk drive features, you must sign a Standby CoD agreement. Each subsequent order for Standby CoD features requires a supplement to the agreement.

To activate Standby CoD disk drives (and exchange them for regular disk drives), you must order a feature exchange. This results in the removal of the Standby CoD feature and the addition of the corresponding regular disk drive feature of the same capacity and speed. The transaction is invoiced at the differential price between the features removed and added.

Feature codes for IBM Full Disk Encryption Standby CoD disk drives

Use the IBM Full Disk Encryption (FDE) Standby Capacity On Demand (Standby CoD) feature codes to order IBM FDE Standby CoD disk sets for your storage unit.

Each IBM Full Disk Encryption disk drive set feature provides 8 or 16 IBM Full Disk Encryption Standby CoD drives. Table 19 provides the various IBM Full Disk Encryption Standby CoD disk drive sets that you can order (based on disk size and RPM), and the feature codes to use.

Table 19. Feature codes for IBM Full Disk Encryption Standby CoD disk drive sets (8 or 16 disk drives per set)

Feature Code	Size and description (see Notes)	Disk speed in RPM (K = 1000)	Models
5108	146 GB FDE CoD Drive Set	15K	961 and 96E
5308	300 GB FDE CoD Drive Set	15K	961 and 96E
5708	600 GB FDE CoD Drive Set	10K	961 and 96E
5758	900 GB FDE CoD Drive Set	10K	961 and 96E
5858	3 TB FDE CoD Drive Set	7.2K	961 and 96E

Table 19. Feature codes for IBM Full Disk Encryption Standby CoD disk drive sets (8 or 16 disk drives per set) (continued)

Feature Code	Size and description (see Notes)	Disk speed in RPM (K = 1000)	Models
Notes: 1. The maximum number of Standby CoD disk drive set features that you can have on a 961 or 96E storage unit is six. 2. An intermix of encryption and nonencryption disk drives is not supported.			

Disk enclosure fillers

Disk enclosure fillers fill empty disk drive slots in disk enclosures.

One disk enclosure filler feature provides a set of 8 or 16 disk enclosure fillers and assists in maintaining a proper temperature for the storage enclosure. It is required that you order two filler features if only one disk drive set feature is in the expansion enclosure pair. One filler feature is required if two disk drive set features are in the expansion enclosure pair.

Feature codes for disk enclosure fillers

Use the disk enclosure filler feature code to order filler sets for the disk enclosure when you have one or two regular or standby CoD features in the enclosure.

A disk enclosure filler set includes 16 fillers (8 fillers for 3.5" disk enclosure filler set). The following feature codes can be used on all models.

2997	3.5" Disk enclosure filler set
2998	Disk enclosure half-filler set
2999	Disk enclosure filler set

Device adapters

Device adapters provide the connection between storage devices and the storage facility images through I/O ports.

Device adapters are ordered and installed in pairs. A device adapter pair supports two independent paths to all of the disk drives served by the pair. The two paths connect to two different network fabrics to provide fault tolerance and to help ensure availability. The physical links allow two read operations and two write operations to be performed simultaneously around the fabric.

Feature codes for device adapters

Use device adapter feature codes to plan for and order the device adapters for your storage unit.

Each device adapter feature includes a pair of device adapters. Table 20 shows the feature codes to use and the applicable models for each feature code.

Table 20. Device adapter feature codes

Feature code	Device adapter types	Models
3053	Device adapter pair I	961 and 96E

Disk drive cables

You must order at least one disk cable set to connect the disk drives to the device adapters.

The disk drive cable feature provides you with a complete set of Fibre Channel cables to connect all the disk drives that are supported by the model to their appropriate device adapters.

Disk drive cable groups have the following configuration guidelines:

- The minimum number of disk drive cable group features for each model is one.
- The disk drive cable groups must be ordered as follows:
  - If the disk drives connect to device adapters within the same base model, order disk drive cable group 1.
  - If the disk drives connect to device adapters within the same expansion model, order disk drive cable group 2.
  - If the disk drives are in a second expansion model (position 2 expansion model), order disk drive cable group 4.
  - If the disk drives are in a third expansion model, order disk drive cable group 5.

Feature codes for disk drive cables

Use the disk drive cable feature codes to order the cable groups for each DS8870 model.

Table 21 shows the feature codes to use and the connection type that is supported by each group.

Table 21. Disk drive cable feature codes

Feature Code	Disk Drive Cable Group	Connection Type
1246	Disk drive cable group 1 - standard	Connects the disk drives to the device adapters within the same base Model 961.
1247	Disk drive cable group 2 - standard	Connects the disk drives to the device adapters within the same expansion Model 96E. Used when the Model 96E is the first expansion model (position 1) within the storage unit.
1248	Disk drive cable group 4 - standard	Connects the disk drives from a second expansion Model 96E to the base Model 961 and first expansion Model 96E.
1249	Disk drive cable group 5 - standard	Connects the disk drives from a third expansion Model 96E to the base Model 961 and second expansion Model 96E.
1250	Disk drive cable group 1 - business class	Connects the disk drives to the device adapters within Model 961, but with business class configuration, reducing the number of installed device adapters and I/O enclosures, while increasing the number of storage enclosures attached to the remaining device adapters.

Configuration rules for storage features

Use the following general configuration rules and ordering information to help you order storage features.

You must order at least one disk drive set for each base Model 961.

Each disk enclosure pair must contain one or a combination of the three hardware components:

- Encryption disk drives
- Standby CoD disk drives
- Disk enclosure fillers

If the disk enclosure contains regular or Standby CoD disk drives, the disk drive features must be of the same capacity.

- Model 961 requires a minimum of 16 disk drives (of the same type, capacity, and RPM)
- Two device adapter (DA) pairs are required for a business class configuration. For business class configuration with feature 4311 (16 GB processor memory) or 4312 (32 GB processor memory), two DA pairs are supported.

Note: Storage features, such as disk enclosures, are installed from the bottom to the top of each base or expansion model. Filling a model is not required for you to begin adding storage features to the next model in the storage unit.

Configuration rules for Standby CoD disks

Use the following configuration rules and ordering information to help you order and activate Standby Capacity On Demand (Standby CoD) disk drive sets.

Standby CoD capacity must be activated within one year of purchase. When you activate Standby CoD capacity, you must order a feature conversion to convert the Standby CoD disk drive set feature to the corresponding regular disk drive set feature. You must activate all drives in the Standby CoD disk set at once. Once you activate Standby CoD disk drive set features, the activation is permanent (once activated, disk capacity cannot be reduced).

Additional storage feature information

To help you determine the type and number of disk drives to add to your storage unit, this section includes additional information.

The following additional information is provided:

- Calculating physical and effective capacity of disk drives

Calculating physical and effective capacity

Use the following information to calculate the physical and effective capacity of a storage unit.

To calculate the total physical capacity of a storage unit, multiply each disk drive set feature by its total physical capacity and sum the values. For DS8000, a disk drive set feature consists of 16 identical disk drives with the same capacity and RPM.

The logical configuration of your storage affects the effective capacity of the disk drive set.

Specifically, effective capacities vary depending on the following configurations:

- Data format

  Physical capacity can be logically configured as fixed block (FB) or count key data (CKD). Data accessed by open systems hosts or Linux on System z that support Fibre Channel protocol must be logically configured as FB. Data accessed by System z hosts with z/OS or z/VM must be configured as CKD.

- Array or rank configuration

  The disk drive arrays on the system can be contained in RAID ranks and RAID configurations. A rank can contain only one array.

Each RAID rank is divided into equal-sized segments known as extents. All extents are approximately 1 GB. However, FB extents are slightly larger than CKD extents.

DS8000 series

DS8000 RAID capacities for RAID 5 arrays, Table 23 on page 80, and Table 24 on page 80 describe the effective capacities for RAID arrays.

Table 22. DS8000 RAID capacities for RAID 5 arrays

Disk size and storage unit	Total physical capacity (GB) per disk drive set	Fixed block (FB) or count key data (CKD)	Effective capacity in GB (Number of Extents) (See Notes)	
			Rank with RAID 5 array	
			6 + P	7 + P
146 GB (SAS)	2336	FB	794.6 (740)	933.1 (869)
		CKD	793.66 (829)	931.5 (973)
300 GB (SAS)	4800	FB	1655.7 (1542)	1936 (1803)
		CKD	1653.36 (1727)	1934 (2020)
400 GB (SSD)	6400	FB	1846.84 (1720)	2230.16 (2077)
		CKD	1845.79 (1928)	2227.77 (2327)
600 GB (SAS)	9600	FB	3372.62 (3141)	3936.33 (3666)
		CKD	3367.99 (3518)	3931.87 (4107)
900 GB (SAS)	14400	FB	5077.73 (4729)	5925 (5518)
		CKD	5071.13 (5297)	5917.43 (6181)

Notes:

1. Physical capacities are in decimal gigabytes (GB). One decimal GB is 1,000,000,000 bytes.
2. Disk drive sets contain 16 drives and half disk drive sets contain 8 drives. An array site contains 8 drives. The effective capacities shown are for a single array, which resides in one array site.
3. Rank capacities are slightly smaller (34GB) on DS8870 as compared to the similar DS8800. This reduction of extents must be planned for when moving or migrating data to the DS8870.

Table 23. DS8000 RAID capacities for RAID 6 arrays

Disk size and storage unit	Total physical capacity (GB) per disk drive set	Fixed block (FB) or count key data (CKD)	Effective capacity in GB (Number of Extents) (See Notes)	
			Rank with RAID 6 array	
			5 + P + Q	6 + P + Q
146 GB (SAS)	2336	FB	640 (596)	777.39 (724)
		CKD	639.52 (668)	777.38 (812)
300 GB (SAS)	4800	FB	1341.10 (1249)	1621.35 (1510)
		CKD	1340.30 (1400)	1618.89 (1691)
600 GB (SAS)	9600	FB	2738.04 (2550)	3301.75 (3075)
		CKD	2736.13 (2858)	3298.09 (3445)
900 GB (SAS)	14400	FB	4125.32 (3842)	4971.43 (4630)
		CKD	4122.38 (4306)	4966.77 (5188)
3 TB (SAS)	48000	FB	13840.53 (12890)	16662.33 (15518)
		CKD	13831.90 (14448)	16644.63 (17386)

Notes:

1. Physical capacities are in decimal gigabytes (GB). One decimal GB is 1,000,000,000 bytes.
2. Disk drive sets contain 16 drives and half disk drive sets contain 8 drives. An array site contains 8 drives. The effective capacities shown are for a single array, which resides in one array site.
3. Rank capacities are slightly smaller (34GB) on DS8870 as compared to the similar DS8800. This reduction of extents must be planned for when moving or migrating data to the DS8870.

Table 24. DS8000 RAID capacities for RAID 10 arrays

Disk size and storage unit	Total physical capacity (GB) per disk drive set	Fixed block (FB) or count key data (CKD)	Effective capacity in GB (Number of Extents) (See Notes)	
			Rank with RAID 10 array	
			3 + 3	4 + 4
146 GB (SAS)	2336	FB	379.03 (353)	517.55 (482)
		CKD	378.16 (395)	516.97 (540)

Table 24. DS8000 RAID capacities for RAID 10 arrays (continued)

Disk size and storage unit	Total physical capacity (GB) per disk drive set	Fixed block (FB) or count key data (CKD)	Effective capacity in GB (Number of Extents) (See Notes)	
			Rank with RAID 10 array	
			3 + 3	4 + 4
300 GB (SAS)	4800	FB	809.60 (754)	1092 (1017)
		CKD	808.01 (844)	1090.43 (1139)
600 GB (SAS)	9600	FB	1667.52 (1553)	2236.60 (2083)
		CKD	1665.80 (1740)	2232.56 (2332)
900 GB (SAS)	14400	FB	2520.07 (2347)	3374.77 (3143)
		CKD	2516.89 (2689)	3368 (3518)

Notes:

1. Physical capacities are in decimal gigabytes (GB). One decimal GB is 1,000,000,000 bytes.
2. Disk drive sets contain 16 drives and half disk drive sets contain 8 drives. An array site contains 8 drives. The effective capacities shown are for a single array, which resides in one array site.
3. Rank capacities are slightly smaller (34GB) on DS8870 as compared to the similar DS8800. This reduction of extents must be planned for when moving or migrating data to the DS8870.

I/O adapter features

You must select the I/O adapter features that you want on your DS8000 models.

The I/O adapter features are separated into the following categories:

- I/O enclosures
- Device adapters and cables
- Host adapters and cables

I/O enclosures and cables

I/O enclosures are required for your storage unit configuration.

The I/O enclosures hold the I/O adapters and provide connectivity between the I/O adapters and the storage unit processors. I/O enclosures are ordered and installed in pairs.

The I/O adapters contained in the I/O enclosures can be either device or host adapters. Each I/O enclosure pair can support up to four device adapters (two pairs) and four host adapters.

The I/O cables are PCIe that provide the connection between the I/O enclosures and the base model processors.

Feature codes for I/O enclosures

For Model 961, use I/O enclosure feature code 1301 to order one I/O enclosure pair.

Feature codes for I/O cables

Use I/O cable feature codes to order the I/O cables you require for your storage unit.

Table 25 provides the I/O cable groups that you can order, a description of the connection that is provided by the group, the supported models, and the feature codes to use.

Table 25. PCIe cable feature codes

Feature Code	Cable Group	Description	Models
1320	PCIe cable group 1	Connects device/host adapters in an I/O enclosure pair to the processor.	961
1321	PCIe cable group 2	Connects device/host adapters in I/O enclosure pairs to the processor.	961
1322	PCIe cable group 3	Connects device/host adapters in an I/O enclosure pair to the processor.	96E

Fibre Channel (SCSI-FCP and FICON) host adapters and cables

You can order Fibre Channel host adapters for your storage unit configuration.

The Fibre Channel host adapters enable the storage unit to attach to Fibre Channel (SCSI-FCP) and FICON servers, and SAN fabric components. They are also used for remote mirror and copy control paths between DS8000 storage units or between a DS8000 storage unit and a DS6000 storage unit or a 2105 storage unit (Model 800 or 750). Fibre Channel host adapters are installed in an I/O enclosure.

The adapters have four or eight ports and support 4 or 8 Gbps full-duplex data transfer over longwave or shortwave fibre links.

Supported protocols include the following types:

- SCSI-FCP ULP (Upper Layer Protocol) on point-to-point, fabric, and arbitrated loop (private loop) topologies.
- FICON ULP on point-to-point and fabric topologies.

Notes:

1. SCSI-FCP and FICON are supported simultaneously on the same adapter, but not on the same port.
2. For highest availability, ensure that you add adapters in pairs.

A Fibre Channel cable is required to attach each Fibre Channel adapter port to a server or fabric component port. Each cable has a Lucent connector (LC) at one end to attach to the Fibre Channel adapter port. The cables are available with either a LC or standard connector (SC) at the other end to attach to the server or fabric component port. You can also order a conversion cable that can be used to attach the Fibre Channel adapter port to a cable with an SC connector.

Feature codes for Fibre Channel host adapters

Use Fibre Channel feature codes when you plan for and order Fibre Channel host adapters for your storage unit.

Table 26 provides a list of the types of Fibre Channel adapters that you can order, their characteristics, and their feature codes.

Table 26. Fibre Channel host adapters feature codes

Feature Code	Description	Model	Protocols	Link Speed	Receptacle Type
3153	Shortwave host adapter PCIe, 4-port	961, 96E	FCP and FICON	8 Gbps	LC
3157	Shortwave host adapter PCIe, 8-port		FCP and FICON	8 Gbps	LC
3253	Longwave host adapter PCIe, 4-port		FCP and FICON	8 Gbps	LC
3257	Longwave host adapter PCIe, 8-port		FCP and FICON	8 Gbps	LC

Feature codes for Fibre Channel cables

Use Fibre Channel cable feature codes when you plan for and order Fibre Channel cables to connect Fibre Channel host adapters to your storage unit.

Table 27 provides the feature codes for the available Fibre Channel cables.

Table 27. Fibre Channel cable feature codes

Feature Code	Cable Type	Connector Types		Length	Compatible Fibre Channel Host Adapter Features
		First End	Second End		
1410	50 micron Fibre Channel cable, multimode	LC connector	LC connector	40 m (131 ft)	• Short wave Fibre Channel/ FICON host adapters (feature 3153 and 3157) • Long wave Fibre Channel/ FICON adapters (feature 3253 or 3257).
1411	50 micron Fibre Channel cable, multimode	LC connector	SC connector	31 m (102 ft)	
1412	50 micron Fibre Channel conversion cable, multimode	LC connector	SC receptacle	2 m (6.5 ft)	
1420	9 micron Fibre Channel cable, single mode	LC connector	LC connector	31 m (102 ft)	• Long wave Fibre Channel/ FICON adapters (feature 3253 or 3257).
1421	9 micron Fibre Channel cable, single mode	LC connector	SC connector	31 m (102 ft)	
1422	9 micron Fibre Channel conversion cable, single mode	LC connector	SC receptacle	2 m (6.5 ft)	

Configuration rules for I/O adapter features

To order I/O adapter features, you must follow specific configuration rules.

The following configuration rules affect I/O adapter features:

- Configuration rules for I/O enclosures, I/O cables, and device adapters
- Configuration rules for host adapters and host adapter cables

Configuration rules for I/O enclosures, I/O cables, and device adapters

Use these configuration rules and ordering information to help you order I/O enclosures, I/O cables, and device adapters.

You must consider your entire storage system (base model and any attached expansion units) when you order. Every disk enclosure pair must be populated with either 16, 32, or 48 disk drives. If a disk enclosure pair is populated with only 16 or 32 disk drives, it must be populated with one or two disk enclosure filler sets (feature #2999).

Use Table 28 to determine the number of I/O enclosures and device adapters features that you need in various storage unit configurations. To use the table, find the rows that contain the type of storage unit you are configuring. Then find the row that represents the number of disk enclosures that are installed on that storage unit. Look in the last two columns to find the number of I/O enclosures and device adapters that you need on the storage unit.

Table 28. Model 961 required I/O enclosures and device adapters (based on disk enclosures)

Storage Unit Type	Storage Unit Configuration	Disk Enclosure Features (1241)	Required Device Adapter Features (3053) (Note 1)	Required I/O Enclosure Features (1301) (Notes 2 and 3)
961 (2-core) storage unit	Business Class	1-2	1	1
		3	2	1
961 (4-core) storage unit	Base model	1-2	1	1
		3	2	1
		4-5	4	2
96E (8-core or 16-core) storage unit	Expansion Model	1	1	1
		2	2	2
		3	3	2
		4-7	4	2

Notes:

1. Each device adapter feature code represents one device adapter pair. There is one device adapter pair in each I/O enclosure.
2. The maximum quantity is two device adapter features for each I/O enclosure feature in the storage unit.
3. Each I/O enclosure feature represents one I/O enclosure pair. An I/O enclosure pair can support up to two device adapter pairs.

Configuration rules for host adapters and cables

Use the following configuration rules and ordering information to help you order host adapters and cables.

When you configure your DS8000 storage unit, consider the following issues when ordering the host adapters for the storage unit:

- What are the minimum and maximum numbers of host adapters that I can install?
- How can I balance the host adapters across the storage unit to help ensure optimum storage unit performance?
- What host adapter configurations help ensure high availability of my data?
- How many and what type of cables do I need to order to support the host adapters?

In addition, consider the following host adapter guidelines:

- You can include a combination of Fibre Channel host adapters in one I/O enclosure.
- Feature conversions are available to exchange installed adapters when purchasing new adapters of a different type.

Maximum and minimum configurations

Table 29. Model 961 minimum and maximum host adapter features

Storage Unit Type	Storage Unit Configuration	Minimum Number of Host Adapter Features for the Base Model	Maximum Number of Host Adapter Features for the Storage Unit (See Note)
961 (2-core) Business class	Base model	2	4
961 (4-core)	Base model	2	8
	Base model + 1-3 expansion models	2	16
Note: The maximum number of host adapters for any one model cannot exceed 8 with 8 Gbps host adapters. You can add host adapters only to the base model in a 961 storage unit and the first expansion model, 96E.			

Configuring for highest availability

After you have met the initial minimum order requirement, you can order one host adapter at a time. However, to ensure the highest availability of your data, always add host adapters (of the same type) in pairs.

For optimum storage unit performance, it is important that you order host adapters to balance them within your storage unit.

Notes:

- Although one multiport adapter can provide redundant pathing, keep in mind that if you install only one adapter and if there is a failure or service action affecting that adapter, a loss of access to all data through that adapter can occur.

- If you have an IBM service representative move existing host adapters from one slot to another, you can configure the host ports on your storage unit using the IBM System Storage DS Storage Manager or the IBM System Storage DS CLI. See the "DS Storage Manager configuration for I/O Attachment" section in the *IBM System Storage DS8000 Host Systems Attachment Guide* for information on configuring storage unit host I/O ports.

Ordering host adapter cables

For each host adapter, you must also order the appropriate host adapter cables. Typically, to connect Fibre Channel host adapters to a server or fabric port, you order the following cables:

- For shortwave Fibre Channel host adapters, order one of the 50 micron multimode fiber-optic cables terminated with an LC connector.
- For longwave Fibre Channel host adapters, you can order either the 9 micron single mode that ends in an LC connector or one of the 50 micron multimode fiber-optic cables that ends in an LC connector. Only the 9 micron cable is supported when the adapter feature is operating at a 2, 4 or 8 Gbps transfer rate.

IBM Global Services Networking Services can provide assistance for any unique cabling and installation requirements.

Processor memory features

These features specify the amount of memory you want for the processors on your model.

Feature codes for processor memory

Use processor memory feature codes to plan for and order processor memory for your storage unit configuration.

Table 30 provides the processor memory feature codes for the DS8000 models.

Table 30. Processor memory[1] feature codes

Feature Code	Description	Models
4311[2]	16 GB processor memory	961 Business Class (2-core)
4312[2]	32 GB processor memory	961 Business Class (2-core)
4313[3]	64 GB processor memory	961 (4-core)
4314[4]	128 GB processor memory	961 (8-core)
4315[4]	256 GB processor memory	961 (8-core)
4316[5]	512 GB processor memory	961 (16-core)
4317[5]	1 TB processor memory	961 (16-core)

Notes:

1. Memory is not the same as cache. The amount of cache is less than the amount of available memory.
2. Feature codes 4311 and 4312 require feature code 4401.
3. Feature code 4313 requires feature code 4402.
4. Feature codes 4314 and 4315 require feature code 4403.
5. Feature codes 4316 and 4317 require feature code 4404.

Configuration rules for processor memory

Use the configuration rules and ordering information to help you select and order processor memory for your storage unit.

You must order one processor memory feature for the configuration of each base model.

Model 961 two-core configuration, business class feature code 4311 and 4312
You can select from 16 GB to 32 GB of processor memory.

Note: The 16 GB (feature code 4211) and 32 GB (feature code 4212) processor memory options are available only for the two-core configuration, business class feature.

Model 961 four-core configuration
Offers 64 GB of processor memory.

Model 961 eight-core configuration
You can select from 128 GB to 256 GB of processor memory.

Model 961 sixteen-core configuration
You can select from 512 GB to 1 TB of processor memory.

Power features

You must specify the power features to include on your DS8000 series models.

The power features are separated into the following categories:

- Power cords
- Input voltage
- DC-UPS (direct current uninterruptible power supply)

For the DS8870, models 961 and 96E, the DC-UPS is included in your order.

Power cords

A pair of power cords is required for each base or expansion model. (Power cords are also known as power cables.)

Both of the power supplies for each expansion model (96E) need power to be present at both of the enclosure power supply locations. This helps to prevent facility power loss to a single power cord.

Feature codes for power cords

Use power cord feature codes when you order power cords for your base or expansion model. Each feature code represents two power cords.

Table 31 provides the power cord feature codes and associated wire gauges for the DS8870. Ensure that you meet the requirements for each power cord and connector type that you order.

Table 31. Power cord feature codes for the DS8870

Feature Code	Power Cord Type	Wire Gauge
1061	Single-phase power cord, 200-240V, 60A, 3-pin connector	10 mm² (6awg)

Table 31. Power cord feature codes for the DS8870 (continued)

Feature Code	Power Cord Type	Wire Gauge
1068	Single-phase power cord, 200-240V, 63A, no connector	10 mm² (6awg)
1072	Top exit single-phase power cord, 200-240V, 60A, 3-pin connector	10 mm² (6awg)
1073	Top exit single-phase power cord, 200-240V, 63A, no connector	10 mm² (6awg)
1081	Three-phase power cord, wye, 380V-415V, 32A, no connector	6 mm² (10awg)
1082	Three-phase power cord, delta, 200-240V, 60A, 4-pin connector	10 mm² (6awg)
1083	Top exit three-phase power cord, wye, 380V-415V, 32A, no connector	6 mm² (10awg)
1084	Top exit three-phase power cord, delta, 200-240V, 60A, 4-pin connector	10 mm² (6awg)

Table 32. Additional feature codes for top exit power cords

Feature Code	Installation Item
1101	Universal ladder for top exit cable access

Note: For storage units with top exit power cords (feature codes 1072, 1073, 1083, 1084) a minimum of one IBM safety-approved ladder (feature code 1101) must be ordered per customer site. This ladder is a requirement for storage unit installation.

Input voltage

The DS8000 DC-UPS distributes full wave, rectified power that ranges from 200 V ac to 240 V ac.

DC-UPS

The IBM System Storage DS8870 rack power system includes the DC-UPS (direct current uninterruptible power supply) with integrated batteries.

Each DS8870 rack includes 2 DC-UPS. Each DC-UPS can include one or two battery assembly sets depending on the configuration ordered.

The DS8870 uses DC-UPS power supplies with integrated battery for data protection. A separate feature code is not required for the DC-UPS. Each DS8870 includes two DC-UPS. The extended power line disturbance (ePLD) option (feature code 1055) is designed to protect your storage unit for 50 seconds, rather than 4 seconds without the ePLD feature, from a power line disturbance.

Note: If no ePLD option is ordered, one BSM set per DC-UPS (for both the main and expansion racks) is needed. If the ePLD option is ordered, two BSM sets per DC-UPS (for both the main and expansion racks) are needed (feature code 1051).

The DC-UPS monitors it's own ac (alternating current) input. Each DC-UPS rectifies and distributes the input ac. If the DC-UPS detects a loss of input line power it switches its output to distribute the rectified ac from it's partner DC-UPS. If both lose input ac, they switch to battery power.

Activation and Recovery for system failure - If both power cords lose ac input, the DC-UPS senses that both partner power and local power is running on batteries. Both stay on battery power and provide status to the RPC (rack power control), which initiates an recovery process. This process occurs if any phase of the three-phase system is lost.

Feature codes for battery assemblies

Use battery assembly feature codes to plan for and order battery assemblies for your base or expansion model.

The following feature codes applies to all models.

1051 Battery assembly

Configuration rules for power features

Ensure that you are familiar with the configuration rules and feature codes before you order power features.

When you order power cord features, the following rules apply:

- You must order a minimum of one power cord feature for each model. Each feature code represents a pair of power cords (two cords).
- You must select the power cord that is appropriate to the geographic region where the storage unit is located.

For battery assemblies, the following rules apply:

- You must order battery assemblies (feature 1051) for each base and each of the expansion models. The extended PLD feature is 1055. Table 33 provides the quantity of battery assembly features or extended PLD features (1055) you must order.
- No minimum order is required for the 961 base model and the 96E expansion model, unless either unit contains an extended PLD feature. If an extended PLD feature is installed, you must order a battery assembly (feature 1055) to power the system when the external power system is lost. All DC-UPS in all models require one battery assembly set. There are two DC-UPS in each model.

Table 33. Required quantity of battery assemblies

Model 961 and 96E with feature code 1055 or 1301	Model 961 and 96E without feature code 1055	Model 961 and 96E with feature code 1055
2 each	1 each	2 each

Other configuration features

Additional features beyond the standard configuration are available for shipping and setup of a DS8000 storage unit.

You can select other options for the shipping and setup of your DS8000 storage unit in addition to the standard configuration. Optional feature codes that you can specify to customize or to receive your DS8000 storage unit include:

- Extended power line disturbance (EPLD) option
- Remote System z power control option

- Earthquake Resistance Kit option
- BSMI certificate (Taiwan)
- Shipping weight reduction option

Extended power line disturbance

The extended power line disturbance (EPLD) feature allows your storage unit to be protected for 50 seconds, rather than only milliseconds, from a power line disturbance. This feature is optional for your storage unit configuration.

Without the EPLD feature, a standard DS8000 storage unit offers you about 4 seconds of protection from power line disturbances. Adding this feature increases your protection to 50 seconds.

You order the EPLD feature for your storage unit. All models must contain battery assemblies. "Configuration rules for power features" on page 89 provides more information about the configuration rules for battery assemblies.

Feature code for extended power line disturbance

Use extended power line disturbance feature codes when you plan for and order the extended power line disturbance features for your storage unit.

You can order this feature with the following feature code:

1055 Extended power line disturbance (all models)

Note: If no ePLD option is ordered, one BSM set per rack (for both the main and expansion racks) is needed. If the ePLD option is ordered, two battery assembly sets per rack (for both the main and expansion racks) are needed (feature code 1051).

Remote zSeries power control feature

The optional remote zSeries power control feature adds a logic card that allows one or more attached System z or S/390 hosts to control the power on and power off sequences for your storage unit.

When you use this feature, you must specify the **zSeries power control** setting in the DS Storage Manager that is running on the management console.

This feature includes the cables necessary to connect the logic card.

Feature code for remote zSeries power control

Use the zSeries feature code when you plan for and order the remote zSeries power control feature for your storage unit.

1000 Remote zSeries power control

Earthquake Resistance Kit

The Earthquake Resistance Kit is an optional seismic kit for stabilizing the storage unit rack, so that the rack complies with IBM earthquake resistance standards.

The Earthquake Resistance Kit option is available for models 961 and 96E (by feature code number 1906).

It is important for computer systems to be adequately restrained during earthquakes. This precaution helps to prevent human injury. It also ensures the availability of the system following an earthquake by limiting potential damage to critical system components such as hard drives. This optional Earthquake Resistance Kit feature includes cross-braces on the front and rear of the rack, which prevent the rack from twisting. Hardware at the bottom of the rack secures it to the floor. The Earthquake Resistance Kit ensures that your storage unit complies with the earthquake resistance objectives that are documented in Earthquake Resistance for IBM Hardware Products (IBM Corporate Bulletin C-B 1-9711-009 9202).

You are responsible for obtaining specific fastening hardware and preparing the floor before the IBM service representative can install the Earthquake Resistance Kit. Installation of the required floor hardware and the Earthquake Resistance Kit is disruptive. If the Earthquake Resistance Kit feature is installed on an existing storage unit, the storage unit must be turned off and temporarily moved while the floor preparations are made and the kit is installed.

Notes:

- If you order the optional Earthquake Resistance Kit, you must order one for each storage unit rack.
- If you want IBM to remove a previously installed Earthquake Resistance Kit, it must be removed by an IBM Service Representative.

Feature code Earthquake Resistance Kit

Use the Earthquake Resistance Kit feature code when you plan for and order an Earthquake Resistance Kit option for your DS8000.

Use this feature code when you order the Earthquake Resistance Kit option for Models 961 and 96E.

1906 Earthquake Resistance Kit (all models)

BSMI certificate (Taiwan)

The BSMI certificate for Taiwan option provides the required Bureau of Standards, Metrology and Inspection (BSMI) ISO 9001 certification documents for DS8000 shipments to Taiwan.

If the DS8000 models that you order are shipped to Taiwan, you must order this option for each model that is shipped.

Feature code for BSMI certificate (Taiwan)

Use the BSMI certificate feature code when you plan for and order the BSMI certificate options for a DS8000 model.

0400 This feature provides the BSMI certification documents that are required when the DS8000 model is shipped to Taiwan.

Shipping weight reduction

The shipping weight reduction option allows you to receive delivery of a DS8000 model in multiple shipments.

If your site has delivery weight constraints, IBM offers a shipping weight reduction option that ensures the maximum shipping weight of the initial model shipment does not exceed 909 kg (2000 lb). The model weight is reduced by removing selected components, which are shipped separately.

The IBM service representative installs the components that were shipped separately during the storage unit installation. This feature increases storage unit installation time, so order it only if it is required.

Feature code for shipping weight reduction

Use the shipping weight reduction feature code when you plan for and order the shipping weight reduction option for your DS8000 model.

0200 This feature ensures that the maximum shipping weight of any DS8000 base model or expansion model does not exceed 909 kg (2000 lb) each. Packaging adds 120 kg (265 lb).

Chapter 5. Planning use of licensed functions

Licensed functions are the storage unit system operating system and functions. Required features and optional features are included.

IBM authorization for licensed functions is purchased as 239x machine function authorizations. However, the license functions are actually machine models. For example, the operating environment license (OEL) is listed as a 239x Model LFA, OEL license (242x machine type). The 239x machine function authorization features are for billing purposes only.

239x function authorization models (242x machine types)

To establish the extent of IBM authorization for a licensed function, you purchase a *function authorization model* by ordering a specific feature code that indicates the size, in terabytes (or TBs, where 1 TB equals 1,000,000,000,000 bytes), of the extent of IBM authorization.

The function authorization model size (or level) represents physical capacity. The total authorization level for a given licensed function is the sum of the TBs associated with all the purchased feature numbers.

Function authorizations are purchased for the DS8000 base model and they establish the authorization level for the entire storage unit (base model plus any expansion models). The operating environment license authorizations (239x Model LFA, OEL license) must be authorized for the full physical capacity of the storage unit. When you order optional licensed functions, you purchase a license for a specific authorization level (a specific number of TBs) for the storage unit.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

After you purchase the function authorizations, you manage and activate the functions through the following IBM Disk Storage Feature Activation (DSFA) website:

www.ibm.com/storage/dsfa

Licensed function indicators

Each licensed function indicator feature that you order on a DS8000 series base unit enables that function at the system level.

After you receive and apply the IBM feature activation keys for the licensed function indicators, your functions are enabled for you to use. The license function indicators are also used for maintenance billing purposes.

DS8000 Series Function Authorization (242x machine type or 239x functional authorization machine type) feature numbers must be purchased to establish the extent of IBM authorization for the licensed function before the feature activation code is provided by IBM.

Note: You do not select these features for any attached 242x expansion units in the storage unit.

Table 34 provides the appropriate licensed function indicators for each licensed function for Model 961.

Table 34. Licensed function indicators for Model 961

Licensed function	Hardware machine type 242x indicator feature numbers	Function authorization machine type 239x models and features
Operating environment	0700	Model LFA OEL features 70*xx*
FICON attachment	0703	Model LFA FICON attachment feature 7091
Thin Provisioning	0707	Model LFA feature 7071
DB protection	0708	Model LFA Database protection feature 7080
High Performance FICON	0709	Model LFA zHPF feature 7092
IBM System Storage Easy Tier	0713	Model LFA IBM System Storage Easy Tier feature 7083
z/OS Distributed Data Backup	0714 and 7094	Model LFA feature number 7094
Point-in-time copy	0720	Model LFA PTC features 72*xx*
FlashCopy SE	0730	Model LFA SE features 73*xx*
Metro/Global Mirror	0742	Model LFA MGM features 74*xx*
Metro Mirror	0744	Model LFA MM features 75*xx*
Global Mirror	0746	Model LFA GM features 74*xx*
Remote mirror for z/OS	0760	Model LFA RMZ features 76*xx*
z/OS Metro/Global Mirror Incremental Resync (RMZ resync)	0763	Model LFA RMZ resynchronization features 76*xx*
Parallel access volumes	0780	Model LFA PAV features 78*xx*
IBM HyperPAV	0782	Model LFA HyperPAV feature 7899
I/O Priority Manager	0784	Model LFA feature 7840-7850

License scope

Licensed functions are activated and enforced within a defined license scope.

License scope refers to the following types of storage and types of servers with which the function can be used:

Fixed block (FB)

The function can be used only with data from Fibre Channel attached servers.

Count key data (CKD)

The function can be used only with data from FICON attached servers.

Both FB and CKD (ALL)

The function can be used with data from all attached servers.

Some licensed functions have multiple license scope options, while other functions have only a single license scope. Table 35 provides the license scope options for each licensed function.

Table 35. License scope for each DS8000 licensed function

Licensed Function	License Scope Options
Operating environment	ALL
FICON attachment	CKD
High Performance FICON	
Database protection	FB, CKD, or ALL
Point-in-time copy	
Point-in-time copy add	
FlashCopy SE	
FlashCopy SE add	
Remote mirror and copy	
Global mirror	
Global mirror add	
Metro mirror	
Metro mirror add	
Remote mirror for z/OS	CKD
Parallel access volumes	
HyperPAV	
Thin Provisioning	FB
IBM System Storage Easy Tier	FB, CKD, or All
I/O Priority Manager	FB, CKD
z/OS Distributed Data Backup	CKD
z/OS Global Mirror Incremental Resync	
w	

You do not specify the license scope when you order function authorization feature numbers. Feature numbers establish only the extent of the IBM authorization (in terms of physical capacity), regardless of the storage type. However, if a licensed function has multiple license scope options, you must select a license scope when you initially retrieve the feature activation codes for your storage unit. This activity is performed using the Disk Storage Feature Activation (DSFA) website:

www.ibm.com/storage/dsfa

Note: Retrieving feature activation codes is part of managing and activating your licenses. Before you can logically configure your storage unit, you must first manage and activate your licenses.

When you use the DSFA website to change the license scope after a licensed function has been activated, a new feature activation code is generated. When you install the new feature activation code into the machine, the function is activated and enforced using the newly selected license scope. The increase in the license scope (changing FB or CKD to ALL) is a nondisruptive activity but takes effect at the next machine IML. A lateral change (changing FB to CKD or changing CKD to FB) or a reduction of the license scope (changing ALL to FB or CKD) is also a nondisruptive activity and takes effect at the next machine IML.

Ordering licensed functions

After you decide which licensed functions to use with your storage unit, you are ready to order the functions. Functions to include are operating environment license (OEL) features and optional licensed functions

Licensed functions are purchased as DS8000 function authorization features.

To order licensed functions, use the following general steps:

1. Order the operating environment license (OEL) features that support the total physical capacity of your storage unit.
2. Order optional licensed functions for your storage unit.

Ordering rules for licensed functions

An operating environment license (OEL) is required for every DS8000 base model. All other licensed functions are optional.

For all licensed functions, you can combine feature codes to order the exact capacity that you need. For example, if you determine that you need 23 TB of point-in-time capacity, you can order two 7253 features (10 TB each) and three 7251 features (1 TB each).

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

When you calculate physical capacity, consider the capacity across the entire storage unit, including the base model and any expansion models. To calculate the physical capacity, use Table 36 to determine the total size of each regular disk drive feature on your storage unit, and then add all the values.

Note: Standby CoD disk drive features do not count toward the physical capacity.

Table 36. Total physical capacity of each type of disk drive feature

Size of Disk Drives	Total Physical Capacity	Disk drives per Feature
146 GB	2336 GB	16
300 GB	4800 GB	16
400 GB	6400 GB	16
600 GB	9600 GB	16

Table 36. Total physical capacity of each type of disk drive feature (continued)

Size of Disk Drives	Total Physical Capacity	Disk drives per Feature
900 GB	14,400 GB	16
3 TB	48,000 GB	8

Rules specific to 239x Model LFA, OEL license (machine type 242x)

The operating environment license (OEL) must cover the full physical capacity of your storage unit, which includes the physical capacity of any expansion model within the storage unit. The license must cover both open systems data (fixed block data) and System z data (count key data). Standby CoD drives are not included in this calculation.

Note: Your storage unit cannot be logically configured until you have activated the OEL for it. Upon activation, disk drives can be logically configured up to the extent of the IBM OEL authorization level.

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need 25 TB of Metro Mirror capacity, you can order two 7503 features (10 TB each) and one 7502 feature (5 TB each).

As you add additional disk drives to your storage unit, you must increase the OEL authorization level for the storage unit by purchasing additional license features. (Otherwise, you cannot logically configure the additional disk drives for use.)

When you activate Standby CoD disk drives, you must also increase the OEL authorization to cover the activated Standby CoD capacity.

Rules specific to optional licensed functions

The following ordering rules apply when you order point-in-time licenses for FlashCopy or remote mirror and copy licenses:

- If the function is used with only open systems data, a license is required for only the total physical capacity that is logically configured as fixed block (FB).
- If the function is used with only System z data, a license is required for only the total physical capacity that is logically configured as count key data (CKD).
- If the function is used for both open systems and System z data, a license is required for the total configured capacity.
- You must use Fibre Channel host adapters with remote mirror and copy functions. To see a current list of environments, configurations, networks, and products that support remote mirror and copy functions, click **Interoperability Matrix** at the following DS8000 website:

  www.ibm.com/systems/support/storage/config/ssic
- You must purchase features for both the source (primary) and target (secondary) DS8000 storage units.
- If you use the Metro/Global Mirror solution in your environment, the following rules apply:
  - Site A - You must have a Metro/Global Mirror license, and a Metro Mirror license.

Note: A Global Mirror Add-on license is required if you remove Site B and you want to resync between Site A and Site C.

  - Site B - You must have a Metro/Global Mirror license, a Metro Mirror license, and a Global Mirror Add-on license.
  - Site C - You must have a Metro/Global Mirror license, a Global Mirror license, and a point-in-time copy license.

  A Metro/Global Mirror solution is available with the Metro/Global Mirror indicator feature numbers 74xx and 0742 and corresponding DS8000 series function authorization (2396-LFA MGM feature numbers 74xx).

    - Site A - You must have a Metro/Global Mirror license, and a remote mirror and copy license.
    - Site B - You must have a Metro/Global Mirror license, and a remote mirror and copy license.
    - Site C - You must have a Metro/Global Mirror license, a remote mirror and copy license, and a point-in-time copy license.

- If you use Global Mirror, you must use the following additional rules:
  - A point-in-time copy function authorization (239x Model LFA, PTC license, 242x machine type) must be purchased for the secondary storage unit.
  - If Global Mirror is to be used during failback on the secondary storage unit, a point-in-time copy function authorization must also be purchased on the primary system.

The following ordering rule applies to remote mirror for z/OS licenses:

- A license is required for only the total physical capacity that is logically configured as count key data (CKD) volumes for use with System z host systems.
- When failback from the secondary storage unit to the primary storage unit is required, the remote mirror for z/OS function authorization (239x Model LFA, RMZ license, 242x machine type) must be purchased for both systems.

For parallel access volumes (PAV), a license is required for only the total physical capacity that is logically configured as count key data (CKD) volumes for use with System z host systems.

The following ordering rule applies to IBM HyperPAV:

- A license for IBM HyperPAV requires the purchase of PAV licensed features.

The initial enablement of any optional DS8000 licensed function is a concurrent activity (assuming that the appropriate level of microcode is installed on the machine for the given function). The removal of a DS8000 licensed function to deactivate the function is a non-disruptive activity but takes effect at the next machine IML.

If you have an active optional function and no longer want to use it, you can deactivate the function in one of the following ways:

- Order an inactive or disabled license and replace the active license activation key with the new inactive license activation key at the IBM Disk Storage Feature Activation (DSFA) website.
- Go to the DSFA website and change the assigned value from the current number of terabytes (TB) to 0 TB. This value, in effect, makes the feature inactive. If this

change is made, you can later go back to DSFA and reactivate the feature, up to the previously purchased level, without having to repurchase the feature.

Regardless of which method is used, the deactivation of a licensed function is a non-disruptive activity but takes effect at the next machine IML.

Note: Although you do not need to specify how the licenses are to be applied when you order them, you must allocate the licenses to the storage image when you obtain your license keys on the IBM Disk Storage Feature Activation (DSFA) website.

Operating environment license (239x Model LFA, OEL license, 242x machine type)

The operating environment model and features establish the extent of IBM authorization for the use of the IBM System Storage DS operating environment.

For every storage unit, you must order an operating environment license (OEL). This operating environment license support function is called the 239x Model LFA, OEL license on the 242x hardware machine type. The OEL licenses the operating environment and is based on the total physical capacity of the storage unit (base model plus any expansion models). It authorizes you to use the model configuration at a given capacity level. Once the OEL has been activated for the storage unit, you can configure the storage unit. Activating the OEL means that you have obtained the feature activation key from the DSFA website and entered it into the DS Storage Manager.

Feature codes for the operating environment license

You must order an operating environment license (OEL) feature for every storage unit.

Table 37 on page 100 provides the feature codes for the operating environment license.

Table 37. Operating environment license feature codes

Feature code	Description	Hardware models
7030	OEL - inactive	961
7031	OEL - 1 TB unit	
7032	OEL - 5 TB unit	
7033	OEL - 10 TB unit	
7034	OEL - 25 TB unit	
7035	OEL - 50 TB unit	
7040	OEL - 100 TB unit	
7045	OEL - 200 TB unit	
7050	OEL - inactive	
7051	OEL - 1 unit	
7052	OEL - 5 unit	
7053	OEL - 10 unit	
7054	OEL - 25 unit	
7055	OEL - 50 unit	
7060	OEL - 100 unit	
7065	OEL - 200 unit	
7091	FICON indicator	
7092	High Performance FICON	
Note: In China, feature code 7090 is no longer available for hardware machine type 2423.		

Parallel access volumes (239x Model LFA, PAV license; 242x machine type)

The parallel access volumes (PAV) features establish the extent of IBM authorization for the use of the parallel access volumes licensed function.

Feature codes for parallel access volume

When you order the parallel access volume (PAV) function, you must specify the feature code that represents the physical capacity allowed for the function.

A license is required for the total physical capacity in the storage unit that is configured as count key data (CKD). The total authorization level must be greater than or equal to the total physical capacity of the unit.

Table 38 on page 101 provides the feature codes for the PAV function.

Note: If you currently have an active PAV feature, and you replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 38. Parallel access volume (PAV) feature codes

Feature code	Description	Hardware models
7820	PAV - Inactive	961
7821	PAV - 1 TB unit	
7822	PAV - 5 TB unit	
7823	PAV - 10 TB unit	
7824	PAV - 25 TB unit	
7825	PAV - 50 TB unit	
7830	PAV - 100 TB unit	
7899	HyperPAV	

IBM HyperPAV (242x Model PAV and 239x Model LFA, PAV license)

You can add the optional IBM HyperPAV feature to any licensed parallel access volume (PAV) feature.

IBM HyperPAV can be enabled only if PAV is enabled on the storage image. The IBM HyperPAV feature is available for a single charge (flat fee) regardless of the extent of IBM authorization that you have for the corresponding PAV feature. “Ordering rules for licensed functions” on page 96 describes any further ordering requirements for this feature.

Feature code for IBM HyperPAV

Use the IBM HyperPAV feature code when you add the IBM HyperPAV function to an existing or new parallel access volumes (PAV) function on a storage unit.

7899 IBM HyperPAV (all hardware models)

IBM System Storage Easy Tier

Support for IBM System Storage Easy Tier is available with the IBM System Storage Easy Tier licensed feature indicator 0713 and corresponding DS8870 Function Authorization (239x-LFA) feature number 7083.

The Easy Tier license feature enables the following modes:

- Easy Tier: automatic mode
- Easy Tier: manual mode

The license feature enables the following functions for the storage type:

- The capability to migrate volumes for logical volumes
- The reconfigure extent pool function of the extent pool
- The dynamic extent relocation with an Easy Tier managed extent pool

The Easy Tier LIC feature key contains a storage-type indication that determines the type of storage for which the key is applicable. It also contains an allowed capacity value. This value refers to the total amount of physical capacity configured into any real rank of the specified storage types on the storage facility image. The allowed capacity is required to be set to either 0 or to the maximum value, indicating whether the LIC feature is on or off.

To validate an Easy Tier LIC feature key, the allowed capacity indication must meet all of the following criteria:

- The specified storage type must be fixed block (FB) or count key data (CKD).
- The specified capacity must be either zero or the maximum capacity value.

When an Easy Tier LIC feature key is installed, if the Easy Tier functions are not enabled and the license feature key has a capacity greater than 0 bytes, then the storage facility image enables the Easy Tier functions.

If the LIC feature key that is disabled, while the Easy Tier functions are enabled, the disabled LIC feature key is accepted and the Easy Tier functions are disabled immediately. Any extent migrations that were in progress during disablement are either nullified or completed. Any extent migrations queued later are stopped and any requests to initiate a volume migration or an extent pool reconfiguration are rejected.

Point-in-time copy function (239x Model LFA, PTC license) and FlashCopy SE Model SE function (239x Model LFA, SE license)

The point-in-time copy licensed function model and features establish the extent of IBM authorization for the use of the point-in-time copy licensed function on your storage unit.

The IBM System Storage FlashCopy function is a point-in-time licensed function.

Feature codes for point-in-time copy

When a point-in-time copy function is ordered, you must specify the license feature code that represents the physical capacity you want to authorize for that function.

The point-in-time copy (PTC) license feature codes enable the use of the point-in-time copy licensed function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need 23 TB of point-in-time capacity, you can order two 7253 features and three 7251 features.

Table 39 on page 103 provides the feature codes for the point-in-time copy function.

Note: If you have an active point-in-time feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 39. Point-in-time copy (PTC) feature codes

Feature code	Description	Hardware models
7250	PTC - Inactive	961
7251	PTC - 1 TB unit	
7252	PTC - 5 TB unit	
7253	PTC - 10 TB unit	
7254	PTC - 25 TB unit	
7255	PTC - 50 TB unit	
7260	PTC - 100 TB unit	

Feature codes for FlashCopy SE

When you order FlashCopy SE function, you specify the feature code that represents the physical capacity you want to authorize for the function.

The FlashCopy SE license feature codes enable the use of the FlashCopy SE licensed function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

You can combine feature codes to order the exact capacity that you need.

Note: If you have an active point-in-time feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 40 provides the feature codes for the FlashCopy SE function.

Note: If you have an active FlashCopy SE feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 40. FlashCopy SE feature codes

Feature code	Description	Hardware models
7350	SE - Inactive	961
7351	SE - 1 TB unit	
7352	SE - 5 TB unit	
7353	SE - 10 TB unit	
7354	SE - 25 TB unit	
7355	SE - 50 TB unit	
7360	SE - 100 TB unit	

Remote mirror and copy functions (242x Model RMC and 239x Model LFA)

The remote mirror and copy licensed function model and features establish the extent of IBM authorization for the use of the remote mirror and copy licensed functions on your storage unit.

The following functions are remote mirror and copy licensed functions:

- Metro Mirror (formerly Synchronous PPRC)
- Global Mirror (formerly Asynchronous PPRC)
- Global Copy (formerly PPRC Extended Distance)
- Metro/Global Mirror

Feature codes for remote mirror and copy

When you order remote mirror and copy functions, you must specify the feature code that represents the physical capacity to authorize for the function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

The remote mirror and copy license feature codes enable the use of the following remote mirror and copy (RMC) licensed functions:

- IBM System Storage Metro Mirror (MM)
- IBM System Storage Global Mirror (GM)
- IBM System Storage Metro Global Mirror (MGM)

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need a function authorization for 35 TB of remote mirror and copy capacity, you would order one 7504 feature and one 7503 feature.

Note: If you have an active remote mirror and copy feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 41 on page 105 provides the feature codes for the remote mirror and copy functions.

Table 41. Remote mirror and copy (RMC) feature codes

Feature code	Description	Hardware models
7480	MGM - inactive	961
7481	MGM - 1 TB unit	
7482	MGM - 5 TB unit	
7483	MGM - 10 TB unit	
7484	MGM - 25 TB unit	
7485	MGM - 50 TB unit	
7490	MGM - 100 TB unit	
7500	MM - Inactive	
7501	MM - 1 TB unit	
7502	MM - 5 TB unit	
7503	MM - 10 TB unit	
7504	MM - 25 TB unit	
7505	MM - 50 TB unit	
7510	MM - 100 TB unit	
7520	GM - Inactive	
7521	GM - 1 TB unit	
7522	GM - 5 TB unit	
7523	GM - 10 TB unit	
7524	GM - 25 TB unit	
7525	GM - 50 TB unit	
7530	GM - 100 TB unit	
7650	RMZ - Inactive	961
7651	RMZ - 1 TB	
7652	RMZ - 5 TB	
7653	RMZ - 10 TB	
7654	RMZ - 25 TB	
7655	RMZ - 50 TB	
7660	RMZ - 100 TB	

Feature codes for I/O Priority Manager

When you order I/O Priority Manager functions, you specify the feature code that represents the physical capacity to authorize for the function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need a function authorization for 35 TB of I/O Priority Manager capacity, you would order one 7843 feature and one 7844 feature.

Table 42 provides the feature codes for the I/O Priority Manager functions.

Table 42. I/O Priority Manager feature codes

Feature code	Description	Hardware models
7840	I/O Priority Manager - Inactive	961
7841	I/O Priority Manager - 1 TB Indicator	
7842	I/O Priority Manager - 5 TB Indicator	
7843	I/O Priority Manager - 10 TB Indicator	
7844	I/O Priority Manager - 25 TB Indicator	
7845	I/O Priority Manager - 50 TB Indicator	
7850	I/O Priority Manager - 100 TB Indicator	

z/OS licensed features

This section describes z/OS licensed features supported on the DS8000.

Remote mirror for z/OS (242x Model RMZ and 239x Model LFA, RMZ license)

The remote mirror for z/OS licensed function model and features establish the extent of IBM authorization for the use of the z/OS remote mirroring licensed function on your storage unit.

The IBM System Storage z/OS Global Mirror function is a z/OS remote mirroring licensed function.

Feature codes for z/OS Global Mirror

When you order the z/OS Global Mirror function, you must specify the feature code that represents the physical capacity you want to authorize for this function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need 30 TB of capacity, you would order one 7654 feature and one 7652 feature.

Note: If you have an active z/OS Global Mirror feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 43 on page 107 provides the feature codes for remote mirror for System z functions.

Table 43. Remote mirror for System z (RMZ) feature codes

Feature code	Description	Hardware models
7650	RMZ - Inactive	961
7651	RMZ - 1 TB unit	
7652	RMZ - 5 TB unit	
7653	RMZ - 10 TB unit	
7654	RMZ - 25 TB unit	
7655	RMZ - 50 TB unit	
7660	RMZ - 100 TB unit	

Feature codes for z/OS Metro/Global Mirror Incremental Resync (RMZ Resync)

When you order the z/OS Metro/Global Mirror function, you must specify the feature code that represents the physical capacity you are authorizing for the function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

You can combine feature codes to order the exact capacity that you need. For example, if you determine that you need 30 TB of capacity, you would order one 7684 feature and one 7682 feature.

Note: If you have an active z/OS Metro/Global Mirror feature and replace it with an inactive feature, but later want to use the feature again, adhere to the requirements for deleting an active license.

Table 44 provides the feature codes for z/OS Metro/Global Mirror Incremental Resync (RMZ Resync) System z functions.

Table 44. z/OS Metro/Global Mirror Incremental Resync (RMZ Resync) for System z feature codes

Feature code	Description	Hardware models
7680	RMZ resync - Inactive	961
7681	RMZ resync - 1 TB unit	
7682	RMZ resync - 5 TB unit	
7683	RMZ resync - 10 TB unit	
7684	RMZ resync - 25 TB unit	
7685	RMZ resync - 50 TB unit	
7690	RMZ resync - 100 TB unit	

z/OS Distributed Data Backup

z/OS Distributed Data Backup (zDDB) is an optional licensed feature on Model 961 that allows hosts, attached through a FICON or ESCON interface, to access data on fixed block (FB) volumes through a device address on FICON or ESCON interfaces.

If the zDDB LIC feature key is installed and enabled and a volume group type specifies either FICON or ESCON interfaces, this volume group has implicit access to all FB logical volumes that are configured in addition to all CKD volumes specified in the volume group. Then, with appropriate software, a z/OS host can perform backup and restore functions for FB logical volumes configured on a storage facility image for open systems hosts.

The hierarchical storage management (DFSMS-HSM) function of the z/OS operating system can manage data that is backed up. If you have not installed or enabled the zDDB LIC feature key, during a DS8000 power on sequence, the logical volumes and the LSSs that are associated with this licensed feature are offline to any FICON or ESCON interfaces. If a zDDB LIC feature key is disabled when it was previously enabled, the logical volumes and the LSSs that are associated with the licensed features remain online to any FICON or ESCON interfaces until the next power off sequence, but any I/O issued to these logical volumes is rejected.

The key data in a zDDB LIC feature key contains an allowed capacity value. This value refers to the total amount of physical capacity configured into any FB real rank on the storage facility image. The allowed capacity is required to be set to either 0 or to the maximum value, which the LIC feature is on or off.

To validate a zDDB feature key, the new LIC key must meet the following criteria:

- The specified storage type must be FB storage only
- The specified capacity is either zero or the maximum capacity value

When a zDDB LIC feature key is installed and the LIC feature key has a capacity greater than 0 bytes, then the DS8000 enables the zDDB function and notifies any attached hosts through the appropriate interface. If a zDDB LIC feature key that is disabled is installed while the zDDB facility is enabled, the LIC feature key is accepted, but the zDDB facility is concurrently disabled. While the feature is disabled, logical volumes that are associated with this feature are either offline to FICON or ESCON hosts or I/O issued to logical volumes associated with the feature are rejected on FICON or ESCON interfaces.

Feature codes for z/OS Distributed Data Backup

Use either of these optional z/OS Distributed Data Backup feature codes to enable data backup of open systems from distributed server platforms through a System z host.

Table 45. License z/OS Distributed Data Backup function indicator

License function	Hardware machine type 239x indicator feature	Hardware machine type 242x indicator feature
z/OS Distributed Data Backup Indicator	7094	Model LFA 7094

Thin provisioning LIC key feature

To use the thin provisioning facility with extent space-efficient logical volumes, you must have the thin provisioning LIC feature key.

The thin provisioning LIC feature enables the following functions for the storage type that is indicated by the LIC feature key:

- The creation of extent space-efficient logical volumes

- The creation of virtual ranks

The thin provisioning LIC feature key data contains the following information:

- A storage-type indication that determines the type of storage that is applicable for the LIC feature key
- A capacity value that refers to the total amount of physical capacity that is configured into any real rank for the storage types on the storage facility image

For the thin provisioning LIC feature key to be valid, the capacity value must meet all of the following criteria:

- The specified storage type must be fixed block (FB)
- The specified capacity must be either zero or the maximum capacity value

The support of FB thin provisioning depends on the model. If thin provisioning is not supported on all supported storage types, the LIC feature key must still indicate both storage types. A request to create either an extent space-efficient logical volume or a virtual rank in a storage type that is not supported is rejected. Subsequent changes to storage types that are supported do not require a new LIC feature key to be installed. Support of thin provisioning is only indicated to the host types that access storage types that provide support for thin provisioning.

When a thin provisioning LIC feature key is installed, if the thin provisioning facility is not currently enabled and the LIC feature key has a capacity greater than 0 bytes, the storage facility image enables the thin provisioning facility and notifies any attached hosts through the appropriate interface protocol to single this condition. If there are one or more extent space-efficient logical volumes configured on the storage facility image and the installed LIC feature key is disabled while the thin provisioning facility is enabled, the LIC feature key is rejected. Otherwise, the following occurs:

- The disablement LIC feature key is accepted
- The thin provisioning facility is immediately disabled
- Any capabilities that were previously enabled for the thin provisioning facility are disabled

  Note: If a capability is enabled by some other LIC feature key, it remains enabled.
- All attached hosts are notified through the appropriate interface protocol that the thin provisioning facility is disabled

If configuration-based enforcement is in effect while the thin provisioning facility is enabled by a LIC feature key, the configuration of additional real ranks of the specified storage types is suppressed on the storage facility image if the resulting storage facility image physical capacity of the specified storage types can exceed the amount that is allowed by the LIC feature key.

Feature codes for thin provisioning

Use either of these feature codes when you add the IBM System Storage DS8000 Thin Provisioning function to an existing or new storage unit.

Table 46. License function indicators for the Thin Provisioning feature

License function	Hardware machine type 239x indicator feature	Hardware machine type 242x indicator feature
Thin Provisioning Indicator	7071	0707

Chapter 6. Meeting DS8000 series delivery and installation requirements

You must ensure that you properly plan for the delivery and installation of your DS8000 storage unit.

This chapter provides the following planning information for the delivery and installation of your DS8000 storage unit:

- Planning for delivery of your storage unit
- Planning the physical installation site
- Planning for power requirements
- Planning for network and communication requirements
- Energy savings

For more information about the equipment and documents that IBM includes with DS8000 series models, see Appendix C, “IBM-provided DS8000 equipment and documents,” on page 177.

Delivery requirements

Before you receive your DS8000 shipment, ensure that you meet all delivery requirements.

The topics in this section help you ensure that you select a site that meets all requirements.

Attention: Customers can prepare their environments to accept the new product based on the installation planning information with assistance from an IBM Advanced Technical Services (ATS) representative or an IBM authorized service provider. In anticipation of the equipment delivery, the final installation site must be prepared in advance so that professional movers can transport the equipment to the final installation site within the computer room. If this preparation is not possible at the time of delivery, customers must make arrangements to have the professional movers return to finish the transportation at a later date. Professional movers must transport the equipment. The IBM authorized service provider only performs minimal frame repositioning within the computer room, as needed, to perform required service actions. Customers are also responsible for using professional movers in the case of equipment relocation or disposal.

Receiving delivery

The shipping carrier is responsible for delivering and unloading the DS8000 series model as close to its final destination as possible. You must ensure that your loading ramp and your receiving area can accommodate your DS8000 shipment.

Use the following steps to ensure that your receiving area and loading ramp can safely accommodate the delivery of your storage unit:

1. Find out the packaged weight and dimensions of the DS8000 container and other containers of your shipment.
2. Ensure that your loading dock, receiving area, and elevators can safely support the packaged weight and dimensions of the shipping containers.

Note: You can order a weight-reduced shipment of a DS8000 model when a configured model exceeds the weight capability of the receiving area at your site.

3. To compensate for the weight of the DS8000 shipment, ensure that the loading ramp at your site does not exceed an angle of 10°. (See Figure 15.)

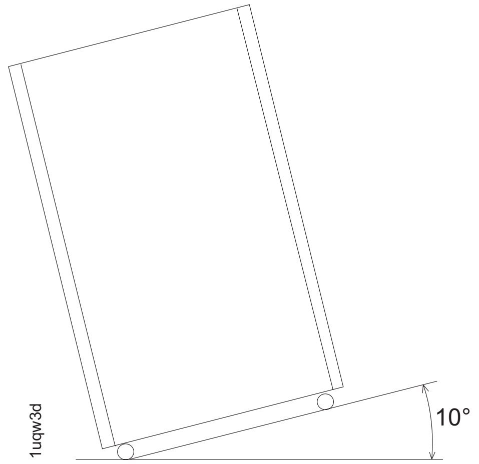


Figure 15. Maximum tilt for a packed unit is 10°

Shipment weights and dimensions

To help you plan for the delivery of your storage unit, you must ensure that your loading dock and receiving area can support the weight and dimensions of the packaged DS8000 shipments.

You receive at least two, and up to three, shipping containers for each DS8000 model that you order. You always receive the following items:

- A container with the DS8000 model. In the People's Republic of China (including Hong Kong S.A.R. of China), India, and Brazil, this container is a wooden crate. In all other countries, this container is a pallet covered by a corrugated fiberboard (cardboard) cover.
- A container with the remaining ship group items, such as power cords, CDs, and other ordered features or peripherals for your model.

If ordered, you also receive the following container:

- A container with the external management consoles (MCs).

Table 47 on page 113 shows the final packaged dimensions and maximum packaged weight of the storage unit shipments.

To calculate the weight of your total shipment, add the weight of each model container and the weight of one ship group container for each model. If you ordered any external management consoles, add the weight of those containers, as well.

Table 47. Packaged dimensions and weight for DS8000 models (all countries)

Shipping container	Packaged dimensions (in centimeters and inches)	Maximum packaged weight (in kilograms and pounds)
Model 961	**Height** 207.5 cm (81.7 in.) **Width** 101.5 cm (40 in.) **Depth** 137.5 cm (54.2 in.)	1325 kg (2920 lb)
Model 961E	**Height** 207.5 cm (81.7 in.) **Width** 101.5 cm (40 in.) **Depth** 137.5 cm (54.2 in.)	1311 kg (2890 lb)
External MC container (when ordered)	**Height** 69.0 cm (27.2 in.) **Width** 80.0 cm (31.5 in.) **Depth** 120.0 cm (47.3 in.)	75 kg (165 lb)
Note: With an overhead cabling option (top exit bracket, feature code 1400) installed on the base model, an additional 10.16 cm (4 inches) are added to the standard, packaged height of the base model. This increases the total height of the model to 87.6 cm (217.5 inches).		

CAUTION:
A fully configured model in the packaging can weigh over 1406 kg (3100 lb).

Installation site requirements

You must ensure that the location where you plan to install your DS8000 storage units meets all requirements.

The topics in this section can help you ensure that you select a site that meets all requirements.

Planning for floor and space requirements

Ensure that the location of your DS8000 storage units meets space and floor requirements. Decide if your storage unit is to be installed on a raised or nonraised floor.

When you are planning the location of your storage units, you must answer the following questions that relate to floor types, floor loads, and space:

- Will you install on a raised or nonraised floor? For example, nonraised floors using a top exit for cabling have special requirements and specific cable lengths.
- If the planned location has a raised floor, does the floor require preparation (such as cutting out tiles) to accommodate cable entry into the units?
- Does the floor of the location meet floor load requirements?
- Can the location accommodate the amount of space that is required by the storage units, and does the space size meet the following criteria?
  - Weight distribution area that is needed to meet floor load requirements
  - Service clearance requirements

Use the following steps to ensure that your planned installation location meets space and floor load requirements:

1. Identify the base models and expansion models that are included in your storage units. If your storage units use external management consoles, include the racks containing the external management consoles.
2. Decide whether to install the storage units on a raised or nonraised floor.
   a. If the location has a raised floor, plan where the floor tiles must be cut to accommodate the cables.
   b. If the location has a nonraised floor, resolve any safety problems, and any special equipment considerations, caused by the location of cable exits and routing.
3. Determine whether the floor of the location meets the floor load requirements for the storage units.
4. Calculate the amount of space to be used by the storage units.
   a. Identify the total amount of space that is needed for the storage units using the dimensions of models and the weight distribution areas calculated in step 3.
   b. Ensure that the area around each standalone model and each storage unit meets the service clearance requirements.

   Note: Any expansion units within the storage unit must be attached to the base model on the right side (as you face the front of the units).

Installing on raised or nonraised floors

You can install your DS8000 storage units on a raised or nonraised floor. Raised floors can provide better cooling than nonraised floors unless optional overhead cable management is used.

Raised floor considerations

Installing the models on a raised floor provides the following benefits:

- Improves operational efficiency and allows greater flexibility in the arrangement of equipment.
- Increases air circulation for better cooling.
- Protects the interconnecting cables and power receptacles.
- Prevents tripping hazards because cables can be routed underneath the raised floor.

When you install a raised floor, consider the following factors:

- The raised floor must be constructed of fire-resistant or noncombustible material.

- Avoid the exposure of metal or highly conductive material at ground potential to the walking surface when a metallic raised floor structure is used. Such exposure is considered an electrical safety hazard.
- The raised floor height must be at least 30.5 cm (12 in.). For processors with multiple channels, a minimum raised floor height of 45.7 cm (18 in.) is required. Clearance must be adequate to accommodate interconnecting cables, Fibre Channel cable raceways, power distribution, and any piping that is present under the floor. Floors with greater raised floor heights allow for better equipment cooling.
- When a raised floor tile is cut for cable entry or air supply, an additional floor tile support (pedestal) might be required to restore the structural integrity of the panel to the previous requirement.
- The use of a protective covering (such as plywood, tempered masonite, or plyron) is required to prevent damage to floor tiles, carpeting, and panels while equipment is being moved into or is relocated within the installation. When the equipment is moved, the dynamic load on the casters is greater than when the equipment is stationary.
- Concrete subfloors require treatment to prevent the release of dust.
- Use noncombustible protective molding to eliminate sharp edges on all floor cutouts, to prevent damage to cables and hoses, and to prevent casters from rolling into the floor cutout.
- Seal raised floor cable openings to prevent chilled air that is not used to directly cool the equipment from escaping.
- Pedestals must be firmly attached to the structural (concrete) floor using an adhesive.

Nonraised floor considerations

Raised flooring is best but an overhead cabling option is available for the DS8870 (Model 961), which is the top exit bracket for Fibre cable. This feature can be used on nonraised floors. Follow the special considerations and installation guidelines as described in the sections about overhead cable management.

Overhead cable management (top exit)

An overhead cabling feature (top exit) is available for models in the DS8000 series.

Overhead cabling (top exit) is an optional feature and includes a top exit bracket for managing your cables. This feature is an alternative to the standard, rear cable exit. Using overhead cabling provides many of the cooling and safety benefits provided by raised flooring in a nonraised floor environment. Unlike raised-floor cabling, the installation planning, cable length, and the machine location in relation to the cable entry point are critical to the successful installation of a top cable exit.

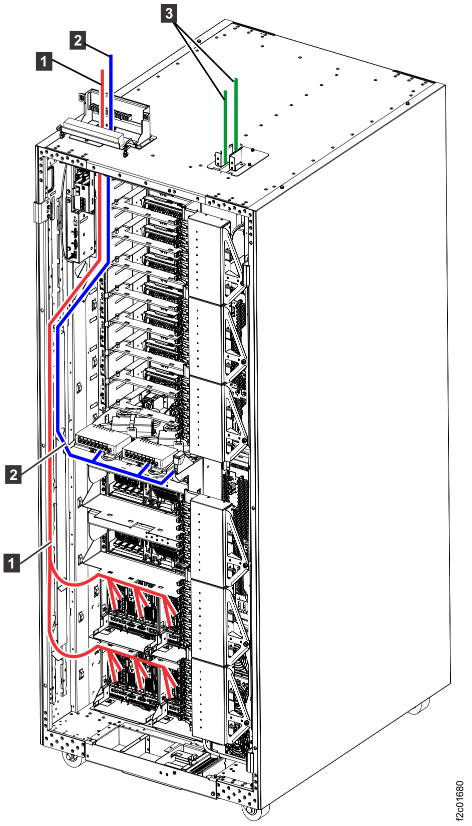


Figure 16. DS8000 with top exit feature installed (cable routing and top exit locations)

Figure 16 illustrates the location of the cabling for the top exit bracket for Fibre cable feature. When you order a top exit feature, the feature includes clamping hardware, internal cable routing brackets for rack 1 or rack 2, and two top exit mainline power cords for each rack. The following notes provide more information about the color-coded cable routing and components in Figure 16.

1 Customer Fibre Channel host cables. The Fibre Channel host cables, shown in red, are routed from the top of the rack down to I/O enclosure host adapter cards.

2 Network Ethernet cable and customer analog phone line (if used). The network Ethernet cable, in blue, is routed from the top of rack to rack's rear connector. The rack connector has an internal cable to the HMC. DS8000 private network Ethernet cables (two, one gray and one black) for another storage facility (if installed) are also located here.

3 Mainline power cords. Two top exit mainline power cords for each rack, shown in green, are routed here.

Notes:

- Power cords are routed to the rack by the customer.
- Fibre Channel host cables are internally routed and connected by either the customer or by an IBM service representative.
- All remaining cables are internally routed and connected by an IBM service representative.

Feature Codes for overhead cabling (top exit bracket)

Use the following feature code information when ordering this option.

Table 48. Feature codes for overhead cable option (top exit bracket)

Feature Code	Description
1400	Top exit bracket for Fibre cable
Note: In addition to the top exit bracket and top exit power cords, one universal ladder (Feature code 1101) must also be purchased for a site where the top exit bracket for Fibre cable feature is used. The universal ladder is used to ensure safe access when a DS8000 unit is serviced with a top exit bracket feature installed.	

Installation and safety requirements

For example, if the cables are too long, there will not be enough room inside of the unit to handle the extra length or they will interfere with the service process, preventing concurrent repair. This new option has the following specifications and limitations you must consider prior to ordering:

- In contrast to the raised-floor power cords, which have a length from the tailgate to the connector of about 16 feet, the length of the top exit power cords are only 6 feet from the top of the unit.
- IBM Corporate Safety restricts the servicing of your overhead equipment to a maximum of 10 feet from the floor. Therefore, your power source must not exceed 10 feet from the floor and must be within 5 feet of the top of the power cord exit gate. Servicing any overhead equipment higher than 10 feet requires a special bid contract. Contact your IBM Representative for more information on special bids.
- In order to meet safety regulations in servicing your overhead equipment, you must purchase a minimum of one feature code 1101 for your top exit bracket feature per site. This feature code provides a safety-approved 8-foot platform ladder, which is required to service feature codes 1072, 1073, 1083, 1084, and 1400. This provides SSRs the ability to perform power safety checks and other service activities on the top of your unit. Without this approved ladder, IBM SSRs are not able to install or service a unit with top cable exit features.
- To assist you with the host top exit cable routing, feature code 1400 provides a cable channel bracket, which mounts directly below the topside of the tailgate and its opening. Cables can be easily slid into the slots on its channels. The cable bracket directs the cables behind the rack ID card and towards the rear, where the cables drop vertically into a second channel, which mounts on the left-side wall (when viewing the unit from the rear). There are openings in the vertical channel for cables to exit toward the I/O drawers.

Accommodating cables

You must ensure that the location and dimensions of the cable cutouts for the models can be accommodated by the installation location. An overhead cable management option (top exit bracket) is available for DS8870 (Models 961, 96E), which have special planning and safety requirements.

Use the following steps to ensure that you prepare for cabling for each unit:

1. Based on your planned storage unit layout, ensure that you can accommodate the locations of the cables exiting each unit.

   See Figure 17 for the cable cutouts for the DS8870.

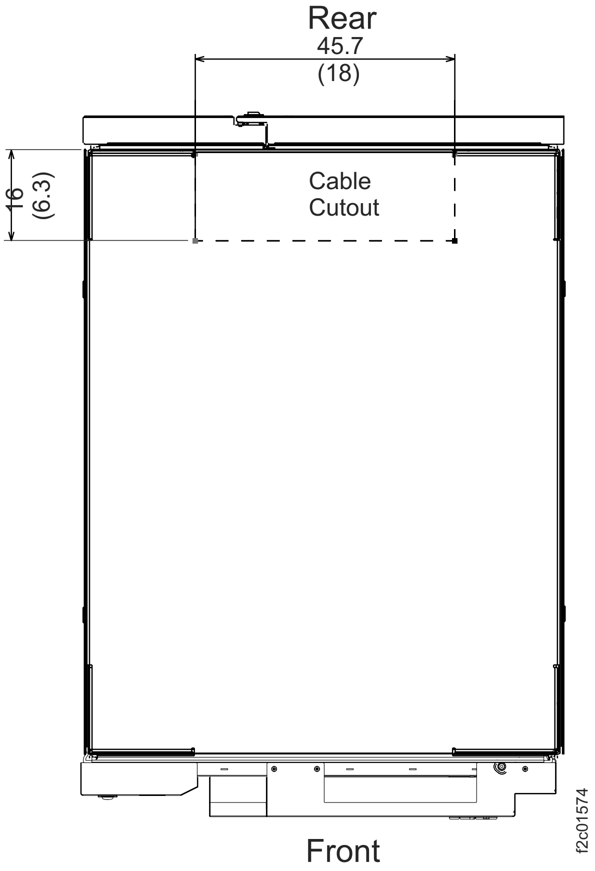


Figure 17. Cable cutouts for a DS8870

2. If you install the storage units on a raised floor, use the following measurements when you cut the floor tile for the cabling:
   - Width: 45.7 cm (18.0 in.)
   - Depth: 16 cm (6.3 in.)

   Note: If both rack 1 and 2 use an overhead cable management (top exit bracket) feature for the power cords and communication cables, the PCIe and SPCN cables can be routed under the rack, on top of the raised floor. This is the same routing used for nonraised floor installations. There is room under the racks to coil extra cable length and prevent the need for custom floor tile cutouts. Also, racks 3 and 4 do not need floor tile cutouts when the top exit bracket feature is installed as only routing for power cords is needed.

Nonraised floors with overhead cable management

Raised floors are recommended to provide better support for the cabling needed by the storage units, and to ensure you have efficient cooling for your units. However, for the DS8870 (Model 961) an option is available for overhead cabling (the top exit bracket feature), which provides many benefits for nonraised floor installations. Unlike raised-floor cabling, the installation planning, cable length, and the machine location in relation to the cable entry point are quite critical to the successful installation of a top exit bracket feature. Measurements for this feature are given in Figure 18. You can find critical safety, service, and installation considerations for this feature in the area discussing overhead cable management.

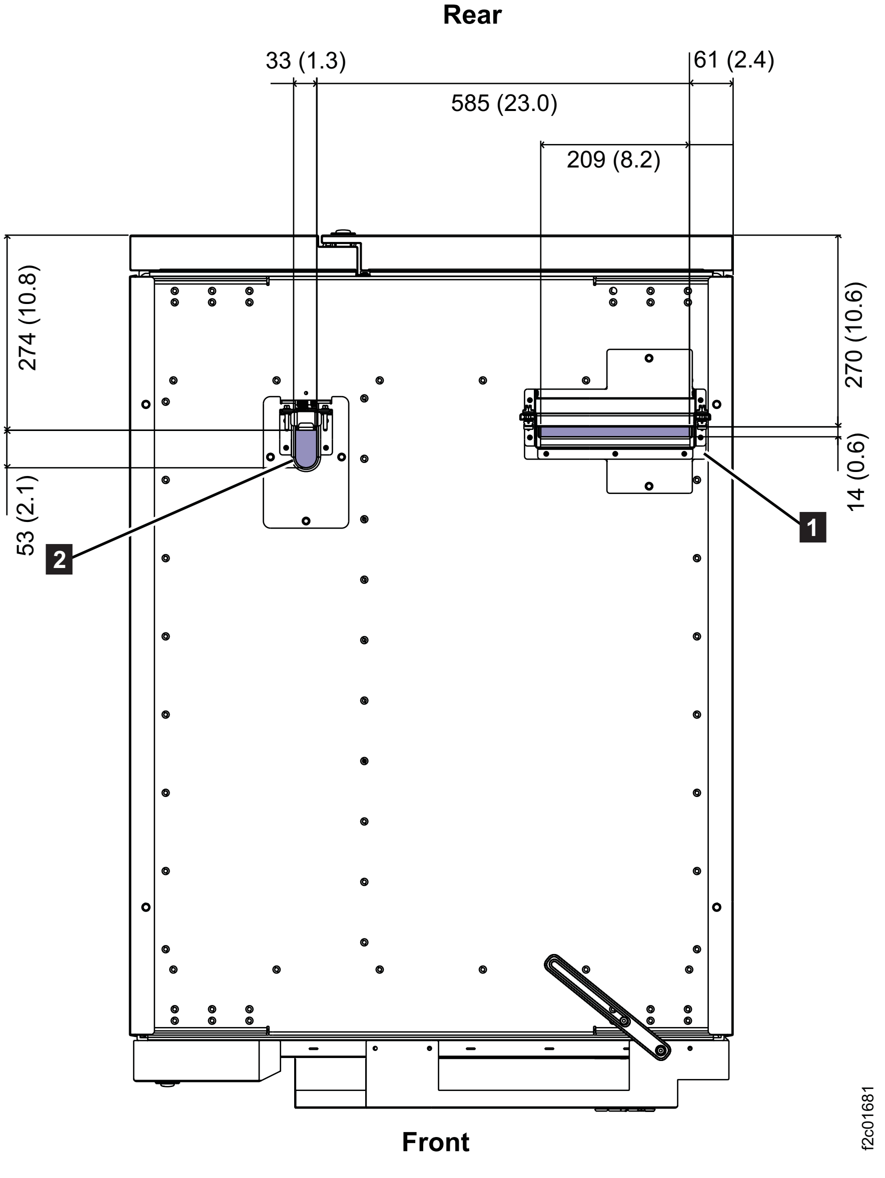


Figure 18. Measurements for DS8000 placement with top exit bracket feature present

The following notes provide information about the labeled components in Figure 18:

1 Top exist bracket for Fibre cables

2 Top exit cable channel bracket

Meeting floor load requirements

It is important for your location to meet floor load requirements.

Use the following steps to ensure that your location meets the floor load requirements and to determine the weight distribution area required for the floor load:

1. Find out the floor load rating of the location where you plan to install the storage units.

   Important: If you do not know or are not certain about the floor load rating of the installation site, be sure to check with the building engineer or another appropriate person.
2. Determine whether the floor load rating of the location meets the following requirements:
   - The minimum floor load rating used by IBM is 342 kg per m² (70 lb. per ft²).
   - When you install a storage unit, which includes both base models and expansion models, the minimum floor load rating is 361 kg per m² (74 lb. per ft²). At 342 kg per m² (70 lb per ft²), the side dimension for the weight distribution area exceeds the 76.2 cm (30 in.) allowed maximum.
   - The per caster transferred weight to a raised floor panel is 450 kg (1000 lb.).
3. Using Table 49, complete the following steps for each storage unit.
   a. Find the rows that are associated with the storage unit.
   b. Locate the configuration row that corresponds with the floor load rating of the site.
   c. Identify the weight distribution area needed for that storage unit and floor load rating.

Table 49. Floor load ratings and required weight distribution areas

Configuration of storage unit (Note 1)	Total weight of configuration (Note 2)	Floor Load Rating, kg per m² (lb per ft²)	Weight Distribution Areas (Notes 3, 4, and 5)		
			Sides cm (in.)	Front cm (in.)	Rear cm (in.)
Model 961 (2-core)	1172 kg (2585 lb)	610 (125)	2.54 (1)	76.2 (30)	76.2 (30)
		488 (100)	17.8 (7)	76.2 (30)	76.2 (30)
		439 (90)	25.4 (10)	76.2 (30)	76.2 (30)
		342 (70)	55.9 (22)	76.2 (30)	76.2 (30)
Model 961 (4-core)	1324 kg (2920 lb)	610 (125)	7.62 (3)	76.2 (30)	76.2 (30)
		488 (100)	25.4 (10)	76.2 (30)	76.2 (30)
		439 (90)	35.6 (14)	76.2 (30)	76.2 (30)
		342 (70)	68.6 (27)	76.2 (30)	76.2 (30)
Model 961 and one 96E expansion model	2601 kg (5735 lb)	610 (125)	10.2 (4)	76.2 (30)	76.2 (30)
		488 (100)	43.2 (17)	76.2 (30)	76.2 (30)
		439 (90)	76.2 (30)	76.2 (30)	76.2 (30)
		410 (84)	76.2 (30)	76.2 (30)	76.2 (30)

Table 49. Floor load ratings and required weight distribution areas (continued)

Configuration of storage unit (Note 1)	Total weight of configuration (Note 2)	Floor Load Rating, kg per m^2 (lb per ft^2)	Weight Distribution Areas (Notes 3, 4, and 5)		
			Sides cm (in.)	Front cm (in.)	Rear cm (in.)
Model 961 and two 96E expansion models	3923 kg (8650 lb)	610 (125)	15.2 (6)	76.2 (30)	76.2 (30)
		488 (100)	63.5 (25)	76.2 (30)	76.2 (30)
		464 (95)	76.2 (30)	76.2 (30)	76.2 (30)

Notes:

1. A storage unit contains a base model and any expansion models associated with it.
2. Model 961 attaches to expansion model 96E. The expansion model weighs 123.2 kg (56 lb) fully populated and 2354 kg (5190 lb) combined with model 961.
3. Weight distribution areas cannot overlap.
4. Weight distribution areas are calculated for maximum weight of the models.
5. The base and expansion models of each storage unit are bolted to each other with 5-cm (2-in.) spacers. Move one side cover and mounting brackets from the base model to the side of the expansion model. Side clearance for racks that are bolted together applies to both sides of the assembled racks.

Note: Consult a structural engineer if you are unsure about the correct placement and weight distribution areas for your units.

Calculating space requirements

When you are planning the installation location, you must first calculate the total amount of space that is required for the storage units.

Perform the following steps to calculate the amount of space that is required for your storage units.

1. Determine the dimensions of each model configuration in your storage units.
2. Calculate the total area that is needed for model configuration by adding the weight distribution area to the dimensions determined from Table 49 on page 120.
3. Determine the total space that is needed for the storage units by planning the placement of each model configuration in the storage units and how much area each configuration requires based on step 2.
4. Verify that the planned space and layout also meets the service clearance requirements for each unit and system.

Dimensions and weight of individual models

When you are planning the floor and space requirements for your storage units, consider the dimensions and weights of the models that compose your storage units.

Table 50 on page 122 provides the dimensions and weights of the DS8000 models.

Table 50. DS8000 dimensions and weights

Model	Dimensions (see Note 1)	Maximum weight of fully configured base models and expansion models (see Notes 2 and 3)	Maximum weight of second expansion models (see Notes 2 and 4)
Model 961	**Height** 193.4 cm (76 in.) **Width** 84.8 cm (33.4 in.) **Depth** 122.7 (48.3 in.)	1324 kg (2920 lb)	N/A
Model 96E	**Height** 193.4 cm (76 in.) **Width** 84.8 cm (33.4 in.) **Depth** 122.7 (48.3 in.)	1265 kg (2790 lb)	1310 kg (2890 lb)

Notes:

1. These dimensions include casters and covers. (The casters are recessed and do not require extra clearance.)
2. Weight is in kilograms (kg) and pounds (lb).
3. Use this column for all base models and for an expansion model that can be fully configured with I/O enclosures and adapters. Expansion models can be fully configured only when they are attached to a 961 base model.
4. Use this column for the second expansion model that is attached to a 961.

Service clearance requirements

The service clearance area is the area around the storage unit that IBM service representatives need to service the unit.

CAUTION:
Servicing of this product or unit is to be performed by trained personnel only.

(C032)

For DS8000 models, IBM services representatives must open the front and rear covers to service the unit. Use the following minimum service clearances. (These dimensions are also shown on Figure 19 on page 123.)

- For the front of the unit, allow a minimum of 121.9 cm (48 in.) for the service clearance.
- For the rear of the unit, allow a minimum of 76.2 cm (30 in.) for the service clearance.
- For the sides of the unit, allow a minimum of 12.7 cm (5 in.) for the service clearance.

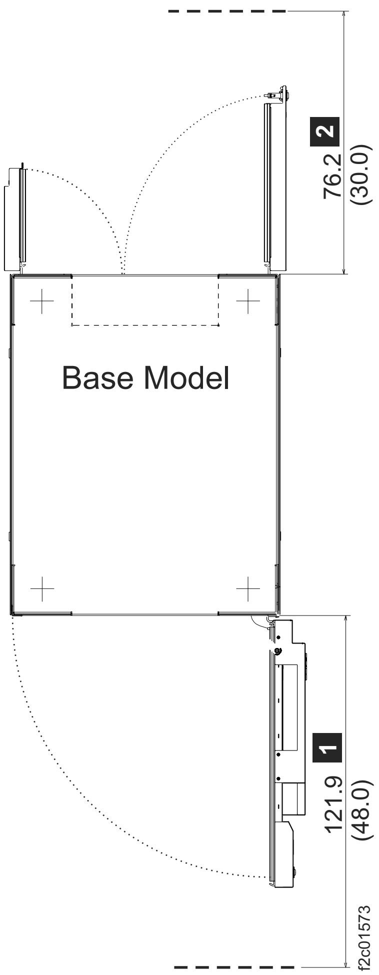


Figure 19. Service clearance requirements

Unlike weight distribution areas that are required to handle floor loading, keep in mind that service clearances of adjacent unrelated storage units can overlap.

Note: The terms *service clearance* and *weight distribution area* are often confused with each other. The service clearance is the area that is required to open the service covers and to pull out components for servicing. The weight distribution area is the area that is required to distribute the weight of the storage unit.

Earthquake Resistance Kit installation preparation

Before an IBM service representative can install the Earthquake Resistance Kit on any of your storage units racks, you must purchase fastening hardware and prepare the location where the kit is to be installed.

The required tasks that you must perform before the Earthquake Resistance Kit installation depends upon whether your storage unit sits on a raised or a nonraised floor. For either type of installation, work with a consultant or structural engineer to ensure that your site preparations meet the requirements.

The following list provides an overview of the preparations necessary for each type of floor:

Raised floor

- Cut the necessary holes and cable cutouts in the raised floor.
- Purchase and install eyebolt fasteners in the concrete floor.

Nonraised floor

Purchase and install fasteners in the concrete floor.

Further instructions for the preparation of your site for the Earthquake Resistance Kit are provided in “Preparing a raised floor for the Earthquake Resistance Kit installation” and “Preparing a nonraised floor for the Earthquake Resistance Kit” on page 127.

Preparing a raised floor for the Earthquake Resistance Kit installation:

You must prepare a raised floor as well as the concrete floor underneath before an Earthquake Resistance Kit can be installed on any of your storage units racks.

To ensure that you meet all site requirements, obtain the service of a qualified consultant or structural engineer to help you prepare the floor.

Figure 20 on page 125 provides an illustration of the Earthquake Resistance Kit after the IBM service representative installs it for a raised floor. Before the IBM service representative installs the kit, you must prepare the area shown as **2** in the figure.

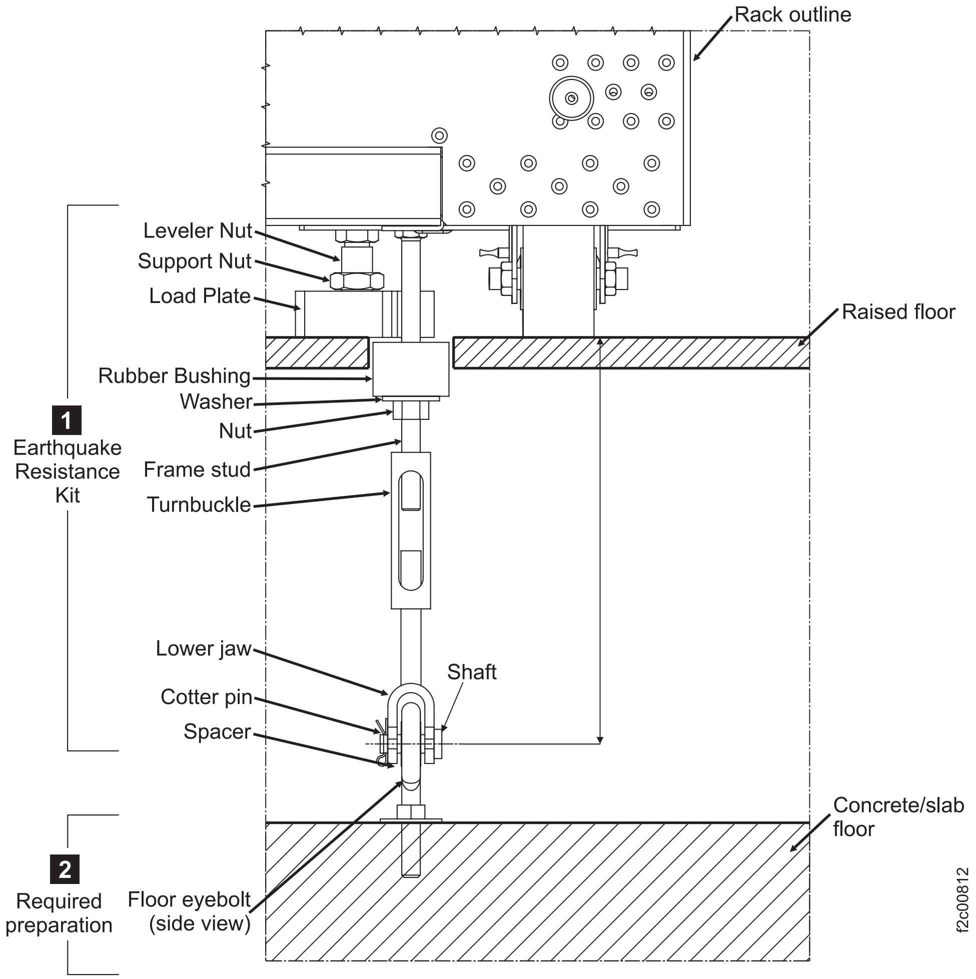


Figure 20. Earthquake Resistance Kit, as installed on a raised floor

Use the following steps to prepare your raised floor:

1. Cut the following openings in the raised floor for each rack that uses an Earthquake Resistance Kit:
   - Four holes for the rubber bushings of the kit to fit through the floor
   - One cable cutout for power and other cables that connect to the rack

   Use Figure 21 on page 126 as a guide for the location and dimensions of these openings.

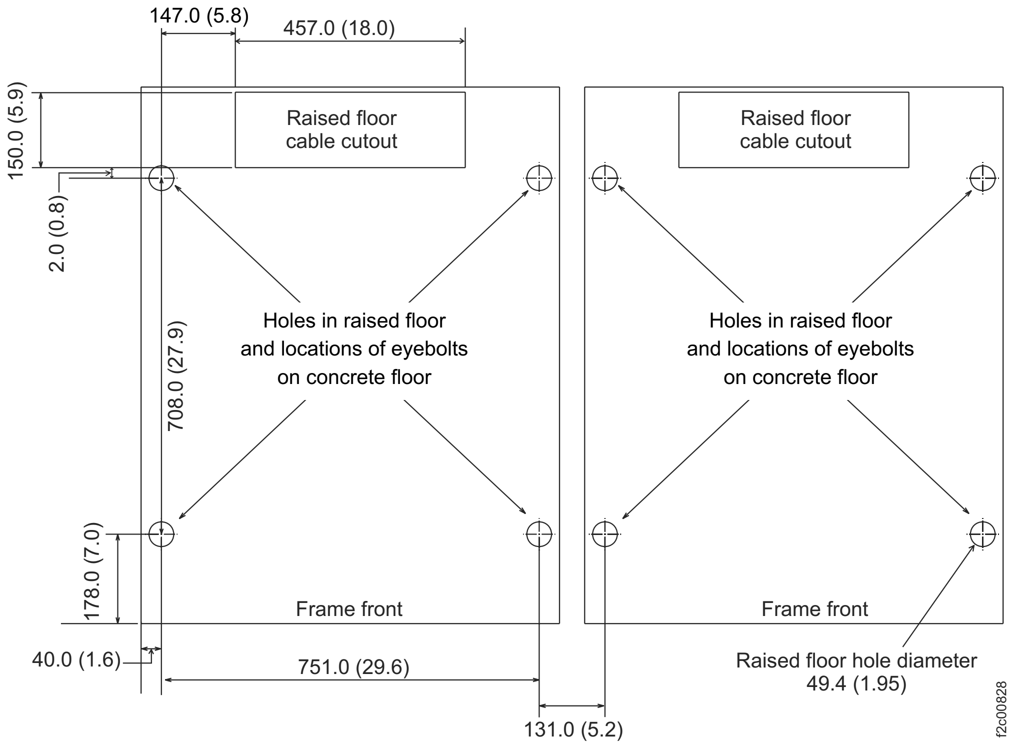

147.0 (5.8)
457.0 (18.0)
150.0 (5.9)
2.0 (0.8)
Raised floor cable cutout
Raised floor cable cutout
Holes in raised floor and locations of eyebolts on concrete floor
Holes in raised floor and locations of eyebolts on concrete floor
708.0 (27.9)
178.0 (7.0)
Frame front
Frame front
40.0 (1.6)
751.0 (29.6)
131.0 (5.2)
Raised floor hole diameter 49.4 (1.95)
f2c00828

Figure 21. Locations for the cable cutouts and rubber bushing holes in the raised floor and the eyebolt installation on the concrete floor. The pattern repeats for up to five models. Dimensions are in millimeters (inches).

2. Obtain four fasteners that are heavy duty concrete or slab floor eyebolts. These eyebolts are used to secure the Earthquake Resistance Kit. Work with your consultant or structural engineer to determine the correct eyebolts to use, but each eyebolt must meet the following specifications:
   - Each eyebolt must withstand 3600 lb pull force.
   - The dimensions of the eyebolt must allow the turnbuckle lower jaw of the kit to fit over the eyebolt (**1** on Figure 22 on page 127) and allow the spacer of Earthquake Resistance Kit to fit inside the eye (**2** on Figure 22 on page 127).

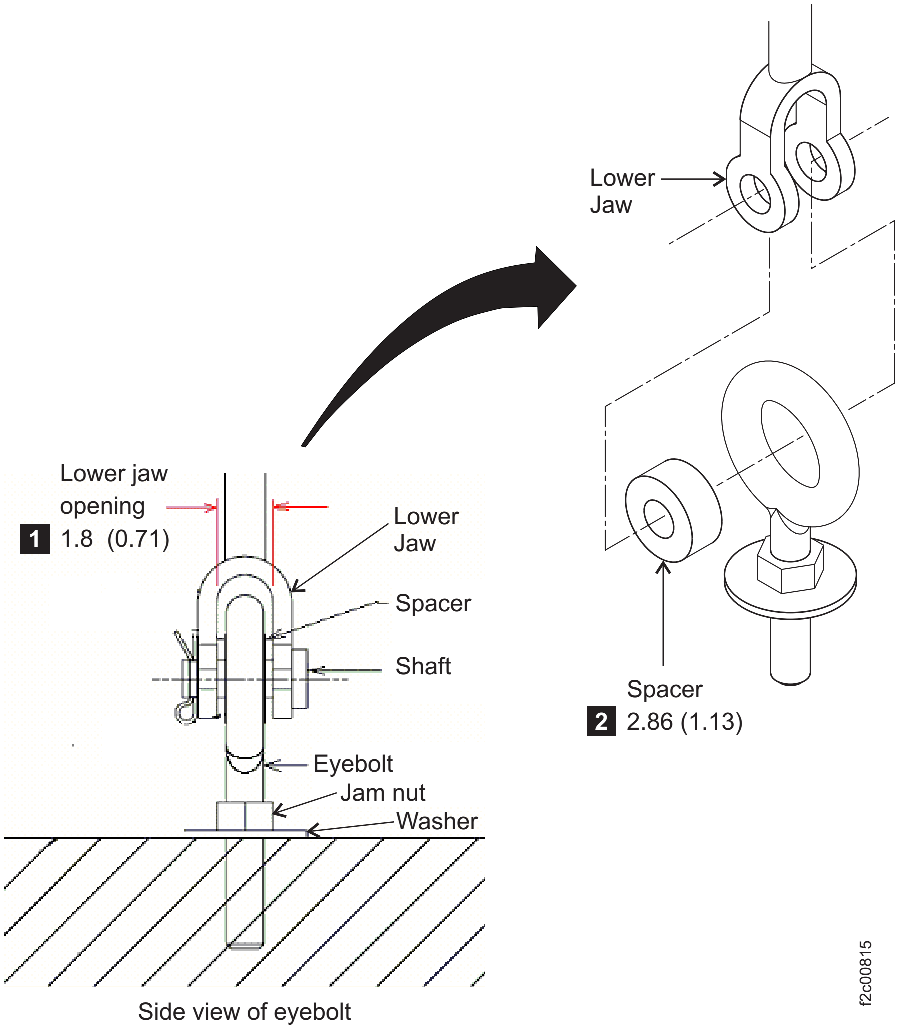


Figure 22. Eyebolt required dimensions. Dimensions are in millimeters (inches).

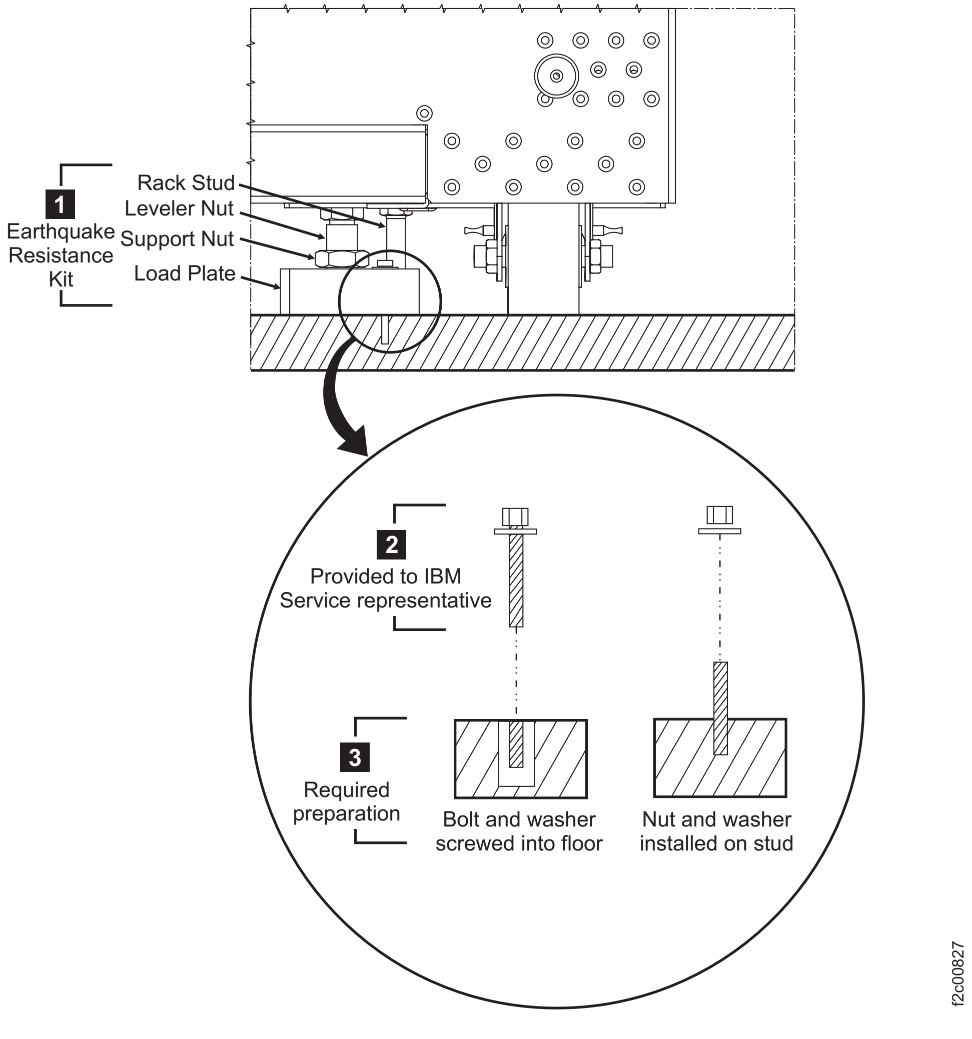
3. Install the eyebolt fasteners in the concrete floor using the following guidelines:
   - Use Figure 21 on page 126 to determine the placement of the eyebolts. The eyebolts must be installed so that they are directly below the holes that you cut in the raised floor for the rubber bushings.
   - Ensure that the installed eyebolts do not exceed a height of 101 mm (4 in.) from the floor to the center of the eye. This maximum height helps to reduce any bending of the eyebolt shaft.
   - Ensure that the installation allows the eyebolts to meet the required pull force after they are installed (3600 lb pull force for raised floor eyebolts).
   - If you use a threaded eyebolt that secures into a threaded insert in the floor, consider using a jam nut and washer on the shaft of the eyebolt. Talk to your consultant or structural engineer to determine whether a jam nut is necessary.

Preparing a nonraised floor for the Earthquake Resistance Kit:

You must prepare a nonraised floor before an Earthquake Resistance Kit can be installed on any of your storage units racks.

To ensure that you meet all site requirements, obtain the service of a qualified consultant or structural engineer to help you prepare the floor.

Figure 23 provides an illustration of the Earthquake Resistance Kit (**1** in the figure) after the IBM service representative installs it on the nonraised floor. Before the IBM service representative installs the kit, you must prepare the area shown as **3** in the figure.



1
Earthquake Resistance Kit
Rack Stud
Leveler Nut
Support Nut
Load Plate
2
Provided to IBM Service representative
3
Required preparation
Bolt and washer screwed into floor
Nut and washer installed on stud
f2c00827

Figure 23. Earthquake Resistance Kit, as installed on a nonraised floor. The detail shows two of the most common fasteners that you could use.

Use the following steps to prepare your nonraised floor:

1. Obtain six fastener sets for each rack that uses the Earthquake Resistance Kit. These fastener sets are used to secure the Earthquake Resistance Kit load plate. The type of fastener set that you use can be determined by your consultant or structural engineer. However, each bolt or stud must meet the following specifications:
   - Each fastener set must withstand 2400 lb pull force.
   - The fasteners must have a dimension that fits into the load plate holes, which are each 27 mm (1.0 in.) in diameter.
   - The fasteners must be long enough to extend through and securely fasten a load plate that is 30 mm (1.2 in.) thick. The fasteners must also be short

enough so that the height of the installed fastener does not exceed 65 mm (2.5 in.). This maximum height ensures that the fastener can fit under the rack.

The following examples provide descriptions of nonraised floor fastener sets:

- Threaded hole insert that is secured into the concrete floor and a bolt (with a washer) that screws into the insert
- Threaded stud that is secured into the concrete floor with a nut (with a washer) that screws over it

Figure 23 on page 128 shows illustrations of the example fastener sets.

2. Work with your consultant or structural engineer and use the following guidelines to install the fasteners in the concrete floor:
   - Use Figure 24 to determine the placement of the fasteners.
   - Ensure that the installed fasteners do not exceed a height of 65 mm (2.5 in.) from the floor. This maximum height ensures that the fastener can fit under the rack.
   - Ensure that the installation allows the fasteners to meet the required pull force after they are installed (2400 lb pull force).
   - If you use a threaded bolt that secures into a threaded insert in the floor and the bolt extends longer than 30 mm (1.2 in.), which is the thickness of the load plate, consider using a jam nut and a washer on the shaft of the bolt so that the load plate can be secured snugly to the floor. Talk to your consultant or structural engineer to determine whether a jam nut is necessary.

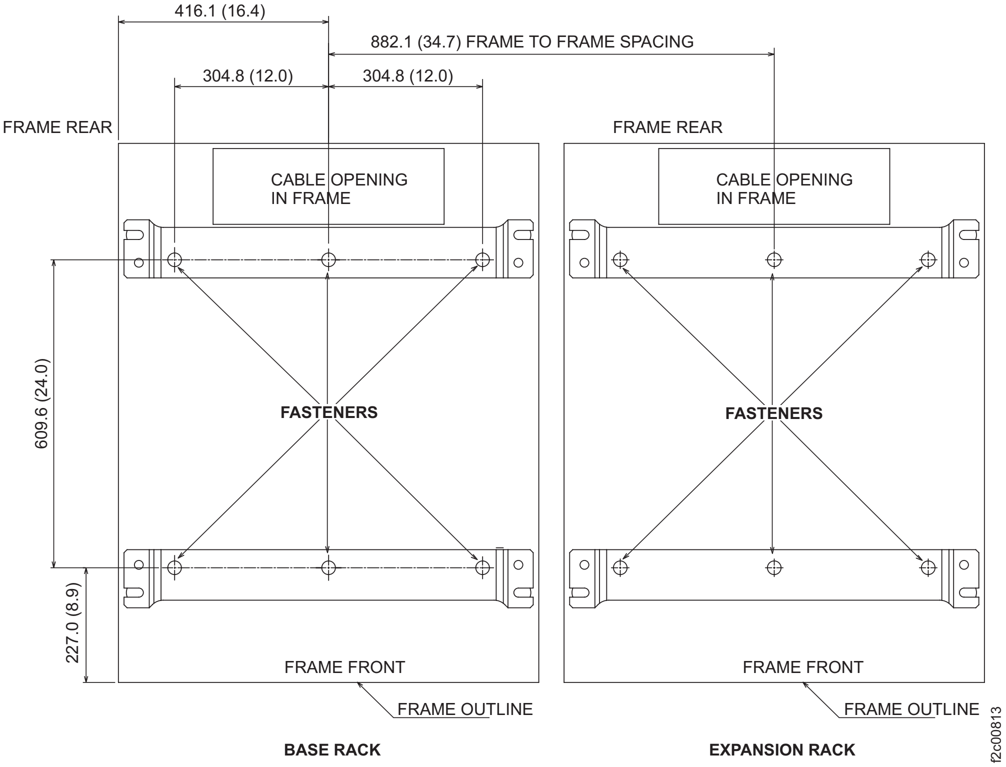


Figure 24. Locations for fastener installation (nonraised floor). The pattern repeats for up to five models. Dimensions are in millimeters (inches).

3. When the IBM service representative arrives to install the Earthquake Resistance Kit, provide the other fastener parts (**2** in Figure 23 on page 128) so that the representative can use these parts secure the load plates onto the floor.

Planning for power requirements

You must select a DS8000 storage complex location that meets specific power requirements.

When you consider the DS8000 storage complex location, consider the following issues:

- Power control selections
- Power outlet requirements
- Input voltage requirements
- Power connector requirements
- Remote force power off switch requirements
- Power consumption and environment

IBM cannot install the DS8000 series model if your site does not meet these power requirements.

Attention: Implementation of surge protection for electronic devices as described in the EN 62305 standard or IEEE Emerald Book is recommended. In case of lightning surge or other facility transient voltages a Surge Protection Device (SPD) limits the surge voltage applied at the DS8870 system power input. An SPD is required for facilities in Korea or customers conforming to the European EMC Directive or CISPR 24.

Overview of DS8000 power controls

The DS8000 series provides power controls on the model racks. Power controls can be configured by an IBM service support representative. Power controls can also be accessed through the Management Console.

The DS8000 models have these following manual power controls in the form of physical switches on the racks:

- **Local/remote switch**

  (Available on base models) The local/remote switch setting determines your use of local or remote power controls. When you set the switch to local, the local power on/local force power off switch controls power in the storage unit. You can access this switch by opening the rear cover of the unit. When the local/remote switch is set to remote, the power for the storage unit is controlled by remote power control settings that are entered in the DS Storage Manager. **Planning requirements:** None.
- **Local power on/local force power off switch**

  (Available on base models) The local power on/local force power off switch initiates a storage unit power on sequence or a storage unit force power off sequence. This switch is applicable only when the local/remote switch is set to local. You can access this switch by opening the rear cover of the unit. **Planning requirements:** None.

  Note: To activate this switch, press and hold it for 8 seconds.
- **Unit emergency power off switch**

(Available on all models) *Use this switch only in extreme emergencies. Using this switch often results in data loss.* If activated, the unit emergency power off (UEPO) switch causes the individual model rack to immediately drop all power, including any power that is provided by the battery system. When active, this switch overrides all other power controls for the specific rack. This switch is located behind the covers of each model. **Planning requirements:** None.

The following power controls can be configured by an IBM service support representative. You can also use the following power controls through the DS Storage Manager (running on the Management Console):

- **Local power control mode**

  (Visible in the DS Storage Manager) You cannot change this setting in the DS Storage Manager. This mode is enabled when the local/remote switch on the storage unit is in the local position. When this setting is used, the local power on/local force power off switch on the storage unit controls the power. **Planning requirements:** None.
- **Remote power control mode**

  (Visible in the DS Storage Manager) If you select the **Remote** power control mode, you choose one of the following remote mode options. **Planning requirements:** If you choose the **Remote zSeries Power Control** options, you must have the remote zSeries power control feature. There are no requirements for the other options.
  - **Remote Management Console, Manual**: Your use of the DS Storage Manager power on/off page controls when the unit powers on and off.
  - **Remote Management Console, Scheduled**: A schedule, which you set up, controls when the unit powers on and off.
  - **Remote Management Console, Auto**: This setting applies only in situations in which input power is lost. In those situations, the unit powers on as soon as external power becomes available again.
  - **Remote Auto/Scheduled**: A schedule, which you set up, controls when the unit powers on and off. A power on sequence is also initiated if the unit was powered off due to an external power loss while the units are scheduled to be on and external power becomes available again.
  - **Remote zSeries Power Control**: One or more attached System z or S/390 hosts can control the power on and power off sequences.

Power outlet requirements

Plan for the required power outlets when planning for the installation of your storage units.

The following power outlets are required:

- Two independent power outlets for the two DS8000 power cords needed by each base model and expansion model.

  Important: To eliminate a single point of failure, the outlets must be independent. This means that each outlet must use a separate power source and each power source must have its own wall circuit breaker.
- Two outlets that are within 3.1 m (10 ft.) of the external management console. Typically, these outlets are in a rack that you provide.

Input voltage requirements

When you plan for the power requirements of the DS8000 series model, consider the input voltage requirements.

Table 51 provides the input voltages and frequencies that the DS8000 storage units support. Inputs are balanced and either single or three phase.

Table 51. DS8000 input voltages and frequencies

Characteristic	Low Voltage	High voltage feature
Nominal input voltages	200, 208, 220, or 240 RMS V ac	380, 400, or 415 RMS V ac
Minimum input voltage	180 RMS V ac	333 RMS V ac
Maximum input voltage	264 RMS V ac	456 RMS V ac
Customer wall breaker rating (1-ph, 3-ph)	50-60 Amps	30-35 Amps
Steady-state input frequencies	50 ± 3 or 60 ± 3.0 Hz	50 ± 3 or 60 ± 3.0 Hz
PLD input frequencies (<10 seconds)	50 ± 3 or 60 ± 3.0 Hz	50 ± 3 or 60 ± 3.0 Hz

Power connector requirements

Ensure that the site where you plan to install the DS8000 storage units meets the power connector requirements.

Table 52 on page 133 provides the power cords and the inline connectors and receptacles types that they support. Find the power cord row that is appropriate for your site. Ensure that the site where you plan to install the DS8000 storage units meets the power connector requirements that are shown in that row.

Phase rotation on three-phase power-cable connectors is counterclockwise as you look at the power cord plug. Phase rotation is clockwise as you look at the face of the power receptacle at your installation site.

Attention

- For reliable operation do not use Ground Fault Circuit Interrupter (GFCI), Earth Leakage Circuit Breaker (ELCB), or Residual Current® Circuit Breaker (RCCB) type circuit breakers with the DS8870. The DS8870 is certified for safe operation and compliant with IEC, EN, UL and CSA 60950-1 standards. If local electrical practice requires leakage detection circuit breakers they should be rated at minimum to 300mA or larger to reduce the risk of outage due to spurious actuation.
- Low-voltage, three-phase installations (200-240 V) require wall circuit breakers that have a rating of 50 to 60 A.
- High-voltage, three-phase installations (380- 415 V) require wall circuit breakers that have a rating of 30 to 35 A.

  Note: Special applications that use 30 A power cords must rely on 30 A wall circuit breakers for power cord protection.
- Low voltage, single-phase and three-phase delta installations require wall circuit breakers that have a rating of 50 to 60 A.
- High voltage, three-phase wye installations require wall circuit breakers that have a rating of 30 to 35 A.

- Do not exceed the wire rating of the facility.

Table 52. DS8870 power cords

Power Cord Feature Code	Power Cord Description	Inline Connector	Receptacle
1061 (See notes 1, 2, 3, 4, 5)	Single-phase power cord, 200-240V, 60A, 3-pin connector	HBL360C6W, Pin and Sleeve Connector, IEC 309, 2P3W	HBL360R6W, AC Receptacle, IEC 60309, 2P3W
1068 (See notes 2, 3, 4)	Single-phase power cord, 200-240V, 63A, no connector	Not applicable	Not applicable
1072 (See notes 1, 2, 3, 4, 5)	Top exit single-phase power cord, 200-240V, 60A, 3-pin connector	HBL360C6W, Pin and Sleeve Connector, IEC 309, 2P3W	HBL360R6W, AC Receptacle, IEC 60309, 2P3W
1073 (See notes 2, 3, 4)	Top exit single-phase power cord, 200-240V, 63A, no connector	Not applicable	Not applicable
1081 (See notes 2, 3, 4)	Three-phase power cord, wye, 380V-415V, 32A, no connector	Not applicable	Not applicable
1082 (See notes 1, 2, 3, 4, 5)	Three-phase power cord, delta, 200-240V, 60A, 4-pin connector	HBL460C9W, Pin and Sleeve Connector, IEC 309, 3P4W	HBL460R9W, AC Receptacle, IEC 60309, 3P4W
1083 (See notes 2, 3, 4)	Top exit three-phase power cord, wye, 380V-415V, 32A, no connector	Not applicable	Not applicable
1084 (See notes 1, 2, 3, 4, 5)	Top exit three-phase power cord, delta, 200-240V, 60A, 4-pin connector	HBL460C9W, Pin and Sleeve Connector, IEC 309, 3P4W	HBL460R9W, AC Receptacle, IEC 60309, 3P4W

Notes:

1. **The customer connector must be IEC 60309; prior power cords cannot be reused.**
2. All power cords are rated at 250 V ac, except power cords without inline connectors are rated at 600 V ac. Single-phase power cord has 2W+G configuration. Delta three-phase power cord has 3W+G configuration. Wye three-phase power cord has 3W+N+G configuration.
3. The conductor size for three-phase EMEA power cords is 6 mm² (10awg). The conductor size for single-phase EMEA power cords is 10 mm² (6awg). The conductor size for signal-phase and three-phase non-EMEA power cords is 10 mm² (6awg).
4. Power® cords that exit the bottom are 4.2 M (14 ft) from the lowest point where they exit the frame to the mating face of the plug or bare leads. Power cords that exit the top are 1.8 M (6 ft) from the highest point from the frame to the mating face of the plug or bare leads.
5. The IEC60309 receptacle must be installed in a metal-backed box with the green wire ground-connected to the grounding lug within the box. Ensure continuity between the box and the metallic shielding of the liquid-tight conduit.

Power consumption and environmental information

When you are planning to meet the power requirements for the DS8000 series, consider the power consumption and other environmental points of the storage unit.

This power consumption and environmental information for the IBM System Storage DS8870 is provided in Table 53 on page 134.

Table 53. Power consumption and environmental information for the DS8000 series - Models 961 and 96E

Measurement	Units	Base model 961	Expansion model 96E
Peak electric power (See Notes 1 and 3)	kilovolt amperes (kVA)	6	5.8
Thermal load	British thermal units (BTU) per hour	20,612	19,605
Capacity of exhaust	cubic meters per minute (cubic feet per minute or CFM)	44.2 (1500)	51.8 (1800)
Ground leakage current	milliamperes (mA)	60	60
Startup current	amperes (A or amp)	≤ 100	≤ 100
Startup current duration	microseconds (µs or µsec)	< 200	< 200
Idle and operating sound power level, LWAd (see Note 2)	A-weighted bels (B)	7.5	7.5

Notes:

1. The values represent data that was obtained from typical systems, configured as follows:
   - Base models that contain 15 disk drive sets (16 drives per disk drive set, 15 disk drive sets x 16 = 240 disk drives) and fibre-channel adapters.
   - Expansion models that contain 21 disk drive sets per enclosure (21 disk drive sets x 16 = 336 disk drives) and fibre-channel adapters.
2. LWAd is the statistical upper-limit A-weighted sound power level, expressed in bels, declared in conformance with ISO 9296. The values correspond to DS8870 models containing 240 disk drives. The values represent data obtained during preliminary testing. Bels relate to decibels (dB) as follows: *1 B = 10 dB*. The ratings are rounded to the nearest 0.1 B. Measurements are in conformance with ISO 7779.
3. All models and configurations that are used in single-phase mode must not exceed 8 kVA.

Acoustic declaration for the DS8000 series

Table 54 describes the acoustic declaration information for the DS8000 series DS8870.

Table 54. Acoustic declaration for the DS8000 series, including the DS8870

Product Description	Declared A-Weighted Sound Power Level, LWAd (B)		Declared A-Weighted Sound Pressure Level, LpAm (dB)	
	Operating	Idling	Operating	Idling
DS8870 fully configured Model 961	**7.9**	**7.9**	**61**	**61**
DS8870 fully configured Model 96E	**7.9**	**7.9**	**61**	**61**

Notes:

- LWAd is the statistical upper-limit A-weighted sound power level (rounded to the nearest 0.1 B).
- LpAm is the mean A-weighted emission sound pressure level measured at the 1-meter bystander positions (rounded to the nearest dB).
- 10 dB (decibel) = 1 B (bel).
- All measurements made in conformance with ISO 7779 and declared in conformance with ISO 9296.

Planning for environmental requirements

You must install your storage unit in a location that meets the operating environment requirements to properly maintain your DS8000 storage unit.

Take the following steps to ensure that you meet these requirements:

1. Note where air intake locations are on the models that compose your storage unit.
2. Verify that you can meet the environmental operating requirements at the air intake locations.
3. Consider optimizing the air circulation and cooling for the storage unit by using a raised floor, adjusting the floor layout, and adding perforated tiles around the air intake areas.

Fans and air intake areas

The DS8000 models provide air circulation through various fans throughout the frame. You must maintain the correct operating environment requirements for your models at each air intake location.

Table 55 summarizes fan, intake, and exhaust locations.

Table 55. Machine fan location

DS8870 Fan Location	Machine Location	Intake Location	Exhaust Location
Entire machine	Entire	Front covers	Rear covers
Power complex	Left-side	Front covers	Rear covers

Operating environment requirements

You must meet specific operating environment requirements at all the air intake locations of your DS8000 models.

The operating points vary depending on the state of the model. The models can be in the following states:

- Powered on
- Powered off
- In storage

Powered on:

Plan for the DS8000 operating ranges and recommended operating points when the storage unit is on.

Table 56 provides the operating ranges for your storage unit when the power is on.

Table 56. Operating extremes with the power on

Altitude	0 - 2133 m (0 - 7000 ft)
Dry bulb temperature	16 - 32°C (60 - 90°F)
Relative humidity	20 - 80%
Wet bulb temperature (maximum)	23°C (73°F)

Table 57 on page 136 provides the optimum operating points for your storage unit with the power on.

Table 57. Optimum operating points with the power on

Temperature	22°C (72°F)
Relative humidity	45%

Table 58 provides the operating ranges for a storage unit with the power on.

Table 58. Optimum operating ranges with the power on

Temperature	16 - 32°C (60 - 90°F)
Relative humidity	40 - 50%

Powered off:

Plan for the required DS8000 temperature and humidity ranges when the storage unit is off.

Table 59 provides the temperatures and humidity requirements for your storage unit when the power is off.

Table 59. Temperatures and humidity with the power off

Temperature	10 - 43°C (50 - 110°F)
Relative humidity	8 - 80%
Wet bulb temperature (maximum)	27°C (80°F)

In storage:

Plan for the required DS8000 temperature and humidity ranges when the storage unit is in storage.

Table 60 provides the temperatures and humidity requirements for storing your storage unit.

Table 60. Temperatures and humidity while in storage

Temperature	**1 - 60°C (34 - 140°F)**
Relative humidity	**5 - 80%**
Wet bulb temperature (maximum)	**29°C (84°F)**

Corrosive gasses and particulates

Plan for air quality that meets standards for corrosive gases and particulates.

The DS8000 is designed to operate reliably in a General Business class environment. A General Business class environment is one that has automated 24x7x365 temperature and humidity controls and also operates with the following specifications for corrosive gases and particulates: G1 for corrosive gases, P1 for particulates.

Operating vibration requirements

The vibration levels designed for the DS8870 comply with class V1 requirements included in the product classes for vibration.

The DS8870 is designed to operate under the vibration V1 levels described in Table 61. Additional information includes random vibration PSD profile breakpoints and operational shock levels.

Table 61. Vibration levels for the DS8870

Class	***g*rms**	***g* Peak Sine**
V1L	0.10	0.06 @ 50 and 60 Hz
Notes: 1. All values in this table are in g^2/Hz 2. *g* is the peak *g* level of an approximate half-sine pulse.		

Table 62. Random vibration PSD profile breakpoints for the DS8870

Class	**5 Hz**	**17 Hz**	**45 Hz**	**48 Hz**	**62 Hz**	**65 Hz**	**150 Hz**	**200 Hz**	**500 Hz**
V1L	$2.0x10^{-7}$	$2.2x10^{-5}$							
Note: All values in this table are in g^2/Hz.									

Table 63. Operational shock levels forDS8870

Class	**Access**	***g*[1]**	**pw[2]**
S1	V	3.5	3.0
Notes: 1. *g* is the peak *g* level of an approximate half-sine pulse. 2. "pw" is the pulse width in milliseconds.			

Contamination information

You must consider the air quality and contamination levels at your installation site.

Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors, such as humidity or temperature, might pose a risk to the IBM System Storage DS8000 hardware. Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the DS8000 to malfunction or cease functioning altogether. This specification presents limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer.

Attention: In the absence of specific limits that are presented in this document, you must implement practices that maintain particulate or gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have damaged the DS8000, the warranty is void. Implementation of correctional measures is a customer responsibility.

The following criteria must be met:

Gaseous contamination

Severity level G1 as per ANSI/ISA 71.04-1985[1], which states that the reactivity rate of copper coupons must be less than 300 Angstroms per month (Å/month, ≈ 0.0039 µg/cm2-hour weight gain)[2]. In addition, the reactivity rate of silver coupons must be less than 300Å/month (≈ 0.0035 µg/cm2-hour weight gain)[3]. The reactive monitoring of gaseous corrosivity is conducted approximately 2 inches (5 cm) in front of the rack on the air inlet side at one-quarter and three-quarter frame height off the floor, or where the air velocity is much higher.

Particulate contamination

Data centers must meet the cleanliness level of ISO 14644-1 class 8. For data centers without airside economizers, the ISO 14644-1 class 8 cleanliness can be met by selecting one of the following filtration methods:

- The room air can be continuously filtered with MERV 8 filters.
- Air entering a data center can be filtered with MERV 11, or preferably MERV 13 filters.

For data centers with airside economizers, the choice of filters to achieve ISO class 8 cleanliness depends on the specific conditions present at that data center. The deliquescent relative humidity of the particulate contamination must be more than 60% RH[4]. Data centers must be free of zinc whiskers[5].

1. ANSI/ISA-71.04.1985. *Environmental conditions for process measurement and control systems: Airborne contaminants.* Instrument Society of America, Research Triangle Park, NC, 1985.
2. The derivation of the equivalence between the rate of copper corrosion product thickness growth in Å/month and the rate of weight gain assumes that Cu_2S and Cu_2O grow in equal proportions.
3. The derivation of the equivalence between the rate of silver corrosion product thickness growth in Å/month and the rate of weight gain assumes that Ag_2S is the only corrosion product.
4. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote corrosion, ion migration, or both.
5. Surface debris is randomly collected from 10 areas of the data center on a 1.5 cm diameter disk of sticky, electrically conductive tape on a metal stub. If examination of the sticky tape in a scanning electron microscope reveals no zinc whiskers, the data center is considered free of zinc whiskers.

Cooling the storage complex

You can take steps to optimize the air circulation and cooling for your storage units.

To optimize the cooling around your storage units, prepare the location of your storage units as recommended in the following steps.

Note: The installation of a storage unit is done by IBM service representatives. However, the following steps describe the process needed to optimize the air circulation and cooling for your storage units.

DS8870

1. Prepare for the installation of the storage unit on a raised floor. Although the storage unit can be installed on a nonraised floor, installing the storage unit on a raised floor provides increased air circulation for better cooling.
2. Install perforated tiles in the front of each base model and expansion model as follows:

a. For a stand-alone base model, install two fully perforated tiles in front of each base model, as shown in Figure 25 in the single-machine examples (1 and 2 in the figure).

b. For a row of machines, install a row of perforated tiles in front of the machines as shown in Figure 25 (3 and 4 in the figure).

c. For groupings of machines, where a hot aisle/cold aisle layout is used, use a cold aisle row of perforated tiles in front of all machines. A possible minimal configuration is shown in Figure 25 (5 in the figure).

Note: Keep in mind that the dimensions represented in Figure 25 might not be adequate for floor-load requirements.

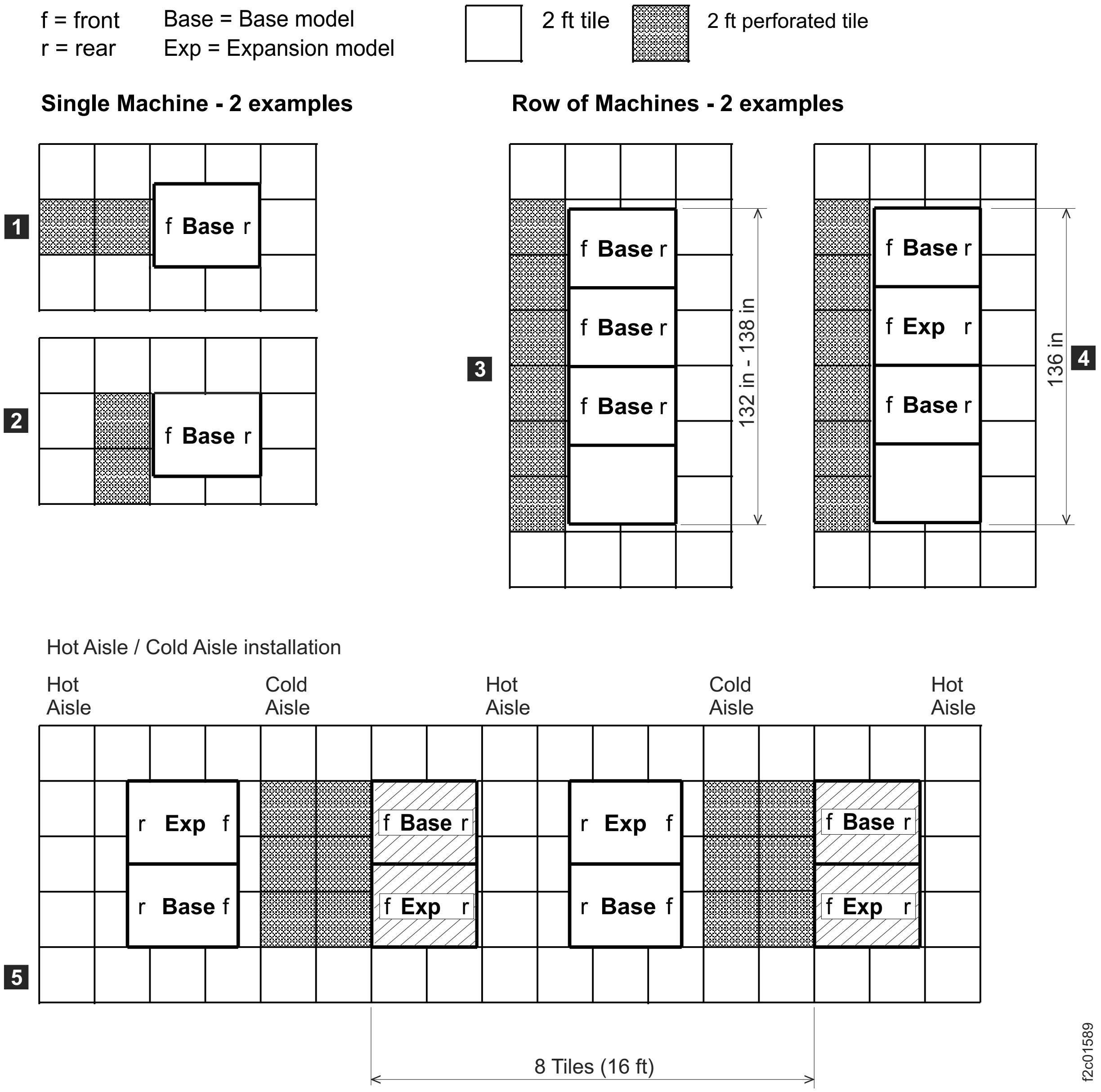


Figure 25. DS8870 layouts and tile setup for cooling

Providing a fire-suppression system

Set up an environment that supports the temperature, cooling, and operating requirements of your DS8000 series. You are responsible for providing a fire suppression system for your storage units.

IBM designs and manufactures equipment to internal and external standards that require certain environments for reliable operation. Because IBM does not test any equipment for compatibility with fire-suppression systems, IBM does not make compatibility claims of any kind. IBM does not provide recommendations on fire-suppression systems.

1. Consult your insurance underwriter, local fire marshal, or local building inspector about selecting a fire-suppression system that provides the proper level of coverage and protection.
2. Set up an environment that supports the temperature and cooling requirements for your DS8000 storage unit as discussed in the environmental temperature requirements planning area.

Considering safety issues

You must consider various safety issues when you plan your DS8000 series location.

The following list identifies some of the safety issues you must consider:

- Fire suppression
- Earthquake safety

Planning for external management console installation

If you use an external management console (feature code 1130), you must plan for its installation.

Attention: The Ethernet port integrated into this product is not intended to be connected directly or indirectly, by any means whatsoever, to interfaces of public telecommunications networks.

You must provide the following for the installation of the external management console:

- A location for the external management console that allows the Ethernet cable, which is 31 m (101 ft), to reach the management console on one end and the storage unit on the other end. You can locate your management console farther away, if necessary; however, this location can make servicing your storage unit more difficult, and you must provide two of your own Ethernet cables. Any Ethernet cables that you supply must meet the following requirements:
  - The cables must be straight 4-pair UTP CAT 5E (or better) cables with RJ-45 jacks.
  - The length of each cable cannot exceed 100 m (328 ft).
  - The two private network cables are labeled or marked on both ends to make it obvious which one belongs to the gray network and which one belongs to the black network.
- A rack in which to mount the management console. This rack can be an IBM rack or a non-IBM rack, but it must meet specifications.
- An external management console must be installed in an environment that does not exceed 35 degrees Celsius (°C).

- Two outlets that are within 3.1 m (10 ft) of the external management console. Typically, these outlets are in the rack that you provide. The outlets are used by the country-specific line cords that you select when you order the external management console.

Both the internal and external management consoles are dedicated servers. The first is always located inside the storage unit.

Rack specifications for the external management consoles

Use rack specifications information to ensure you have the required environment for a non-IBM rack if you plan to install your external management console in a non-IBM rack.

If you install your external management console in a non-IBM rack, ensure that the rack satisfies the required specifications. The following specifications are required for a non-IBM rack:

- The rack must meet EIA-310-D standards for mounting flanges and hole locations.
- The front-to-rear distance of the mounting flanges must be 720 mm (28.3 in.).
- The thickness of the mounting flanges must be between 1.9 and 3.3 mm (0.08 and 1.3 in.).
- The mounting flanges must have either 7.1 mm (0.28 in.) diameter holes or 9.6 mm (0.38 in.) square holes on the standard EIA hole spacing.
- The rack must have a minimum depth of 70 mm (2.76 in.) between the front mounting flange and inside of the front door for appropriate cooling.
- The rack must have a minimum depth of 157 mm (6.2 in.) between the rear mounting flange and inside of the rear door to install the external management console and provide cable management space.
- The minimum side-to-side clearance in the rack between the front and rear mounting flanges must be of 467 mm (18.2 in.) to accommodate the width of the server and the slide mounting brackets.
- The front edge of the keyboard/display tray is 19 in. wide including the tabs for the front thumbscrews. To use the tray, it must be extended out fully on its rails. If the rack is equipped with front covers, ensure that they are hinged in such a way that in their fully open position they allow the keyboard/display tray to be fully extended.
- The rack must include perforated front and rear doors and must not prevent the flow of cool air into or out of the rack.
- The weight-handling capacity of the rack must be able to support the maximum rack configuration, including all servers, external cables, PDUs, and so on.
- The rack must provide proper stabilization so that the rack does not become unstable when the external management console or other equipment are pulled out for use or for service.

Planning for network and communications requirements

You must locate your DS8000 storage units in a location that meets the network and communications requirements.

Keep in mind the following network and communications issues when you plan the location and interoperability of your storage units:

- Management console network requirements
- Remote power control requirements

- Host attachment requirements
- SAN considerations

Management console network requirements

You must plan for the network requirements of the management console.

Each management console requires a dedicated connection to the network.

Note: If you plan on accessing the CLI or the Storage Manager and have a firewall between the management console and your network, you need to open the following TCP/IP ports prior to installation: 427, 1718, 1720, 1722, 1750, 1755, 6989, and 8451-8455.

Remote support connection requirements

You must select a remote connectivity option if you plan to use remote support. Remote support can include inbound or outbound support. You must ensure all equipment requirements are met to use remote support.

IBM's strategic and preferred remote support connectivity method is Internet SSL (Secure Socket Layer) for HMC-to-IBM communication, and Assist-On-Site (AOS) for IBM remote access to the HMC and the DS8000. AOS provides a network-type connection that is secured by SSL and state-of-the-art encryption technology. AOS is installed on a PC that is provided and maintained by the customer. Please contact your IBM service representative for more details.

Another remote support solution is the IBM-controlled HMC VPN. The VPN is used for outbound and inbound connectivity. Since the VPN is always initiated by the HMC either the local HMC service interface or DSCLI must be used to start the VPN. If a modem is configured at the same time it can be used by IBM personnel to initiate the VPN connection. All IBM remote support solutions provide you with an interface to control and secure access to the DS8000. IBM also provides activity and authentication logging.

The modem continues to be an option for inbound and outbound remote support connectivity. Internet FTP (File Transfer Protocol) can be configured for faster offload of dump and trace data. To support the modem connection you must provide the following equipment close enough to each management console:

- One analog telephone line per HMC for initial setup
- A telephone cable to connect the modem to a telephone jack

To enable remote support, you must allow an external connection by one of the following means:

- A telephone line
- An outbound Internet connection through your firewall that allows IBM to use a VPN connection to your management console

All IBM remote support solutions provide you with an interface to control and secure access to the DS8000. IBM also provides activity and authentication logging.

The DS8000 modems support worldwide use, and they meet all required standards.

Remote power control requirements

Use the remote power control settings to control the power of your storage complex. Settings can be controlled through the DS Storage Manager running on the management console.

There are several settings for remote power control. Only the remote zSeries power control setting requires planning on your part.

The remote zSeries power control setting allows one or more attached System z or S/390 hosts to control the power on and power off sequences for your storage unit. If you use the remote zSeries power control setting, you must meet the following requirements:

- Order the remote zSeries power control feature.
- Allow up to four interfaces for remote zSeries power control.

SAN requirements and considerations

Use SAN requirements and considerations information to help you plan for a DS8000 series that attaches to a SAN.

A Fibre Channel storage area network (SAN) is a specialized, high-speed network that attaches servers and storage devices. With a SAN, you can perform an any-to-any connection across the network using interconnect elements such as routers, gateways, hubs, and switches.

For a DS8000 series configuration, you can use SANs to attach storage unit disks and to attach hosts to the storage unit.

When you connect your DS8000 storage units to a SAN, you must meet the following requirements:

- When a SAN is used to attach both disks and hosts to the storage unit, any storage device that is managed by the storage unit must be visible to the host systems.
- When concurrent device adapters and I/O adapter operations are supported through the same I/O port, the SAN attached to the port must provide both host and device access.
- Fibre Channel I/O adapters must be configured to operate in a point-to-point mode fabric topology. See the *IBM System Storage DS8000 Host Systems Attachment Guide*, for more information.

Also consider the following facts:

- Fibre Channel SANs can provide the capability to interconnect open systems and storage in the same network as System z or S/390 host systems and storage.
- A single Fibre Channel I/O adapter can have physical access to multiple Fibre Channel ports on the storage unit.

Host attachment communication requirements

Use host attachment communication requirements information to connect the host attachments in your network.

- You must use worldwide port names to uniquely identify Fibre Channel adapter cards that are installed in your host system.
- For open-system hosts with Fibre Channel adapters, keep in mind that Fibre Channel architecture provides various communication protocols. Each interconnected storage unit within the architecture is referred to as a *node*, and each host is also a node. Each node corresponds to one or more ports. (In the

case of Fibre Channel I/O adapters, these ports are Fibre Channel ports.) Each port attaches to a serial-transmission medium that provides duplex communication with the node at the other end of the medium. You can configure your network structure based on one of three basic interconnection topologies (network structures):
  - Point-to-point
  - Switched fabric
  - Arbitrated loop

  See the *IBM System Storage DS8000 Host Systems Attachment Guide* for more information about these supported topologies.
- The maximum distance between a host Fibre Channel port and the following network components is 300 meters (984 ft) with a shortwave adapter and 10 km (6.2 miles) with a longwave adapter.
  - Fabric switches
  - Fabric hubs
  - Link extenders
  - Storage unit Fibre Channel port

  The maximum distance might be greater than 10 km (6.2 miles) when a link extender provides target initiator functions or controller emulation functions.

  Note: Do not use link extenders with emulation functions on links over which Remote Mirror and Copy operations are performed. These units introduce additional path delay.
- Because the Fibre Channel architecture allows any channel initiator to access any Fibre Channel device, without access restrictions, a security exposure can occur. Have your IBM service representative set the Fibre Channel access modes to the proper setting. See the *IBM System Storage DS8000 Host Systems Attachment Guide* for more information about Fibre Channel access modes.
- DS8000 storage units can connect to IBM SAN Volume Controller host systems. See the *IBM System Storage DS8000 Host Systems Attachment Guide* for more information.

Attention: Signal loss tolerance for Fibre Channel links running at 8 Gbps are reduced -1.4 dB as compared to links running at 4 Gbps. It is recommended that you take necessary steps to ensure links are within the signal loss parameters listed when planning a move from 4 Gbps FC to 8 Gbps FC adapters with existing infrastructure. Use of more than two patch panels or other link connectors between two 8 Gbps ports at maximum distance of 10 km may result in greater link loss than is acceptable. Signal loss tolerance, with measurements including all connectors and patch panel connections, are:

- Loss per 10 km for 8 Gbps speed is -6.4 dB.
- Loss per 10 km for 4 Gbps speed is -7.8 dB.

OM3 Fibre Channel cables are required to support 8 Gbps Host Adapters.

Chapter 7. Planning your DS8000 storage complex setup

During installation, IBM customizes the setup of your storage complex based on information that you provide in the customization work sheets.

Each time you install a new storage unit or management console, you must complete the customization work sheets before the IBM service representatives can perform the installation.

The customization work sheets allow you to specify the initial setup for the following items:

- Company information
- Management console network settings
- Remote support (includes call home and remote service settings)
- Notifications (includes SNMP trap and email notification settings)
- Power control
- Control Switch settings

Important: IBM service representatives cannot install a storage unit or management console until you provide them with the completed customization work sheets.

Company information

Specify on the company information work sheet any information which IBM service personnel (or your service provider) can use to contact you as quickly as possible or to access your storage complex.

This information includes the following items:

- General company information, such as company name and telephone number
- Administrator contact information
- Storage complex location and modem numbers

You must complete this work sheet for all installations that include a management console.

Management console network settings

Use the management console network setting work sheet to specify the IP address and LAN settings for your management console.

The management console network settings include the following items:

- Management console network identification
- Ethernet settings, if you want the management console to connect to your LAN
- DNS settings, if you plan to use a domain name server to resolve network names
- Routings, if you want to specify a default gateway for routing

Note: IBM will attach your LAN after the storage complex is installed and in operation.

You must complete the work sheet for all installations that include an management console. Before completing it, review the exceptions listed in the notes at the bottom of the work sheet. .

Remote support settings

Use the remote support work sheets to specify whether you want outbound (call home) or inbound (remote services) remote support.

Ensure that you enable both outbound and inbound support to help you maintain the highest availability of your data.

When you enable outbound (call home) support, your management console sends an electronic call home record to IBM support when there is a problem within the storage complex. If inbound remote services is also enabled, a response key pair that can be used one time enables IBM service representatives to remotely sign on to the management console in response to the service call. If unattended remote service is configured, a remote IBM service representative can establish a remote service connection from the HMC to IBM. If outbound support is enabled, but inbound remote services is not enabled, the IBM service representative must physically come to your location to troubleshoot and service the storage complex.

When inbound remote services are enabled, service representatives can perform service tasks remotely. They can view error logs and problem logs, and initiate trace or dump retrievals.

You can use DS CLI and its audit log feature to review who and at what time performed remote service on your machine. Contact your IBM service representative for more detailed information on which service actions were performed remotely.

You can use DS CLI to control network access to each individual HMC and the DS8000.

For faster service and maintenance, Secure Sockets Layer (SSL) or Virtual Private Network (VPN) connectivity is preferred over modem connectivity. For information about VPN and SSL, go to the www.ibm.com/support/docview.wss?uid=ssg1S1002693.

You must complete the work sheet for all installations that include a management console.

Notification settings

Use the notification work sheets to specify the types of notifications that you want to receive and that you want others to receive.

Note: The IBM service representative sets up the notification process.

Notifications contain information about your storage complex, such as serviceable events.

You can receive notifications through the following methods:

- Simple Network Management Protocol (SNMP) traps
- Email

You can choose one or both notification methods.

When you choose to have your storage complex generate SNMP traps, you can monitor the storage complex over your network. You can control whether management information base (MIB) information is accessible and what type of SNMP traps to send. You can also specify the maximum number of traps sent for each event and where to send the traps.

Notes:

1. If you have open-systems hosts and remote mirror and copy functions, you must enable SNMP notifications for status reporting.
2. If you plan to use advanced functions SNMP messaging, you must set those functions using DS CLI.

When you choose to enable email notifications, email messages are sent to all the email addresses that you specify on the work sheet when the storage complex encounters a serviceable event or must alert you to other information.

You must complete the work sheet for all installations that include a management console.

Power control settings

If you use the remote System z power control feature, you must specify that on the power control work sheet, so the power mode can be set up to support that feature. Use this work sheet to specify and schedule whether power turns on and off automatically.

If you want to use a scheduled power mode, you must enter the schedule on the power control work sheet. You must complete the power control work sheet for *all installations*.

Control switch settings

Use the control switch settings work sheet to specify certain DS8000 series settings that affect host connectivity. You are asked to enter these choices on the control switch settings work sheet so that your IBM service representative can set them during the installation of your DS8000 series model.

The following control switches are set using the choices you specify on the control settings work sheet.

IBM i LUN serial suffix number

Use this control switch setting only when you attach more than one DS8000 series model to an AS/400 or IBM i host *and* the last three digits of the worldwide node name (WWNN) are the same on any of the DS8000 units.

Control switch settings - attachment to IBM System z

The following control switch settings are specific to System z.

Control-unit initiated reconfiguration (CUIR) support

Control-unit initiated reconfiguration (CUIR) allows automation of channel path quiesce and resume actions during certain service actions. This setting eliminates the requirement for manual actions from the host.

Present SIM data to all hosts

Service Information Messages (SIMs) are offloaded to the first I/O request directed to each logical subsystem in the storage facility if the request is device or control unit related, or offloaded to the individual logical volume when the request is media related. This control switch determines whether SIMs are sent to all, or to only the first, attached IBM System z LPAR making an I/O request to the logical system or logical volume.

Control unit threshold

This control switch provides the threshold level, presenting a SIM to the operator console for controller related errors. SIMs are always sent to the attached IBM System z hosts for logging to the Error Recording Data Set (ERDS). SIMs can be selectively reported to the IBM System z host operator console, as determined by SIM type and SIM severity.

Device threshold

This control switch provides the threshold level, presenting a SIM to the operator console for device related errors. Device threshold levels are the same type and severity as control unit threshold settings.

Media threshold

This control switch provides the threshold level, presenting a SIM to the operator console for media related errors. Media threshold levels are the same type and severity as control unit threshold settings.

Chapter 8. Planning data migration

Use these data migration considerations to formulate your data migration plan.

There are three levels of considerations to keep in mind when selecting the best method for your environment. At the first level, you consider broad questions about your environment to create a generic profile of your needs. At the second level, you compare which migration methods fit into your generic profile. The third level is to review a set of hints and other guidelines that apply to specific environments or that can help you take advantage of a migration to optimize your environment.

Consider creating any new fixed block (FB) volumes with T10 DIF protection. This protection can be used on volumes to which data is migrated, even if the current host server volumes are not T10-protected. T10 DIF-protected volumes can be used even if the host server does not currently support T10 DIF.

The following are some key questions to use to define your generic migration environment:

- Why is the data migrating?
- How much data is migrating?
- How quickly must the migration be performed?
- What duration of service outage can be tolerated?
- Is the data migration to/from the same type storage?
- What resources are available for the migration?

Allow more time or resources to perform any of the following tasks:

- Creating new logical volumes or file systems
- Modifying configuration files
- Receiving integrity checks

After determining general answers to the considerations listed above, a better understanding of some of the migration options along with their advantages and disadvantages will help frame your generic profile into a subset of acceptable migration options. Table 64 compares the data migration options.

Table 64. Comparison of data migration options

Type	Example	Advantages	Disadvantages
OS / LVM Mirroring	Logical Volume Managers, (LVM) Veritas Volume Manager (VxVM), Windows Disk Administrator	Little or no application service disruption	Potential application delays
UNIX or Windows Commands	cpio, cplv, dd, tar, backup restore; copy, scopy, xcopy, drag and drop	Common, easy to use, tested	Length of service interruption varies; scripting prone to errors and additional testing

Table 64. Comparison of data migration options (continued)

Type	Example	Advantages	Disadvantages
Remote Copy	Synchronous Mirror (Metro Mirror); Asynchronous Mirroring (Global Mirror and Global Copy)	Operating system independent	Like storage device types needed
Third party software packages	Data Migration (XoSoft); Backup /Restore (Tivoli, Legato, Veritas)	Some have little application service interruption, standard utilities	Cost of software; some have high application service interruption
Third party migration appliances	IBM San Volume Controller, DataCore SANsymphony	Multiple heterogeneous storage venders supported; migration cycles offloaded to appliance	Cost of migration appliance / service, application disruption to install / remove appliance

Besides these two sets of general considerations, there are a few more specific considerations and hints to review before finalizing your data migration method. Some apply to your environment and some do not. Also keep in mind that data migration is a service offered through IBM Global Services. Contact your IBM Representative for more information.

Select a migration method by your operating system:

- Is it UNIX based? Consider some variation of a logical volume manager.
- Is it a System z? Consider IBM System Storage Global Mirror, Remote Mirror and Copy.
- Is it z/OS? Consider DFDSS, though there are many choices.
- Is it VM? Consider DASD Dump Restore or PTAPE.
- Is it VSE? Consider the VSE fastcopy or ditto commands.

Notes:

- AIX and HP-UX 10.xx ship with logical volume management (LVM) software as part of the base operating system. LVM provides complete control over all disks and file systems that exist on an AIX system. HP-UX has similar volume management software.
- Sun Microsystems has a basic volume management product called Solstice, which is available for the Solaris systems. You can also purchase the Veritas Volume Manager (VxVM) and Veritas File System (VxFS) as optional products for Solaris.
- Linux systems also use the LVM

When replacing existing storage, partition the storage so that its virtual disks are similar in configuration to the disk drives that they are replacing. New configurations must be large enough to accommodate the existing data.

You might want to take advantage of this opportunity to do some remapping. The allocation and distribution of data does not have to be a straight one-to-one relationship, although that is possible. For instance, you can take advantage of using a maximum of 255 logical subsystems whereas the prior limitation was 32 logical subsystems.

Chapter 9. License activation and management

The management and activation of licensed functions are responsibilities that are associated with the role of your storage administrator.

Management refers to the use of the IBM Disk Storage Feature Activation (DSFA) website to select a license scope and to assign a license value. You can perform these activities and then activate the function.

Note: If you are activating features for any of the licensed functions, such as Copy Services, all the features must have the same capacity, including the operating environment license feature.

Activation refers to the retrieval and installation of the feature activation code into the DS8000 system. The feature activation code is obtained using the DSFA website and is based on the license scope and license value.

You perform these activities at the following times:

- After the IBM service representative has installed your storage unit and before you configure it
- When you increase the extent of the function authorization for a licensed function (that is, you add additional capacity to your license)

To perform these activities, you must access the DSFA website at www.ibm.com/storage/dsfa.

When you access DSFA, you must enter information about your DS8000 storage unit so the web application can access the correct function authorization records. You can find the information you must enter into DSFA on the Storage Unit General Properties page in the IBM System Storage DS Storage Manager application.

Planning your licensed functions

As you plan for your licensed functions, it is important to consider increases in your workload requirements. To provide more flexibility with licensing, usage-based licensing is supported on some models in the DS8000 series.

The DS8870 functions, such as Parallel Access Volumes (PAVs) and advanced Copy Services functions, FlashCopy, Metro Mirror, and Global Mirror are priced based on the usage of license capacity you purchase. For example, when you purchase licensed features for these functions, the features no longer have to be purchased with the same license capacity. You can purchase licenses for Copy Services functions with individual capacities instead of having to buy the licensed features with a single capacity. This capability is designed to provide you with more flexible and optimal price and performance configurations.

With the usage-based license capability comes the requirement to plan how much storage capacity you will require for future growth. As you plan for your licensed functions, it is important to consider increases in your workload requirements. For example, consider the following guidelines, which include but are not limited to:

- Plan for disk space allocation. Determine your typical disk storage requirements and consider how much additional storage you would need should you have rapid or unpredictable growth.
- Estimate the amount of capacity you need for current and future Copy Services functions. For example, consider the amount of target volumes you need for FlashCopy relationships at remote sites. As the number of FlashCopy target volumes increase, more available bandwidth of the disk system might be consumed by the copy process. In addition, Copy Service solutions that require multiple copies of data can also require extensive capacity storage.

Recognizing that both your storage and data requirements will increase over time and that capacity and performance planning is your responsibility, purchase and manage your licensed functions for maximum utilization. It can also be more cost effective to purchase more storage capacity to ensure that the maximum usage of your licensed features does not exceed the allowed capacity of that which was purchased. Ensure that you manage and purchase your licensed functions for maximum utilization. Should this happen, IBM will be notified that the usage exceeds the allowed capacity on any given licensed feature. You will be notified by IBM and required to extend enablement of your licensed feature and install a new licensed feature key.

Activating licensed functions

After the IBM service representatives have completed your DS8000 storage complex installation, your first step is to activate your licensed functions.

To activate your licensed functions, you must perform the following actions:
- Obtain your feature activation codes.
- Apply the activation codes to your storage unit. You can apply the activation codes by importing a file that you download from the IBM Disk Storage Feature Activation (DSFA) website.

The initial enablement of any optional DS8000 licensed function is a concurrent activity (assuming that the appropriate level of microcode is installed on the machine for the given function).

Note: The following activities are non-disruptive, but take effect at the next machine IML.
- Removal of a DS8000 licensed function to deactivate the function.
- A lateral change or reduction in the license scope. A lateral change is defined as changing the license scope from fixed block (FB) to count key data (CKD) or from CKD to FB. A reduction is defined as changing the license scope from all physical capacity (ALL) to only FB or only CKD capacity.

Obtaining activation codes

You must obtain feature activation codes for the licensed features for each storage unit by connecting to the IBM Disk Storage Feature Activation (DSFA) website.

Before you can connect to the site, ensure that you have the following items:
- The IBM License Function Authorization documents. If you are activating codes for a new storage unit, these documents are included in the shipment of the storage unit. If you are activating codes for an existing storage unit, IBM sends these documents to you in an envelope.

- A removable media for downloading your activation codes into a file. Use the removable media if you cannot access the IBM System Storage DS Storage Manager from the system that you are using to access the DSFA website. Instead of using removable media, you can also write down the activation codes and then manually enter them into the system that runs the DS Storage Manager.
- The machine serial number, model, and signature.

Complete the following steps to obtain your activation codes.

1. At a computer with an Internet connection and a browser, connect to the IBM Disk Storage Feature Activation (DSFA) website at www.ibm.com/storage/dsfa.
2. The DSFA application displays in the browser. Use the application to obtain the activation codes and follow the instructions on the screen.

   Note: In most situations, the DSFA application can locate your 239x license authorization record when you enter the DS8000 242x machine type, serial number and signature. However, if the 239x license authorization record is not attached to the 242x record, you must assign it to the 242x record in the DSFA application. In this situation, you will need the 239x serial number (which you can find on the License Function Authorization document).

   After you complete these steps, if your license codes are not present or are incorrect for your storage unit, contact your IBM representative.

Importing activation keys

You can import the activation keys that must be applied before you can begin configuring storage on a storage unit.

Notes:

1. Enabling an optional DS8000 licensed function is a concurrent activity (assuming the appropriate level of microcode is installed on the machine for the function). The following activating activities are non-disruptive, but take effect at the next machine IML:
   - Removal of a DS8000 licensed function to deactivate the function.
   - A lateral change or reduction in the license scope. A lateral change is defined as changing the license scope from fixed block (FB) to count key data (CKD) or from CKD to FB. A reduction is defined as changing the license scope from all physical capacity (ALL) to only FB or only CKD capacity.
2. Before you begin this task, you must resolve any current DS8000 problems. Contact IBM Support for assistance in resolving these problems.
3. Before you configure, disable or provide paths through any firewalls, because they might interfere with DS8000 communication.

Complete the following steps to import your activation codes.

1. In the navigation, select **Home** > **System Status**. On the System Status main page, select the storage image for which you want to import the activation key.
2. From the **Action** menu, select **Storage Image** > **Add Activation Key**. The Add Activation Key page is displayed.
3. Click **Import key file**. The Import page is displayed.

4. In the **Select file to import** field, specify the target file. Click **Browse** to navigate to the appropriate directory.
5. After you specify the key file, click **Next** to complete the process.

Adding activation keys

You must apply the activation codes so that you can begin to configure storage on a storage image..

Notes:

1. Enabling an optional DS8000 licensed function is a concurrent activity (assuming that the appropriate level of microcode is installed on the machine for the function). The following activating activities are non-disruptive, but take effect at the next machine IML for Model 961:
   - Removal of a DS8000 licensed function to deactivate the function. Contact your IBM service representative to complete this operation.
   - A lateral change or reduction in the license scope. A lateral change is defined as changing the license scope from fixed block (FB) to count key data (CKD) or from CKD to FB. A reduction is defined as changing the license scope from all physical capacity (ALL) to only FB or only CKD capacity.
2. Before you begin this task, you must check the error log and resolve any current DS8000 problems. Contact IBM Support for assistance in resolving these problems.
3. Before you configure, disable or provide paths through any firewalls because they might interfere with DS8000 communication.

The easiest way to apply the feature activation keys is to download the activation keys from the IBM Disk Storage Feature Activation (DSFA) website to your local computer and then to import the file into the DS Storage Manager. If you cannot access the DS Storage Manager from the same computer that you used to access the DSFA website, you can download the file to a CD or USB flash drive, or write down the information. If you are using either of these latter methods, ensure that you have your CD or USB flash drive that contains the downloaded activation keys file or your paper that contains the written activation codes before you begin the following steps.

Complete the following steps to add your feature activation keys.

1. Ensure that the Import key file page is not open. You cannot have both the Add activation key page and the Import key file page open at the same time. You must close one to access the other.
2. In the navigation, select **Home** > **System Status**. On the System Status main page, select the storage image for which you want to import the activation keys.
3. From the **Action** menu, select **Storage Image** > **Add Activation Key**. The Add Activation Key page is displayed.
   a. If you already imported your activation keys from a file or retrieved existing codes from the storage unit, the values are displayed in the fields and you can modify or overwrite them, as appropriate.
   b. If you have downloaded the activation key from the Disk Storage Feature Activation (DSFA) website, select **Import Key File** from the **Action** list and follow the prompts.

c. If you did not download your activation key, select **Add Activation Key** and follow the prompts.

4. Click **OK** to complete the process.

Scenarios for managing licensing

These topics provide scenarios for managing your DS8000 licenses after you have initially activated them.

The following scenarios are provided:

- Adding storage capacity to an existing machine
- Managing an active license feature

Note: Additional scenarios can be found on the IBM System Storage DS8000 Information Center.

Adding storage to your machine

Storage can be added (in terabytes) to an existing licensed feature such as point-in-time copy.

For this scenario, assume you initially purchased 23 TB of point-in-time capacity. You can order two 7253 features (10 TB each) and three 7251 features (1 TB each). After several months, you need an additional 20 TB for your point-in-time copy operations. To increase storage, you must purchase and activate a larger license. This is a nondisruptive activity and does not require that you reboot your machine.

1. You order two of feature 7253 (10 TB each) against the serial number of the 242x machine type license currently on your machine. These features will be the additional features that will increase your point-in-time copy authorization level.
2. After you have ordered the features, you receive confirmation from IBM that these new features have been processed.
3. Connect to the IBM-supported Disk Storage Feature Activation (DSFA) website at www.ibm.com/storage/dsfa to retrieve an activation code for the licensed feature. This new code represents the total capacity that you now have licensed (or 45 TB). It licenses the original 25 TB plus the additional 20 TB that you just ordered.
4. After you obtain the activation codes for the licensed feature, enter it into the web-based DS Storage Manager. You replace the existing activation code with the new activation code.
5. After the activation code is installed successfully, you now have 45 TB of PTC capacity.

Managing a licensed feature

Use the IBM System Storage DSFA website to change an optional function from active to inactive. Change an assigned value, such as current number of terabytes, for a feature to make that licensed feature inactive.

If you have an active optional function and you want to replace it with an inactive feature, you must later repurchase the feature if you want to use it again. However, you can use the following steps if you want to use the feature again.

1. From the DSFA website, www.ibm.com/storage/dsfa, change the assigned value from the current number of terabytes (TB) to 0 TB:

2. If this change is made, you can later go back to DSFA and reactivate the feature, up to the previously purchased level, without having to repurchase the feature.

Appendix A. Accessibility features for the DS8000

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

Accessibility features

The following list includes the major accessibility features in the IBM System Storage DS8000 Introduction and Planning Guide:

- Keyboard-only operation
- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys. You can navigate the IBM System Storage DS8000 Introduction and Planning Guide information 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.

Appendix B. Encryption

Encryption technology has a number of considerations that are critical to understand to maintain the security and accessibility of encrypted data. This section contains the key information that you have to know to manage IBM encrypted storage and to comply with IBM requirements for using IBM encrypted storage.

Failure to follow these requirements can result in a permanent encryption deadlock, which can result in the permanent loss of all key-server-managed encrypted data at all of your installations.

Encryption concepts

Encryption is the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

Data that is encrypted is referred to as *ciphertext*. Data that is not encrypted is referred to as *plaintext*. The data that is encrypted into ciphertext is considered securely secret from anyone who does not have the decryption key.

The following encryption algorithms exist:

Symmetric encryption algorithm
A common key is used to both encrypt and decrypt data. Therefore, the encryption key can be calculated from the decryption key and the decryption key can be calculated from the encryption key.

Asymmetric encryption algorithm
Two keys are used to encrypt and decrypt data. A public key that is known to everyone and a private key that is known only to the receiver or sender of the message. The public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

The following characteristics of encryption create special considerations:

Security exposures
Occurs when an unauthorized person has access to the plain text encryption key and the cipher text.

Data loss
Occurs if all copies of the decryption key are lost. If you lose the decryption key, you cannot decrypt the associated ciphertext. The data that is contained in the ciphertext is considered cryptographically erased. If the only copies of data are cryptographically erased ciphertext, access to that data is permanently lost.

To preserve the security of encryption keys, many implementation techniques can be used to ensure the following conditions:

- No one individual has access to all the information that is necessary to determine an encryption key.

- If only the symmetric encryption algorithm is used, manage encryption keys so that the data key that is used to encrypt and decrypt data is encrypted or wrapped with a wrapping key that is used to encrypt and decrypt data keys. To decrypt the ciphertext in this case, the wrapping key is first used to decrypt the ciphertext data key and obtain the plaintext data key, which is then used to decrypt the ciphertext and obtain the plaintext. If one unit stores the wrapping keys and a second unit stores the encrypted data key, then neither unit alone has sufficient information to determine the plaintext data key. Similarly, if a person obtains access to the information that is stored on either unit but not both units, there is not sufficient information to determine the plaintext data key. The unit that stores the wrapping keys is referred to as a key server and the unit that stores or has access to the encrypted data keys is referred to as a storage device. A *key server* is a product that works with the encrypting storage device to resolve most of the security and usability issues that are associated with the key management of encrypted storage. However, even with a key server, there is at least one encryption key that must be maintained manually. For example, the overall key that manages access to all other encryption keys.

- More than one individual has access to any single piece of information that is required to determine an encryption key. For redundancy, you can do the following actions:
  - Use multiple independent key servers that have multiple independent communication paths to the encrypting storage devices.
  - Maintain backups of the data on each key server. If you maintain backups, the failure of any one key server or any one network does not prevent storage devices from obtaining access to data keys that are required to provide access to data.
  - Keep multiple copies of the encrypted data key.

Tivoli Key Lifecycle Manager

The DS8000 supports data encryption with the use of Tivoli Key Lifecycle Manager and the IBM Full Disk Encryption feature.

The IBM Tivoli Key Lifecycle Manager implements a key server application and integrates with certain IBM storage products. It is software developed by IBM for managing keys securely for encrypting hardware devices such as disk and tape.

The Tivoli Key Lifecycle Manager server is available as a DS8000 hardware feature code 1760. This feature provides the Tivoli Key Lifecycle Manager server that is required for use with the Tivoli Key Lifecycle Manager software.

The Tivoli Key Lifecycle Manager can be installed on a set of servers to implement a set of redundant key servers. Encryption capable storage devices that require key services from the key server are configured to communicate with one or more key servers and the key servers are configured to define the devices to which they are allowed to communicate.

The Tivoli Key Lifecycle Manager supports two key serving methods. The method that is used by the DS8000 is referred to as the wrapped key method. In the wrapped key method, the configuration processes on the Tivoli Key Lifecycle Manager and storage device define one or more key labels. A *key label* is a user-specified text string that is associated with the asymmetric key pair that Tivoli Key Lifecycle Manager generates when the key label is configured. In the wrapped key method, there are basically two functions that an encryption capable storage device can initiate to a Tivoli Key Lifecycle Manager key server:

Request a new data key

The storage device requests a new data key for one or two specified key labels. The Tivoli Key Lifecycle Manager key server provides one or two properly generated data keys to the storage device in two forms:

Externally Encrypted Data Key

Tivoli Key Lifecycle Manager maintains a public and private key pair for each key label. Tivoli Key Lifecycle Manager keeps the private key a secret. The data key is wrapped with the key label public key and is stored in a structure that is referred to as the externally encrypted data key (EEDK). This structure also contains sufficient information to determine the key label associated with the EEDK. One EEDK is sent for each key label.

Session Encrypted Data Key

The storage device securely obtains the data key from the Tivoli Key Lifecycle Manager and then uses the data key to encrypt or decrypt other subordinate data keys.

Each EEDK is persistently stored by the storage device for future use. The session encrypted data key (SEDK) is decrypted by the storage device using the private key of the storage device to obtain the data key. The data key is then used to symmetrically encrypt and decrypt other subordinate data keys that are required to encrypt, decrypt, or gain access to the data.

Unwrap an existing data key

The storage device requests that Tivoli Key Lifecycle Manager unwrap an existing wrapped data key by sending the request to the Tivoli Key Lifecycle Manager instance with all of the EEDKs and the public key of the storage device. The Tivoli Key Lifecycle Manager key server receives each EEDK, unwraps the data key with the private key for the key label to obtain the data key, wraps the data key with the storage device public key to create an SEDK, and returns an SEDK to the storage device.

The storage device does not maintain a persistent copy of the data key. Therefore, the storage device must access the Tivoli Key Lifecycle Manager to encrypt or decrypt data. Each time the storage device is powered on, it must communicate with the Tivoli Key Lifecycle Manager to obtain the data key. Access to data that is encrypted with a data key requires access to both the EEDKs and the Tivoli Key Lifecycle Manager with the private key that is required to decrypt the EEDKs to obtain the data key.

On System z platforms, the length of the key labels is limited to 32 characters when the Tivoli Key Lifecycle Manager is configured to use a RACF® based key method (either JCERACFKS or JCECCARACFKS) is used. You must limit key labels to 32 characters on those key servers and on storage devices that must interoperate or share keys with zSeries key servers using RACF based key methods.

IBM Tivoli Key Lifecycle Manager server

The IBM Tivoli Key Lifecycle Manager (TKLM) server is available with feature code 1760. A TKLM license is required for use with the TKLM software. The software is purchased separately from the TKLM isolated server hardware.

The TKLM server runs on the Linux operating system (SUSE Linux Enterprise Server 10 Service Pack 3). You must register for Linux support with Novell. Go to the support.novell.com/contact/getsupport.html. Contact Novell directly for all Linux-related problems.

The TKLM server consists of software and hardware:

Hardware
The TKLM server hardware is a specially configured xSeries® server, incorporated into the DS8000 as hardware feature code 1760. For hardware-related problems, contact the IBM hardware support for assistance. Be prepared to provide the correct DS8000 machine type and serial number for which feature code 1760 is a part.

Software
The TKLM server includes licensed TKLM software, which you order separately. For TKLM-related problems, contact IBM software support. Be prepared to provide the software product identification (PID) when you call for assistance.

TKLM installation

The TKLM server is installed and configured by the IBM Lab Services group. After the TKLM server is configured, each installation receives key settings of parameters and a copy of the configuration along with recovery instructions. Should a server be replaced, you must reload the TKLM code and restore the TKLM configuration.

Before installing the TKLM server, you must configure the host name of the server in which TKLM is being installed. Ensure that you note and keep the host name of the server because the host name cannot be changed after configuration. (The DB2® database that is used by the TKLM server will not function without correct host names.) Not accessing correct host names can potentially result in temporary loss of access to the storage device that is being managed by the TKLM server.

If you are installing the TKLM server from the DVD that is included with your product, you can store the contents of the DVD in a temporary directory by using the following steps:

1. Right-click the DVD content diagram that displays after you insert the DVD into the media drive.
2. Select the `Extract to` option and navigate to the temporary directory where you want to store the DVD contents.

Note: For information on installation procedures (including post installation steps) for the TKLM, see the *IBM Tivoli Key Lifecycle Manager/Installation and Configuration Guide* that is included in the http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp.

After the installation of the application is complete, ensure that you set the TKLM application to `auto start` in case of a power outage at your facility. By doing so, you can significantly reduce the time it takes to recover from data loss caused by a power outage.

IBM Security Key Lifecycle Manager for z/OS

IBM Security Key Lifecycle Manager for z/OS generates encryption keys and manages their transfer to and from devices in a System z environment.

IBM Security Key Lifecycle Manager for z/OS is supported on the DS8000. Some of the benefits include, but are not limited to:

- Helps reduce the cost of lost data
- Enhances data security while dramatically reducing the number of encryption keys to be managed
- Centralizes and automates the encryption key management process
- Integrates with IBM self-encrypting storage devices to provide creation and protection of keys to storage devices

For more information, see the IBM Security Key Lifecycle Manager for z/OS Information Center.

DS8000 disk encryption

The DS8000 supports data encryption with the Full Disk Encryption (FDE) feature.

The FDE disks are standard on the DS8870. These drives encrypt and decrypt at interface speeds, with no impact on performance.

Recovery key and dual key server platform support is available on the DS8870. For a list of FDE drives, see “Disk drives” on page 26.

To enable encryption, the DS8000 must be configured to communicate with two or more Tivoli Key Lifecycle Manager key servers. The physical connection between the DS8000 HMC and the key server is through a TCP/IP network.

Each FDE drive has an encryption key for the region of the disk that contains data. When the data region is locked, the encryption key for the region is wrapped with an access credential and stored on the disk media. Read and write access to the data on a locked region is blocked following a power loss until the initiator that is accessing the drive authenticates with the currently active access credential. When the data region is unlocked, the encryption key for the region is wrapped with the unique data key that is assigned to this particular disk and stored on the disk media. This data key is accessible to the device and to any initiator that is attached and the wrapped key is stored on the disk media. Read and write access to the data on an unlocked region does not require an access credential or any interface protocols that are not used on a non-FDE drive. FDE drives still encrypt and decrypt data with an encryption key. However, the encryption and decryption is done transparently to the initiator.

For DS8000, the FDE drive that is a member of an encryption-enabled rank is locked. A FDE drive that is not assigned, a spare, or a member of an encryption-disabled rank is unlocked. Locking occurs when a FDE drive is added to an encryption-enabled rank. Unlocking occurs when an encryption-enabled rank is deleted or when an encryption-enabled rank member becomes a spare. Unlocking implies a cryptographic erasure of a FDE drive. FDE drives are also cryptographically erased when an encryption-disabled rank is deleted. You can cryptographically erase data for a set of logical volumes in an encryption-capable extent pool by deleting all of the ranks that are associated with the extent pool.

FDE drives are not cryptographically erased when the disk fails. In this case, there is no guarantee that the device-adapter intentionally fences the failing drive from the device interface as soon as possible to prevent it from causing any other problems on the interface.

A unique access credential for each locked drive in the SFI is derived from one data key that it obtains from the Tivoli Key Lifecycle Manager key server. The DS8000 stores multiple independent copies of the EEDK persistently and it must be able to communicate with a Tivoli Key Lifecycle Manager key server after a power on to allow access to the disks that have encryption enabled.

In the current implementation of an encryption-capable DS8000, data is persistently stored in one of the following places:

On your disks
Data on your disks (for example, DDM installed through DDM Install Group features) that are members of an encryption-enabled rank is managed through a data key obtained from the Tivoli Key Lifecycle Manager key server. The data is encrypted with an encryption key that is managed through an externally encrypted key. The data on disks that are members of a rank that is not encryption-enabled is encrypted with an encryption key that is encrypted with a derived key and stored on the disk. Therefore, this data is obfuscated.

NVS dump data on system disks
If you start a force power off sequence, write data in flight in the NVS memory is encrypted with an encryption key and stored on the system disk in the DS8000. The data is limited to 8 GBs. The encryption key is encrypted with a derived key and stored on the system disk, hence NVS data is obfuscated. The data on the system disk is cryptographically erased after power is restored and after the data has been restored to the NVS memory during the initial microcode load.

Atomic-parity update (APU) dump data in device flash memories
If a force power off sequence is initiated atomic parity write data in flight within the device adapter memory for RAID 6 arrays is encrypted with an encryption key. The data is stored in flash memory on the device adapter card in the DS8000 system, and is limited to 32 MB per device adapter or 512 MB per storage facility.

Note: The power off requests that are issued through the DS8000 Storage Manager, the command-line interface, or through the IBM System z power control interfaces do not start a Unit Emergency Power Off (UEPO) sequence. Activation of the UEPO switch or loss of AC power does start a power off sequence.

Recovery key configuration operations

A storage administrator must start the process to configure a recovery key for the DS8000 SFI before an encryption group is created. Each configured encryption group has an associated recovery key. You can use the recovery key to access data from an encryption group that is in a configured-inaccessible state when access to the encryption group data key through any key server is not possible.

The security administrator receives a 256-bit key that is generated from the SFI during the configuration process and must securely maintain it for future use if an encryption deadlock occurs. The SFI does not maintain a copy of the recovery key.

The storage administrator must then approve the recovery key configuration request for it to become active. During the configuration process, the following steps take place:

1. The security administrator initiates the configure recovery key function.
2. The SFI generates a recovery key and generates a secure hash of the recovery key producing the recovery key signature.
3. The SFI generates a random key pair (the private key is referred to as the primary recovery key and the public key is referred to as the secondary recovery key).
4. The SFI stores the encrypted primary recovery key, secondary recovery key, and recovery key signature for future use. The encrypted primary recovery key and secondary recovery key are stored in multiple places for reliability.
5. The SFI provides the recovery key to the security administrator.
6. The SFI sets the primary recovery key and recovery key to zero, puts the recovery key in the verify-pending state, and completes the configure recovery key function successfully.
7. The security administrator initiates the verify recovery key function and inputs the recovery key.
8. The storage administrator initiates the authorize recovery key function.
9. The storage facility image puts the recovery key in the configured state and completes the authorize recovery key function successfully.

Within a secure key environment, you might choose to disable the recovery key rather than to configure one. While disabling the recovery key increases the security of the encrypted data in the DS8000, it also increases the risk of encryption deadlock, described under “Encryption deadlock” on page 166.

If you choose to disable the recovery key, you are highly encouraged to strictly follow the guidelines included in “Encryption deadlock prevention” on page 168. Failure to do so might result in permanent loss of all your encrypted data managed by key servers, if an encryption deadlock occurs.

The state of the recovery key must be `Unconfigured` to disable the recovery key. The following includes the process of the recovery key:

1. The security administrator requests that the recovery key be disabled. This action changes the recovery key state from `Unconfigured` to `Disable Authorize Pending`.
2. The storage administrator authorizes the recovery key disablement. This action changes the recovery key state from `Disable Authorize Pending` to `Disabled`.

   Each encryption group configured has its own recovery key that might be configured or disabled. The current DS8000 implementation supports a single encryption group and a single recovery key.

It is possible to re-enable the recovery key of an encryption group once the encryption group is in the unconfigured state. This action implies a prerequisite break down of encrypted volumes, ranks, and extent pools. The following includes the process of enabling the recovery key:

1. The security administrator requests that the recovery key be enabled. This action changes the recovery key state from `Disabled` to `Enable Authorize Pending`.

2. The storage administrator authorizes the recovery key enablement. This action changes the recovery key state from `Enable Authorize Pending` to `Unconfigured`.
3. Normal recovery key configuration steps are followed to configure the recovery key prior to encryption group creation.

Encryption deadlock

An *encryption deadlock* occurs when all key servers that are within an account cannot become operational because some part of the data in each key server is stored on an encrypting device that is dependent on one of these key servers to access the data.

The key server provides an operating environment for the key server application to run in, to access its keystore on persistent storage, and to interface with client storage devices that require key server services. The keystore data is accessed by the key server application by using your specified password. The keystore data is encrypted independently of where it is stored. However, any online data that is required to initiate the key server cannot be stored on storage that has a dependency on the key server to enable access. If this constraint is not met, the key server cannot perform an initial program load (IPL) and therefore cannot become operational. This data includes the boot image for the operating system that runs on the key server as well as any data that is required by that operating system and its associated software stack to run the key server application, to allow it to access its keystore and to allow the key server to communicate with its storage device clients. Similarly, any backups of the key server environment and data must not be stored on storage that has a dependency on a key server to restore or access the backup data.

While an encryption deadlock exists, you cannot access any encrypted data that is managed by the key servers. If all backups of the keystore are also stored on encrypting storage that is dependent on a key server, and you do not have the recovery keys that would unlock the storage devices, the encryption deadlock can become a permanent encryption deadlock such that all encrypted data that is managed by the key servers is permanently lost.

Note: To avoid encryption deadlock situations, ensure that you follow the guidelines outlined in “Encryption deadlock prevention” on page 168.

With encryption-capable disks, the probability of an encryption deadlock increases significantly because of the following factors:

- There are a number of layers of virtualization in the I/O stack hierarchy that make it difficult for you to determine where all the files that are necessary to make the key server and its associated keystore available are stored. The key server can access its data through a database that runs on a file system on a logical volume manager which communicates with a storage subsystem that provisions logical volumes with capacity that is obtained from other subordinate storage arrays. The data that is required by the key server might end up provisioned over various storage devices, each of which might be independently encryption-capable or encryption-enabled.
- Various layers within this I/O stack hierarchy can provide transparent data relocation either autonomically or because of a user-initiated operations.
- As the availability of encryption-capable devices becomes more pervasive, more data is migrated from non-encrypted storage to encrypted storage. Even if the key servers are initially configured correctly, it is possible that a storage

administrator might accidentally migrate some data that is required by the key server from non-encrypted to encrypted storage.

- Consolidation of servers and storage tends to drive data migration and tends to move more data under a generalized shared storage environment which tends to be encryption-capable as time goes on.
- The ability to detect that the data access of a key server has been compromised cannot be detected except by power cycling the entire environment which results in the deadlock if the access of a key server has been compromised. Even with multiple key servers, it might not be possible to detect that all key servers except one are dependent on the operation of the last key server such that a single additional change that compromises the access of the last key server is all that is required to enable the encryption deadlock.
- All IBM server platforms support fabric-attached boot devices and storage. Some IBM servers do not support internal boot devices. It is common for boot devices to be present within the generalized storage environment and accessible to generalized storage management tools that support data management and relocation.

To reduce the risk of encountering an encryption deadlock, you must be directly involved in managing the encryption environment.

Best practices for encrypting storage environments

The recommended techniques for security, availability, and encryption deadlock prevention should be implemented to mitigate the risk of an encryption deadlock.

Security

Ensuring the physical and network security of key server hardware as well as the access security of the keystore password are among the best practices for the encryption of your storage environments.

General

When possible, provide additional physical security around hardware and media elements that are associated with the key servers. You can also provide additional network security around hardware that is associated with key servers.

Keystore

The initiation of a Tivoli Key Lifecycle Manager key server involves the specification of a password that is used to access the keystore. You must decide whether the Tivoli Key Lifecycle Manager password must be provided manually or whether there is some mechanism to automatically provide the password to the Tivoli Key Lifecycle Manager. If a startup script is used on the Tivoli Key Lifecycle Manager server that contains the password, the script file must have access controls to prevent unauthorized access to the file and password. For example, the file permissions cannot allow read, write, or run access by unauthorized users.

Availability

Ensuring the availability of key servers through the recommended configurations are among the best practices for the encryption of your storage environments.

Key server

- Configure key servers to automatically power on when power is available and to automatically initiate the key server application.
- Configure the key server application to automatically start.

- Configure redundant network fabrics between key servers and encrypting storage. Most storage products support two or more network connections. To improve robustness, provide independent network paths through independent to independent key servers.
- Define multiple security administrators and multiple storage administrators on DS8000 storage facility images so that the loss of access to one administrator does not prevent the ability to use a recovery key for recovery purposes.

DS8000

Configure the DS8000 with the dual HMC option to provide redundant access to your network. Dual HMCs can be provided by cross-coupling the HMCs on two DS8000 systems or by providing an additional stand-alone HMC for a single DS8000. The inability of a DS8000 to communicate with a key server when it powers on prevents access to encrypted storage on the DS8000.

Encryption deadlock prevention

Ensuring the proper configuration and operation of all key servers are among the best practices for the encryption of your storage environments while maintaining access to your data.

General

- All personnel capable of configuring Tivoli Key Lifecycle Manager key servers, configuring any encrypted storage products, or managing the placement or relocation of data related to any Tivoli Key Lifecycle Manager key servers must review, understand, and adhere to the information in this document.
- The change management processes at your installation must cover any procedures that are required to ensure adherence to guidelines for proper configuration of key servers, encrypted storage, and data placement.
- You must implement automated monitoring of the availability of any equipment that is associated with management of key services and take appropriate action to keep them operational. This equipment includes but is not limited to key servers, SNMP masters, domain name servers, and DS8000 HMCs.
- Review disaster recovery plans and scenarios and consider the availability of key servers, key server backups, and key server synchronization. When possible, each recovery site must be independent of other recovery sites. Isolate network paths to remote key servers in the context of a site power cycle to test that the key servers at that site are not encryption deadlocked within that site. If such a test is performed, it might be helpful to attempt the power cycle with the isolated key servers offline to verify that the key servers that are not isolated are not encryption deadlocked.

Key Server

- Configure redundant key servers. Redundancy implies independent servers and independent storage devices. For key servers operating in LPARs, do not use data sharing techniques that result in one copy of the data being shared by multiple instances of the key server.
- Configure two or more key servers to have a dedicated server and dedicated non-encrypted storage resources. This requirement physically localizes and isolates the key server environment to a set of hardware

components with known lack of dependency on a key server such that the potential for migrating the key server data outside of the environment becomes negligible with appropriate controls and processes. These key servers are referred to as *isolated key servers*. The DS8000 requires at least one isolated key server be configured, but you must have two for redundancy.

- You can configure additional key servers on generalized server hardware and generalized storage. However, appropriate procedures and controls must be established to prevent these key servers from having their data access compromised by storing the data on key server managed encrypting storage. These key servers are referred to as *general key servers*.
- Configure key servers at independent sites to provide additional immunity to encryption deadlocks because it reduces the probability for all key servers to experience a simultaneous power loss.
- The utilization of uninterruptible power supply units on certain key servers can provide additional immunity to an encryption deadlock.
- The initiation of a Tivoli Key Lifecycle Manager key server involves the specification of a password that is used to access the keystore. Ensure appropriate retention of the password and limit access to the password to appropriate personnel. Loss of a password is a cryptographic erasure of the keystore for the associated key servers. Loss of one or more redundant key servers increase the probability of an encryption deadlock. The permanent loss of all encryption key servers is equivalent to a permanent encryption deadlock.
- You must ensure that all key servers that a storage device is configured to and communicate with have consistent keystore content relative to any wrapping keys that are to be used by the storage device. Any wrapping keys to be used on any key server must be propagated across the set of key servers that are associated with a storage device before the storage device is configured to use those wrapping keys. Failure to synchronize the keystores effectively eliminates one or more key servers from the set of redundant key servers for a device that uses the keys that are not synchronized.
- Backup key server data after it is updated. The backups must not be stored on encrypted storage media that is dependent on a key server.
- Periodically audit all online and backup data that is required to make each key server operational to ensure that it is stored on storage or media that is not dependent on a key server to access the data.
- Do not delete keys on the key server under normal circumstances. The appropriate action to remove a key from a key server is almost always to archive the key. If the wrong key is inadvertently archived causing the loss of access to encrypted data at some point in the future, the archive action allows the key to be restored. Deletion of all copies of a key is a cryptographic erase of all encrypted data that is encrypted under this key.

DS8000

- Recovery keys must be configured and must be securely maintained. As a security or precautionary measure, ensure that you rekey your data key labels for your encryption group periodically. Ensure that the data keys for the primary key label and the secondary key label are unique.

The availability of a recovery key does not eliminate the requirement for configuring isolated key servers or for properly configuring general key servers. If a recovery key is needed to break an encryption deadlock, an outage is already in progress.

- Manually configure DS8000 devices on the Tivoli Key Lifecycle Manager key server. The option to automatically configure them can be used, but increases the risk that an unauthorized DS8000 might gain access to a key server. In addition, automatic configuration associates the device with the default key label. Manual configuration allows the device to be associated with a specific key label so that this association can be detected and can possibly help avoid accidental archival or deletion of an active key label.
- Each DS8000 storage facility image must be assigned a unique key label on the Tivoli Key Lifecycle Manager to facilitate the independent management of each storage facility image.
- The DS8000 supports the attachment of up to four key servers. If encryption is enabled, you must configure a minimum of two key servers to theDS8000. At least one of the key servers that is configured on the DS8000 must be an isolated key server. However, ensure that you configure two isolated key servers on the DS8000. Any other key servers that are configured on the DS8000 can be general key servers. Key servers at the local site are preferable over key servers at a remote site to improve reliability during a site failure.
- The DS8000 verifies that at least two key servers are configured, enabled, and accessible to the DS8000 when the DS8000 is configured to enable encryption. This condition is checked when a encryption-enabled DS8000 is configuring a non-zero encryption group. Encryption group configuration request is rejected if this condition is not met.
- If encryption has not been activated on the DS8000, the DS8000 rejects the configuration of ranks and extent pools with a nonzero encryption group specified.
- The DS8000 monitors all configured key servers. Notification is provided for loss of access to key servers and other key server related errors through DS8000 notification mechanism. For example, SNMP traps and or email. Ensure that you set up monitoring for these indications and take corrective action when a condition is detected which reflects a degraded key server environment. The following conditions are monitored and reported:
  - If at power on, the DS8000 cannot obtain a required unwrapped data key for a configured encryption group from a key server, it reports an error condition to both you and IBM. In this case, the encrypted logical volumes that are associated with the encryption group are not accessible to attached hosts. If subsequent to reporting this error, the DS8000 is able to obtain the required key services from a key server, it reports the condition to both you and IBM and makes the associated logical volume accessible.
  - DS8000 access to each configured key server is verified at five minute intervals. Loss of access is reported to you.
  - The ability of each key server to unwrap data keys that are configured on the DS8000 is verified at 8 hour intervals. Loss of the ability unwrap a configured data key is reported to both you and IBM.

  - The DS8000 detects if there are fewer than two key servers configured, or fewer than two key servers that are available, or there are fewer than two key servers that can unwrap data keys configured on the DS8000 at 8 hour intervals. If detected, this condition is reported to both you and IBM.

Tape Related
Validate keystore backups to assure they are not being encrypted. Validation can be performed by reading the backup through a storage device that has been confirmed as being not encryption capable or as having no access to a key manager.

Encrypted storage installation guidelines

For a successful installation, ensure that you understand and follow the guidelines for installing encryption-capable storage devices.

The following guidelines apply:

- You must have an isolated key server that meets the following hardware and software requirements:
  - IBM System L5420 with the following specifications:
    - Server
    - 6 GB memory
    - 146 GB SAS RAID 1 storage
    - Dual gigabit Ethernet ports
    - SUSE Linux 9.0 (32 bit)
    - Power supply
  - Tivoli Key Lifecycle Manager that includes DB2 9.1 FB4

  Important: The hardware is the same as that is used for the **Tivoli Storage Productivity Center**. However, a different software load has been installed by manufacturing. No other hardware or software is allowed on this server. An isolated server must only use internal disk for all files necessary to start and have the Tivoli Key Lifecycle Manager key server operational.
- You must have at least one isolated key server per site. This key server can be configured to serve keys to any Tivoli Key Lifecycle Manager supported device, including IBM tape.
- You must configure at least one isolated key server to each DS8000 that is encryption enabled.
- You must configure at least two key servers to each DS8000 that is encryption enabled.
- To use encryption on a DS8000, you must be certified for using encryption on each DS8000 storage facility image (SFI). After you are certified, IBM enables the encryption function on the SFI.

The ordering, installation, and encryption activation of an encryption-capable DS8000 involves the following steps:

1. You order a DS8000 from IBM with encryption-capable DDMs.
2. IBM delivers the DS8000 and the IBM service representative installs the DS8000.
3. You configure the key servers to be used with the DS8000. IBM Lab Services or IBM Global Services can be contracted to assist with the setup of the key servers.

4. You configure the Tivoli Key Lifecycle Manager to add the DS8000 SFIs to the device table and configure a key label for the DS8000 SFIs.
5. You configure the DS8000 with the IP addresses of the associated key server ports.
6. Before you configure an encryption group, configure a recovery key either configure a recovery key or disable it. You configure an encryption group on the DS8000 SFIs with a key-label defined on the Tivoli Key Lifecycle Manager.
7. You request encryption certification for the DS8000 SFIs. Encryption certification consists of:
   - You contract IBM Lab Services to provide education and to validate the configuration of key servers that are configured with the DS8000.
   - You notify the IBM sales team that they are ready to activate encryption on the DS8000 SFI.
8. IBM files your agreement and authorizes a LIC authorization key to activate encryption on the SFI. Each LIC authorization key is unique to the SFI for which it is generated.
9. You install the LIC authorization key on the SFI.
10. You can now configure ranks or extent pools for the configured encryption group.

    Notes:

    a. All ranks and extent pools on a given encryption-capable DS8000 SFI must be configured with the same encryption group attribute. The first rank or encryption group that is configured determines what the remaining objects must be configured with. A value of 0 indicates encryption-disabled. A value of 1 indicates encryption enabled. The value 0 can only be specified when there are no encryption groups configured. The value 1 can only be specified when encryption group 1 is configured.

    b. To change between encryption-enabled and encryption-disabled, all ranks and extent pools must be deconfigured. Deconfiguring an encryption-enabled rank causes any data that is stored on the rank to be cryptographically erased and then overwritten to reinitialize the rank. Additionally, if encryption is to be enabled, encryption group 1 must be configured. If encryption is to be disabled, encryption group 1 must be deconfigured.

For the latest available encryption-related best practices and guidelines, go to the IBM Support website at: www.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5081492.

Guidelines and requirements for key server management

Ensure that you are aware of the guidelines and requirements for managing your key servers.

The following guidelines and requirements apply:

- You are responsible for maintaining the physical and logical security of key servers.
- You are responsible for maintaining synchronization of keystores between key servers and for backup of keystore information.
- Back up the key server any time new keys are created that are to be maintained by the key server. Ensure that you perform a backup before these new keys are

used by any client storage devices. For example, before the device is configured to communicate with the key server to request data keys for the associated key label.

- If you provide more than one type of key server, you must use the key export method to transfer keys between heterogeneous key server types. Backup and restore methods can be used between homogeneous key servers.

Exporting and importing keys between key server instances

If you have key servers with different operating systems, you must use the Tivoli Key Lifecycle Manager export method to transfer keys between key server instances.

This task provides the steps to use Tivoli Key Lifecycle Manager to export and import files between key server instances. For more information about Tivoli Key Lifecycle Manager, go to the Tivoli Key Lifecycle Manager section at the IBM Tivoli Information Center .

Perform the following steps to transfer keys:

1. To list all of the known DS8000 devices, run the **tklmDeviceList** command with the **-type** parameter set to DS8K and the **-v** parameter set to y. The following is an example of the command and output:

   ```
   wsadmin>print AdminTask.tklmDeviceList ('[-type DS8K] [–v y]')
   CTGKM0001I Command succeeded.
   Description = salesDivisionDrive
   Serial Number = CCCB31403AFF
   Device uuid = DEVICE-5023fd36-cf2a-4406-80cc-fc2ed4065460
   Device type = DS8K
   World wide name = 61041
   Key alias 1 = certb Key
   alias 2 = certb
   ```

2. Issue the **tklmServedDataList** command to list all the keys that have been served to all devices.
3. Compare the command output from step 1 and step 2.
4. Record alias 1.
5. Verify that this alias is associated with the device. If it is not associated with the device, record the alias that is associated with the device.
6. Repeat steps 3 to 5 until all drive serial numbers and aliases have been recorded.
7. For each alias, issue the **tklmKeyExport** command with the **-type** parameter set to privatekey. This command creates a file for each key alias. The following is an example of the command and output:

   ```
   wsadmin>print AdminTask.tklmKeyExport ('[ -alias certa -fileName mysecretkeys1
    -keyStoreName "Tivoli Key Lifecycle Manager Keystore" -type privatekey
    -keyAlias certa]')
   ```

8. Transfer the files created in step 7 to the server where the second Tivoli Key Lifecycle Manager instance is running.
9. For the second Tivoli Key Lifecycle Manager instance, ensure that the **ds8k.acceptUnknownDrives** parameter is set to *true* in the Tivoli Key Lifecycle Manager configuration file to allow requests from unknown DS8000 storage images.

10. For the second Tivoli Key Lifecycle Manager instance, issue the **tklmKeyImport** command for each of these files. The password that you must specify is the password that was used for the keystore of the Tivoli Key Lifecycle Manager server for which the files were created.
11. Optionally, add the DS8000 devices listed in step 1 on page 173 to the second Tivoli Key Lifecycle Manager instance using the **tklmDeviceAdd** command.

DS8000 encryption considerations

Information pertaining to DS8000 Storage Manager and Tivoli Key Lifecycle Manager support and capabilities should be considered for the use of encryption on the DS8000.

The following information might be helpful in using data encryption on DS8000:

- DS8000 ships from the factory with encryption disabled on each SFI. You must follow the procedures described to have IBM activate encryption on each DS8000 SFI.
- An encryption-capable DS8000 can be configured to either enable or disable encryption. Ensure that the needed configuration is achieved before storing data on any configured storage.
- The DS8000 Storage Manager and command-line interface must be upgraded to the appropriate level to enable encryption on an encryption capable DS8000. If you use an earlier version of DS8000 Storage Manager and command-line interface, the DS8000 is configured with encryption disabled.
- CIM support for DS8000 encrypting storage at this time does not support the configuration of Tivoli Key Lifecycle Manager IP ports, encryption groups, encrypting ranks, or encrypting extent pools. A system that is configured with encrypting extent pools can use the CIM agent to configure encrypting logical volumes and host attachments for encrypting logical volumes.
- Tivoli Key Lifecycle Manager has a policy input for setting the length of time that key label remains valid. For example, the validity period for a new certificate. This input controls the time that a key label supports requests for a new data key. It does not prevent any existing data keys created for that key label from being unwrapped. This input is set for each key label as it is created. Because disks typically obtain a new key after an encryption group is configured, the expiration of the certificate is not significant to the going operation of currently installed and configured encryption groups. It affects whether a new encryption group can be configured with that key label. The default validity period is 20 years.
- When using the RACF on z/OS 1.9, the RACF keystore does not support 2048-bit data keys. Tivoli Key Lifecycle Manager generates 1024 bit wrapping keys when running on this operating system. Tivoli Key Lifecycle Manager key servers that run on other operating systems can import 1024 bit wrapping keys and even though they generate 2048 bit wrapping keys. To support export of keys between z/OS 1.9 and other key server operating systems, key labels must be created on the z/OS and exported to the other operating systems.
- When using the RACF on z/OS 1.10, the RACF keystore supports 2048-bit data keys. There is no limitation on which Tivoli Key Lifecycle Manager operating system is used to create key labels.
- When using the ICSF on z/OS, the ICSF keystore supports 2048-bit data keys. ICSF **Secure Key** mode must be selected in a server configuration that has an isolated key server and System z server. In this case, the isolated key server and System z server share public keys and a public-private key pair is shared

between System z servers in a secure key mode. The procedure to do a public key exchange is different from the procedure to do a public/private key exchange.

Virtual private network

A virtual private network (VPN) is a private network that securely connects corporate networks across the Internet to remote offices and users.

A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. A VPN provides user authentication, data encryption, and data integrity to ensure the security of the data while in transit across private networks and the Internet.

VPNs securely convey information across the Internet by connecting remote users, branch offices, and business partners into an extended corporate network. Many companies are replacing their existing telecommunications infrastructure with VPNs, by implementing secure IP tunnels across the Internet between corporate sites as well as to business partners and remote users.

Because security is a critical issue for companies worldwide, VPN connections provide a secure infrastructure that require systems to work together to mitigate the risk of malicious activity from both external and internal sources. Any connection from your network to the public Internet raises some of the following security concerns:

- Infection by viruses
- Intrusion by hackers
- Accessibility of your data from a remote support site
- Authorization of remote users to access your machine when a remote connection is opened

IBM VPN connections, along with the security features that are built into the DS8000 storage unit, make it possible to access IBM service representatives who can assist you in resolving complex problems without the risks that are associated with a connection to an external network. For information about the IBM VPN implementation including technical details, go to the www.ibm.com/support/docview.wss?uid=ssg1S1002693.

In addition, your IBM representative can inform you about other remote connectivity options, including modem-less operation of the DS8000.

Appendix C. IBM-provided DS8000 equipment and documents

Use the documents that IBM ships with your DS8000 models to identify and check your main components.

The equipment that you receive can be grouped as follows:

- Components that must stay with the shipment because they are needed for installation
- Components that are for customer use
- Components that must stay with the storage unit after installation because they are needed by service representatives

Note: These lists are not intended to be a comprehensive lists. They describe only the main shipped components.

Installation components

Your shipment includes all the equipment that is needed for the installation of your storage units. Equipment includes storage units, power cords, adapters, cables, installation instructions and other essential material.

The following installation components are included with your shipment:

- **Storage unit**

  Your shipment includes one or more of the following models that you ordered:
  - Model 961 (base)
  - Model 96E (expansion)

  When your models arrive, they contain any ordered I/O enclosures, device adapters, disk enclosures, disk drives, and the appropriate cables to support those components. IBM installs these components at the factory.
- **IBM System Storage Management Console**

  A laptop-based Management Console is included with each base model that you order. The management console is physically located (installed) inside the base unit.

  If you order an external management console, you receive this separate workstation, the necessary Ethernet cables, and any required installation hardware to install the external management console to the rack that you provide. The IBM service representatives install the external management console into an IBM or a non-IBM rack when they install your storage unit.
- **Power cords**

  Your shipment includes the country or region-specific power cord that you ordered.
- **Various media**

  IBM ships the following media (typically CDs), which are used during the installation of your storage units:
  - Installation media, which includes installation scripts for the I/O attachment for AIX and HP-UX, IBM System Storage DS CLI (command-line interface) software, and IBM Multipath Subsystem Device Driver installation instructions and software

  - Licensed machine code (LMC) media for the MC
  - Operating system media
  - LMC media for the /242x machine type
  - Quick Code Reference document that details program code, utilities, and documentation included in the ship group
- **Hardcopy installation instructions**

  Your shipment includes hardcopy installation instructions for the IBM service representatives who install your storage unit.
- **Engineering changes (if applicable)**

  IBM occasionally releases engineering changes (ECs) to correct problems or provide additional support. If released, these ECs are included in your shipment for the IBM service representative to install.

Customer components

IBM ships DS8000 media and documents that are intended for you to keep.

- License and warranty documents
- READ ME FIRST for IBM System Storage Products
- Quick Code Reference, which includes a listing of customer publications and media included in the DS8000 ship group
- **DS8000 customer publications CDs:** One CD contains PDFs of customer publications and the other CD contains PDFs of license and warranty documents.

Service components

IBM ships service-related media and documents with your DS8000 shipment.

Keep the following components with your storage unit so that IBM service representatives can use them when they service your storage unit.

Service media

Your delivery includes the following media for IBM service representatives to use:

- Operating system media
- Management console media:
  - Management console critical backup SDHC memory card
  - Dump, trace, statesave SDHC memory card, which IBM service representatives use for extracting statesave information during service
- A program temporary fix (PTF) CD for the operating system
- Service documents CD, which includes the following documentation: DS8000 information center and the DS8000 parts catalog.

Appendix D. Company information work sheet

Use the company information work sheet to provide basic information about your company and administrator, as well as general system information.

Purpose

IBM service representatives use the information that is provided on the company information work sheet to customize your IBM storage complex. When you use any of the remote support features, the management console sends this information to IBM so an IBM service representative can contact you.

You must complete the Table 65 work sheet for all installations that include a management console.

Note: Management console is abbreviated as MC in the work sheet.

Table 65. Company information work sheet

Item or setting	Instructions	Your information
Company name	Provide the name of your company. IBM service representatives use this information to identify your company when they receive call home reports from your IBM storage system. Ensure that the company name that is provided here is consistent with all other machines that correspond to your IBM customer account.	
Customer number	Provide the customer number that is assigned by IBM to your company.	
Administrator information Provide information about your storage system administrator in the following section.		
Administrator name	Provide the name of the individual at your site who service representatives can contact about IBM storage system service matters.	
Administrator email address	Provide the email address that can be used to contact the administrator.	
Administrator telephone number	Provide the primary telephone number for service personnel to use to contact the storage system administrator. Include the area code and the country code, if appropriate.	

Table 65. Company information work sheet (continued)

Item or setting	Instructions	Your information
Alternate telephone number	Provide an alternate or off-shift telephone number that IBM service representatives can use to contact the storage system administrator. Include the area code and the country code, if appropriate.	
Fax number	Provide the primary fax number that IBM service representatives can use when they must fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	
Alternate fax number	Provide an alternate fax number that service personnel can use when they must fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	
Administrator's mailing address	Provide the mailing address for the administrator. Specify the complete address, including the street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Storage system information Provide basic information about your storage system and the management console in the following section.		
System location	If different from the administrator's address, provide the full address where the storage unit is located. Include the street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Modem number (MC1)	For the first MC to take advantage of inbound remote services, Provide the telephone number to the modem of the first MC in the storage complex. Include the area code and the country code, if appropriate.	

Table 65. Company information work sheet (continued)

Item or setting	Instructions	Your information
Modem number (MC2, if installed)	For a second MC to take advantage of inbound remote services, provide the telephone number to the modem of the second MC. Include the area code and the country code, if appropriate.	

Appendix E. Management console network settings work sheet

Specify basic network information on the management console network settings work sheet. Indicate your management console identification, Ethernet settings, DNS settings, and other required information.

When your storage unit sends IBM any call home information through VPN or sends you notices about serviceable events (using SNMP trap or email), these settings are included in the information to identify and provide important information about the management console that has sent a service request.

Work sheet purpose

IBM service representatives use the information you provide on the management console network settings work sheet to set up the network settings that support your management console.

You must complete this work sheet for all installations that include a management console.

Work sheet and instructions

The IP addresses and name server information shown on this work sheet are examples only. Contact your IBM service representative for the correct IP addresses and name servers that function with your DS8000 system. Complete the Table 66 work sheet to provide the IBM service representatives information about how to set up your network settings.

Note: Management console is abbreviated as MC in the work sheet.

Table 66. Management console network settings work sheet

Item or Setting	Instructions	MC1	MC2 (if applicable)
MC name (console name)	Record the console name that you want to assign to the management console workstation (for example, **dsmc1**). The console name and the domain are used to identify the MC to the network.		
Domain name	Provide the domain name that you are assigning to the MC workstation (for example, **medina.xyz.it**).		
Console description	Optional field to enter additional details to further describe this storage facility.		

Table 66. Management console network settings work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
MC time and time zone	Check **Use local time and time zone** to set the MC to the local time and time zone (local to where the MC physically resides). If you want to use a different time zone, check **Use the following time zone** and specify the time zone to use (for example, **Central European Time** or **US Pacific Time**).	_Use local time and time zone _Use the following time zone: ________________	_Use local time and time zone _Use the following time zone: ________________
NTP time server	List one or more external NTP time servers and the NTP protocol version. The time server must be reachable from the HMC. Only HMC 1 needs to be setup for an external time server.	NTP time server IP address or hostname: NTP protocol version: NTP time server IP address or hostname: NTP protocol version:	Not applicable
Ethernet settings Complete the LAN Adapter details section when the MC connects to your LAN.			
Media speed (Ethernet)	Check **Autodetection** or the media speed of the Ethernet adapter. Tip: If you check **Autodetection**, the MC can automatically select the media speed appropriate for your configuration.	**_Autodetection** _10 Mbps Half Duplex _10 Mbps Full Duplex _100 Mbps Half Duplex _100 Mbps Full Duplex _1000 Mbps Half Duplex _1000 Mbps Full Duplex	**_Autodetection** _10 Mbps Half Duplex _10 Mbps Full Duplex _100 Mbps Half Duplex _100 Mbps Full Duplex _1000 Mbps Half Duplex _1000 Mbps Full Duplex
TCP/IP interface address	- Ensure that the TCP/IP address that you select is not in a range that is reserved for the 242x private network. For more information, see "TCP/IP address ranges" on page 186. If you plan to use the IBM Internet VPN connectivity with the Network Address Translation (NAT), the IP address for the MC must be a routable private address (RFC1981) that is not already available on the Internet. - Record the dotted decimal address that you are assigning to the MC (for example, **7.127.152.14**).		

Table 66. Management console network settings work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
242x private network address ranges	Can the default 242x private network address ranges be used? For more information, see "TCP/IP address ranges" on page 186.	[ ] Yes: Use default ranges. [ ] No: Check off the address range option to use. Table 68 on page 187 provides the addresses associated with each option. [ ] Option 1 [ ] Option 2 [ ] Option 3	[ ] Yes: Use default ranges. [ ] No: Check off the address range option to use. Table 68 on page 187 provides the addresses associated with each option. [ ] Option 1 [ ] Option 2 [ ] Option 3
IPv4 and IPv6 config-uration	Select if the HMC is connected to an IPv4 network, an IPv6 network, or a network that supports both IPv4 and IPv6. Select IPv6 only if you plan on assigning or autoconfiguring IPv6 addresses.	IPv4 only [ ] IPv6 only [ ] Both IPv4 and IPv6 [ ]	IPv4 only [ ] IPv6 only [ ] Both IPv4 and IPv6 [ ]
TCP/IP interface network mask	Record the dotted decimal network mask that you want to apply to the TCP/IP address (for example, **127.123.546.0**).		
DNS settings Complete this section if you plan to use a domain name server (DNS) to resolve network names.			
Name server (DNS) internet address 1	Provide the dotted decimal address of the name server to be accessed by the MC workstation (for example, **5.127.42.25**).		
Name server domain name 1	Provide the domain name of the name server (for example, **medina.xyz.it**).		
Name server (DNS) internet address 2 (Optional)	Provide the dotted decimal address of the second name server that this workstation can access (for example, **5.127.42.252**). **Tip:** You can specify a second name server when you configure a backup or secondary server for Copy Services.		
Name server domain name 2	If you have a second name server, provide the domain name of the second name server (for example, **medina2.xyz.it**).		
Routing settings Complete the following section if you want to specify a default gateway for routing. (See Note following this table)			
Gateway address	Confirm and record the dotted decimal or symbolic name address of the gateway (for example, **8.127.155.254** or **londongate**).		

Table 66. Management console network settings work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
Note: Options that are in bold in the MC1 and MC2 columns indicate default settings.			

TCP/IP address ranges

When you select a management console TCP/IP address, ensure that you do not create a TCP/IP address conflict between your network and the 242x private network.

Use the following guidelines to prevent an address conflict:

- The management console TCP/IP address that you select must not be in the same address range as the address used by the 242x private networks.
- The TCP/IP addresses used by the 242x private networks must be outside the address ranges used by any network that the management console can reach.
- The 242x private network has one default address range. If the default address range cannot be used because it conflicts with another network, you can instead specify one of three optional addresses ranges.
- The IBM service documentation can refer to the two private networks as "black" and "gray" regardless of which address range has been assigned.
- Table 67 and Table 68 on page 187 can help you determine the 242x private network address range that the IBM service representative sets during the installation.

Use Table 67 to determine whether the default address range can be used.

Table 67. Default TCP/IP address range determination

Question:	If the answer is no...	If the answer is yes...
Do any of your networks to be reached by the management console use either of these address ranges: • 172.16.0.0 to 172.16.255.255 (172.16.0.0/16) • 172.17.0.0 to 172.17.255.255 (172.17.0.0/16)	There is not a potential address conflict. The default 242x private network address ranges can be used. In Table 66 on page 183, use the following instructions: 1. In the MC1 or MC2 column of the **TCP/IP interface address** row, as appropriate, enter the IP address for the management console. 2. In the MC1 or MC2 column of the **242x private network address ranges** row, as appropriate, check Yes.	There might be an address conflict between your networks and the 242x private networks. Your service representative must reconfigure the 242x private networks to use one address range option from Table 68 on page 187. 1. In Table 68 on page 187, select only one address range option for the242x private network that does not create a potential address conflict. 2. In Table 66 on page 183, in the MC1 or MC2 column of the **242x private networks address ranges** row, as appropriate, check the address range option that you selected from Table 68 on page 187.

If the default address range cannot be used, use one of the optional TCP/IP address range options provided on Table 68 on page 187.

Note: The options in the table are listed from most preferable (Option 1) to least preferable (Option 3).

Table 68. Address ranges of the storage facility private network (LIC bundles 75.xx.xx.xx and above)

	Address range	
Setting	**Black network (HMC eth0)**	**Gray network (HMC eth3)**
Default	172.16.0.0 to 172.16.2.255	172.17.0.0 to 172.17.2.255
Option 1	10.235.0.0 to 10.235.2.255	10.236.0.0 to 10.236.2.255
Option 2	192.168.160.0 to 192.168.162.255	192.168.240.0 to 192.168.242.255
Option 3	9.15.0.0 to 9.15.2.255	9.16.0.0 to 9.16.2.255

IPv6 configuration

Use the options that are provided in Table 69 to configure the HMC for communication over an IPv6 network.

Table 69. IPv6 configuration options

Item or setting	**Instructions**	**MC1**	**MC2**
IPv6 Autoconfig options	Select the autoconfig method for connecting the HMC to an IPv6 network. You can check more than one option.	Autoconfigure IP addresses [ ] Use privacy extensions for autoconfiguration [ ] Use DHCPv6 to configure IP settings [ ]	Autoconfigure IP addresses [ ] Use privacy extensions for autoconfiguration [ ] Use DHCPv6 to configure IP settings [ ]
Static IPv6 address	List the static IPv6 addresses that you want to assign to the HMC. Example IPv6 address: fe80:0:0:0:214:5eff:fe74:7ca8 Example prefix: 64	IPv6 address: Prefix length: IPv6 address Prefix length:	IPv6 address: Prefix length: IPv6 address Prefix length:

Appendix F. Remote support work sheets

These work sheets allow you to specify the outbound (call home) and inbound (remote services) settings.

The remote support work sheets allow you to specify the settings to use for outbound and inbound remote support.

There are two remote support work sheets:

- Outbound (call home) work sheet
- Inbound (remote services) work sheet

Outbound (call home and dump/trace offload) work sheet

The outbound work sheet provide settings for the IBM call home feature and the dump/trace delivery method.

When the IBM service representative sets up the call home feature, the storage system automatically requests service from an IBM service representative when the system identifies a serviceable event. IBM service representatives can then analyze the problem without you having to alert them. The dump and trace offload transmissions provide the necessary information for IBM service representatives to quickly troubleshoot serviceable events.

Note: The IBM call home feature must be configured if you participate in the Standby Capacity On Demand program.

Work sheet purpose

IBM service representatives use the information that is provided on the outbound (call home) work sheet to customize your storage system to use or disable the call home feature.

Work sheet and instructions

Notes:

1. Bold options in the MC1 and MC2 columns indicate default settings.
2. Management console is abbreviated as MC in the following table.

Table 70. Outbound (call home) work sheet

Item or Setting	Instructions	MC1	MC2 (if applicable)
Enable Call Home feature?	If you want IBM to enable the IBM call home feature, check **Yes** and then check the modes to use for call home. (You can select one or more modes. The attempted order of connectivity options is Internet SSL, Internet VPN, and then modem.) If you choose not to enable IBM call home, check **No**. If you select **No**, you have completed this work sheet.	[ ] **Yes** Modes: [ ] By modem [ ] By Internet VPN[1] [ ] By Internet SSL[2] [ ] **No**	[ ] **Yes** Modes: [ ] By modem [ ] By Internet VPN[1] [ ] By Internet SSL[2] [ ] **No**

Table 70. Outbound (call home) work sheet (continued)

Item or Setting	**Instructions**	**MC1**	**MC2 (if applicable)**
Although any combination of modes works, usually either **By Internet VPN** or **By Internet SSL** is configured, depending on your companies network security policies. It is not required to enable those two modes together. Selecting the modem is always recommended as a backup path for VPN or SSL and as a vehicle for unattended remote access.[1] Selecting **By Internet VPN** means that you allow your management console to use VPN over an Internet connection when a connection is established to the IBM service center. The IBM VPN implementation is a client/server VPN that is only active when it is needed. The two VPN endpoints are on the management console and on the IBM Boulder and the IBM Rochester VPN servers. There is no need for additional VPN hardware in your network infrastructure. If you use VPN, the management console must have access through your Internet firewall to the following servers: • **IBM Boulder VPN server** (IP address 207.25.252.196) • **IBM Rochester VPN server** (IP address 129.42.160.16) The first package is always sent from the management console. Only the following ports need to be open to the mentioned servers to use VPN: • Port 500 UDP • Port 4500 UDP [2] If you select **By Internet SSL**, you allow your management console to use a secure sockets layer (SSL) connection over the Internet when a connection is established to the IBM service center. You must open port 443:tcp in your network infrastructure for the following destination servers: Americas • 129.42.160.48 • 129.42.160.49 • 207.25.252.200 • 207.25.252.204 Non-Americas • 129.42.160.48 • 129.42.160.50 • 207.25.252.200 • 207.25.252.205 Problem Reporting Servers • 129.42.26.224 • 129.42.34.224 • 129.42.42.224 Configuration File Servers • 129.42.56.216 • 129.42.58.216 • 129.42.60.216 Your IBM service representative can also provide you with additional information. If VPN or SSL connectivity are not options, you can configure FTP to offload log and trace data faster. For information about the IBM VPN and SSL implementation including technical details, access the following website: www.ibm.com/support/docview.wss?uid=ssg1S1002693			

Table 70. Outbound (call home) work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
Modem settings Complete the following section if you are enabling call home using a modem. Even if your VPN or SSL is configured, a modem can serve as a backup. If the modem is configured, it allows IBM support personnel to remotely access the management console without having a person on-site to initiate a connection.			
Dialing mode used by modem	Check the box that indicates whether your local modem uses tone or pulse dialing.	[ ] **Tone** [ ] Pulse	[ ] **Tone** [ ] Pulse
Wait for dial tone?	If the management console modem waits for a dial tone before dialing a telephone number, check **Yes**. If the modem dials without checking for the dial tone, check **No**.	[ ] Yes [ ] No	[ ] Yes [ ] No
Dial-out prefix	If the modem must dial a prefix to access an outside line, check **Prefixes** and provide the prefix numbers. If no prefix is necessary, check **N/A**.	[ ] Prefixes: _________ [ ] N/A	[ ] Prefixes: _________ [ ] N/A
Internet (SSL) settings Complete the following section to select Internet (SSL) settings.			
Use SSL proxy?	If there is a SSL proxy server in between the HMC and the Internet, provide the address.	[ ] Yes _________ [ ] No	[ ] Yes _________ [ ] No
Authenticate with the SSL proxy?	If the SSL proxy requires a login, provide the user id, and password.	[ ] Yes _________ _________ [ ] No	[ ] Yes _________ _________ [ ] No
Dumps and traces Complete the following section to specify how you want to send trace or dump files to the IBM service center.			

Table 70. Outbound (call home) work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
Delivery method for dumps and traces	Check **Use the call home setup** if you want the management console to use the call home settings for dump and trace call-home transmissions. Check **Use FTP** if you want to send dumps and traces directly to the IBM FTP data repository server. FTP is recommended if VPN or SSL connectivity is not provided. If either VPN or SSL is configured, FTP is not needed. Data is offloaded faster if there is only a modem that is available for call home. (To use FTP, you must connect the management console to your LAN and provide a path to the Internet from the repository server.) If you check **Use the call home setup**, you have completed this work sheet.	[ ] **Use the call home setup** [ ] Use FTP	[ ] **Use the call home setup** [ ] Use FTP
Do you use an FTP firewall?	If you are using FTP to deliver dump and trace call-home transmissions, check **Yes** if your dump and trace files cross a firewall that filters FTP traffic. Check **No** if no FTP firewall filters the transmissions. If you check **Yes**, complete the remaining work sheet items. If you check **No**, you have completed this work sheet.	[ ] Yes [ ] No	[ ] Yes [ ] No
FTP firewall settings Table 71 on page 194 lists the types of FTP firewall that are supported by the management console. Review Table 71 on page 194 to determine the type of FTP to use if you plan to send dumps and traces to the IBM service center and if the dumps and traces pass through an FTP firewall.			

Types of FTP proxy servers

As an alternative to a VPN connection through the Internet, the management console can be set up to use the file transfer protocol (FTP) for sending error data to IBM. Table 71 lists the supported types of FTP proxy servers.

Table 71. Types of FTP proxy servers

Type	MC1	MC2 (if applicable)
1	Connect to the FTP proxy server and log in with USER `user real host name`.	Connect to the FTP proxy server and log in with USER `user real host name`.
2	Connect to the FTP proxy server and log in with the following settings: • USER `fwuser` • PASS `fwpassword` • USER `user real host name`	Connect to the FTP proxy server and log in with the following settings: • USER `fwuser` • PASS `fwpassword` • USER `user real host name`
3	Connect to and log in to the FTP proxy servers. Provide the following settings: SITE `real.host.name`, followed by the regular USER and PASS addresses.	Connect to and log in to the FTP proxy server. Provide the following settings: SITE `real.host.name`, followed by the regular USER and PASS addresses.
4	Connect to and log in to the FTP proxy server. Provide the following settings: OPEN `real.host.name`, followed by the regular USER and PASS addresses.	Connect to and log in to the FTP proxy server. Provide the following settings: OPEN `real.host.name`, followed by the regular USER and PASS addresses.
5	Connect to the FTP proxy server and log in with the following settings: • USER `user wuser@real.host.name` • PASS `pass fwpass`	Connect to the FTP proxy server and log in with the following settings: • USER `user wuser@real.host.name` • PASS `pass fwpass`
6	Connect to the FTP proxy server and log in with the following settings: • USER `fwuser real host name` • PASS `fwpass` • USER `user` • PASS `pass`	Connect to the FTP proxy server and log in with the following settings: • USER `fwuser real host name` • PASS `fwpass` • USER `user` • PASS `pass`
7	Connect to the FTP proxy server and log in with the following settings: • USER `user real host name fwuser` • PASS `pass` • ACCT `fwpass`	Connect to the FTP proxy server and log in with the following settings: • USER `user real host name fwuser` • PASS `pass` • ACCT `fwpass`

Inbound (remote services) work sheet

Use the inbound (remote services) work sheet to specify whether you want unattended inbound remote services through the modem, and the settings to use if you want unattended sessions.

If you choose not to select unattended service sessions during the initial configuration and you later want to have your storage unit serviced remotely, you must make specific scheduling arrangements with an IBM service representative. You then can either configure the management console to temporarily allow unattended remote services (specifying a start and stop date) or appoint an onsite person to manually enable the inbound call from the IBM service representative. This person must remain at the management console during the service session.

For unattended remote service, you must configure the management console for call home and you must select **connectivity mode** for the modem. For fast remote service, also select **By Internet VPN** for call home.

Without an inbound modem connection or for modem-less operation of the DS8000, you must either configure Assist-on-Site (AOS) or the HMC VPN in order for IBM to provide remote support.

Restriction: You cannot use **By Internet SSL** for fast inbound remote support.

Work sheet purpose

IBM service representatives use the information on the inbound remote services work sheet to customize your storage system to allow or prohibit authorized IBM service representatives the ability to dial into your management console and launch unattended sessions to further analyze and resolve serviceable events.

Work sheet and instructions

You must complete Table 72 if inbound connectivity via modem is required.. Contact your IBM service representative if you would like to install fast and secure remote access via IBM Assist-on-Site (AOS).

Notes:

1. Bold options in the MC1 and MC2 columns indicate default settings.
2. Management console is abbreviated as MC in the following table.

Table 72. Inbound (remote services) work sheet

Item or Setting	Instructions	MC1	MC2 (if applicable)
Allow unattended remote sessions?	Check **Yes** if you want to allow authorized IBM service representatives to initiate unattended remote service sessions on your storage unit. Check **No** if you do not want to allow unattended remote services. If you check **No**, you have completed this work sheet.	[ ] **Yes** [ ] No	[ ] **Yes** [ ] No
Unattended remote session settings Complete the following section if you selected **Yes** on whether to allow unattended remote sessions.			

Table 72. Inbound (remote services) work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
Remote service mode	Check the mode that indicates when to allow unattended sessions. Select **Continuous** to enable inbound remote service at any time. Select **Automatic** to allow inbound calls for a specified number of days following a failure on the storage complex.	[ ] **Continuous** [ ] Automatic [ ] Temporary	[ ] **Continuous** [ ] Automatic [ ] Temporary
Number of days for Automatic mode	If you selected the **Automatic** mode, specify the number of days to allow an unattended service session after any failure on the storage complex.		
Interval for Temporary Mode	If you selected the **Temporary** mode, specify the Starting and Ending date of the time period when unattended service sessions are allowed. **Note:** This option allows control of when IBM can perform unattended service. The interval is changed right before a service action takes place.		

Appendix G. Notification work sheets

These work sheets allow you to specify your preferred method of being notified about serviceable events.

Note: The IBM service representative sets up the notification process.

The notification work sheets allow you to specify the settings to use when you want the storage system to notify you or other people in our organization when you have serviceable events.

There are two notification work sheets:
- SNMP trap notification work sheet
- Email notification work sheet

SNMP trap notification work sheet

This work sheet allows you to specify the setting for SNMP trap notifications.

The SNMP trap notification work sheet allows you to indicate whether you want to receive Simple Network Management Protocol (SNMP) trap notifications when a management console encounters serviceable events. For more information about SNMP, visit the IBM System Storage DS8000 Information Center and select Configuring > SNMP traps.

Note: Remote copy status reporting for Copy Services requires SNMP for open-systems hosts.

Work sheet purpose

IBM service representatives use the information on the SNMP trap notification work sheet to customize your storage system for SNMP trap notifications.

Work sheet and instructions

You must complete Table 73 on page 198 for all installations that include a management console.

Notes:

1. Bolded options in the MC1 and MC2 columns indicate default settings.
2. Management console is abbreviated as MC for the following table.

Table 73. SNMP trap notification work sheet

Item or Setting	Instructions	MC1	MC2 (if applicable)
Enable SNMP trap notifications?	Check **Yes** to allow the storage unit to generate and send SNMP trap notifications when the system encounters problems. Check **No** if you do not want the storage unit to send SNMP trap notifications. If you check **No**, you have completed this work sheet.	_ Yes _ No	_ Yes _ No
SNMP trap notification settings: Complete the following section if you checked **Yes** to enable SNMP trap notifications. Do not use the IP address that is shown in the example in this work sheet. The IP address is only an example and does not function. Your IBM service representative can provide the correct IP address.			
SNMP trap destinations	Provide the dotted decimal addresses and community name of the destinations that are to receive SNMP traps (for example, 9.127.152.254 default).		
Note: If you plan to use advanced functions SNMP messaging, you must set those functions using DS CLI.			

Email notification work sheet

This work sheet allows you to specify the setting for email notifications.

The email notification work sheet allows you to specify whether you want to receive email notifications when a management console encounters serviceable events.

Restriction: To receive email notifications, the management console must be connected to your LAN.

Work sheet purpose

IBM service representatives use the information on this work sheet to customize your storage system for email notifications. If you choose to use email notifications, the notification settings are customized so that the specified people in your organization receive emails when there is general or error information to send about the storage complex.

Work sheet and instructions

You must complete Table 74 on page 199 for all installations that include a management console.

Notes:

1. Bold options in the MC1 and MC2 columns indicate default settings.
2. Management console is abbreviated as MC in the following table.

Table 74. Email notification work sheet

Item or Setting	Instructions	MC1	MC2 (if applicable)
Enable email notifications?	Check **Yes** to allow the MC to generate and send emails when the system encounters problems. Check **No** if you do not want the MC to send email notifications. If you check **No**, you have completed this work sheet.	_ Yes _ No	_ Yes _ No
Email notification settings Complete the following section if you previously checked **Yes** (to enable email notifications).			
Host name or network address of smart relay host (Optional)	To use a smart relay host, provide the host name or network address for the smart relay host. **Tip:** You can enable a smart relay host if either: • Your email is sent from a UNIX-based system on which you have specified a mail relay or mail gateway, or • You have installed a message-transfer agent on your mail server.		

Table 74. Email notification work sheet (continued)

Item or Setting	Instructions	MC1	MC2 (if applicable)
Email destinations	Provide the full email addresses where you want to receive the notifications (for example, **maria@host.com**). Check the notification setting that indicates the type of notifications to send to the email address. This work sheet provides spaces for three email addresses, but you can specify more, if necessary.	1. Email address: ___________ Notifications: _ Only call home problem events _ All problem events 2. Email address: ___________ Notifications: _ Only call home problem events _ All problem events 3. Email address: ___________ Notifications: _ Only call home problem events _ All problem events	1. Email address: ___________ Notifications: _ Only call home problem events _ All problem events 2. Email address: ___________ Notifications: _ Only call home problem events _ All problem events 3. Email address: ___________ Notifications: _ Only call home problem events _ All problem events

Appendix H. Power control work sheet

Use the power control work sheet to specify the power mode for your DS8000 storage unit.

You can choose to:

- Use attached System z or S/390 hosts to power on and power off the storage unit. (This option is available only if you have the remote zSeries power control feature installed.)
- Automatically power on and power off the storage unit.
- Use a specified schedule to power on and power off the storage unit.
- Manually power on and power off the storage unit. Use the Power on/off page in the DS Storage Manager.

Work sheet purpose

IBM service representatives use the information on the power control work sheet to customize the power mode for your storage unit.

Work sheet and instructions

You must complete Table 75 for all installations.

Note: Bold options in the "Your information" column indicate default settings.

Table 75. Power control work sheet

Item or Setting	**Instructions**	**Your information**
Enable remote zSeries power control?	If you plan to use the remote zSeries power control feature, check **Yes**. If you check **Yes**, choosing zSeries power mode enables up to four System z or S/390 hosts to control the power on and power off sequences. If you check **Yes**, you have completed this work sheet. Check **No** if you choose not to use the remote zSeries power control feature. If you check **No**, you must complete the rest of this work sheet.	_ Yes _ No
Disabled remote zSeries power control Complete the following section if you checked **No** on whether to use the remote zSeries power control).		

Table 75. Power control work sheet (continued)

Item or Setting	Instructions	Your information
Power mode	Check **Automatic** if you want the storage unit to power on automatically whenever external power is restored, if the unit was originally on. (The **Automatic** power mode automatically powers on the unit when, for example, power is restored after a power outage.) Check **Scheduled** if you want the storage unit to power on and off according to a specified scheduled. Check **Scheduled automatic** to schedule the power on and power off of your storage unit and enable the unit to automatically power on if power is restored while the unit is scheduled to be on. Check **Manual** if you want to manually power on and power off your unit. You can use the Power on/off page in the DS Storage Manager.	_ **Automatic** _ Scheduled (not automatic) _ Scheduled automatic _ Manual
Schedule	If you selected one of the scheduled power modes, **Scheduled** or **Scheduled automatic**, specify the power on and power off schedule.	
Schedule	Check whether you prefer the storage unit to have a power on and power off schedule that is the same every day or prefer a schedule that varies every day. Specify the on and off times for the unit in the appropriate section.	_ Same schedule all days: On ______________ Off ______________ _ Varying schedule: Monday: On ______________ Off ______________ Tuesday: On ______________ Off ______________ Wednesday: On ______________ Off ______________ Thursday: On ______________ Off ______________ Friday: On ______________ Off ______________ Saturday: On ______________ Off ______________ Sunday: On ______________ Off ______________

Appendix I. Control switch settings work sheet

Complete the control switch settings work sheet to indicate whether to enable or disable a particular switch setting. Your DS8000 model can include one or more storage images; consequently, you many need to indicate your individual choice for each.

The switch settings described in this section can be enabled or disabled by indicating your choices on the work sheet that follows the setting descriptions. IBM service personnel use the choices you specify on the work sheet to set the control switches for your unit.

IBM i LUN serial suffix number

Use the IBM i LUN serial suffix number switch setting only when you attach more than one DS8000 series model to an AS/400 or IBM i host and the last three digits of the worldwide node name (WWNN) are the same on any of the DS8000 units.

For example, the WWNN for the first DS8000 is 500507630BFFF958 and the WWNN for an additional DS8000 is 500507630AFFF958. Both DS8000 units would present the same LUN serial number for the same LUN ID. Because the original LUN serial number is used for identification, the AS/400 does not use the LUN from the additional DS8000. Specifying a unique serial number base for the additional DS8000 unit prevents this problem. IBM service personnel enter the control-switch setting for the new serial number base, which you specify for this field.

The WWNN can be found on the WWID label on the inside front left wall of rack one, located near the LED indicators of the upper-primary power supply. For example, WWID: 500507630AFFF99F.

Notes:

- The probability of receiving two DS8000 series models with the same last three WWNN digits is unlikely, but possible.
- After updating the switch settings, a quiesce and resume of the storage facility image is required for the changes to take effect.

The IBM i LUN serial suffix number applies to IBM i and AS/400 environments only.

Control-unit Initiated reconfiguration settings

The control-unit initiated reconfiguration (CUIR) setting indicates whether to enable or disable subsystems. CUIR prevents loss of access to volumes in System z environments due to incorrect path handling. This function automates channel path management in System z environments, in support of selected DS8000 service actions. CUIR relies on a combination of host software and DS8000 firmware. The host systems are affected during host adapter repair or I/O enclosure repair. The CUIR setting on the work sheet enables you to indicate whether this option can be enabled. The CUIR setting applies to IBM System z and S/390 environments only.

Present SIM data to all hosts

Service Information Messages (SIMs) are offloaded to the first I/O request. The SIMs are directed to each logical subsystem in the storage facility if the request is device or control unit related. The SIMs are offloaded to the individual logical volume when the request is media related. This control switch determines whether SIMs are sent to all, or to only the first, attached IBM System z LPAR making an I/O request to the logical system or logical volume. This setting applies to IBM System z and S/390 environments only.

Control unit threshold

This control unit threshold switch provides the threshold level for presenting a SIM to the operator console for controller related errors. SIMs are always sent to the attached IBM System z hosts for logging to the Error Recording Data Set (ERDS). SIMs can be selectively reported to the IBM System z host operator console, as determined by SIM type and SIM severity. This setting applies to IBM System z and S/390 environments only.

Table 76. SIM presentation to operator console by severity

Selection	Severity of SIM presented to operator console
Service	Service, Moderate, Serious, and Acute (all)
Moderate	Moderate, Serious and Acute
Serious	Serious and Acute
Acute	Acute
None	None

Table 77. SIM severity definitions

Severity	Definition
Service	No system or application performance degradation is expected in any environment.
Moderate	Performance degradation is possible in a heavily loaded environment.
Serious	A primary subsystem resource is disabled.
Acute	A major subsystem resource is disabled. Performance may be severely degraded. System or application outages may have occurred.

Device threshold

This control switch provides the threshold level for presenting a SIM to the operator console for device related errors. Device threshold levels are the same type and severity as control unit threshold settings. Device threshold applies to IBM System z and S/390 environments only.

Media threshold

This control switch provides the threshold level for presenting a SIM to the operator console for media related errors. Media threshold levels are the same type and severity as control unit threshold settings. Media threshold applies to IBM System z and S/390 environments only.

Use Table 78 to enter the appropriate response into the information column.

Table 78. Control switch settings work sheet

Control Switch Setting	**Default**	**Your information**
IBM i LUN Serial Suffix number - AS/400 LUN Serial Suffix number	0 (Off)	_____ Enter the last three digits of the DS8000 worldwide node name (WWNN).[1] [ ] 0 = Off (use last three digits of WWNN) [ ] _____ (enter three numeric digits to create a unique identifier)
CUIR support	0 (Disable)	[ ] true = Enable CUIR support [ ] false = Disable CUIR support
Control unit threshold	2	Present SIM to operator console for the following severities: [ ] 0 = Service, Moderate, Serious, and Acute (all) [ ] 1 = Moderate, Serious and Acute [ ] 2 = Serious and Acute [ ] 3 = Acute
Device threshold	2	Present SIM to operator console for the following severities: [ ] 0 = Service, Moderate, Serious, and Acute (all) [ ] 1 = Moderate, Serious and Acute [ ] 2 = Serious and Acute [ ] 3 = Acute
Media threshold	2	Present SIM to operator console for the following severities: [ ] 0 = Service, Moderate, Serious, and Acute (all) [ ] 1 = Moderate, Serious and Acute [ ] 2 = Serious and Acute [ ] 3 = Acute
Present SIM data to all hosts	0 (Disable)	[ ] true = Enable (all hosts) [ ] false = Disable (host issuing start I/O)

Notes:

1. The WWNN can only be determined by reading the WWNN label on the front left inside wall of Rack-1 after it is unpacked. Only then can you determine if there is a duplication of the last three digits with an existing storage facility. If you cannot wait for that to occur, enter three numeric digits to create a unique identifier.

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

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

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

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

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

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

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

Trademarks

Electronic emission notices

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

Federal Communications Commission statement

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

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

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

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

Industry Canada compliance statement

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

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

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
e-mail: 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:

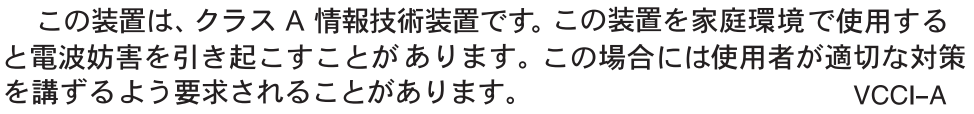
IBM Deutschland GmbH
Technical Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Generelle Informationen:

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

Japanese Voluntary Control Council for Interference (VCCI) class A statement



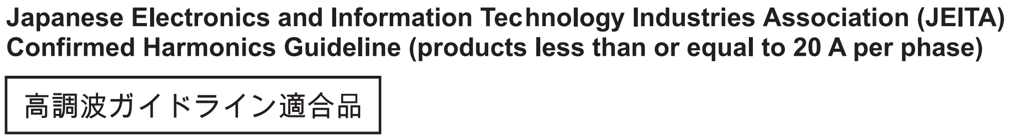
この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI−A

Translation:

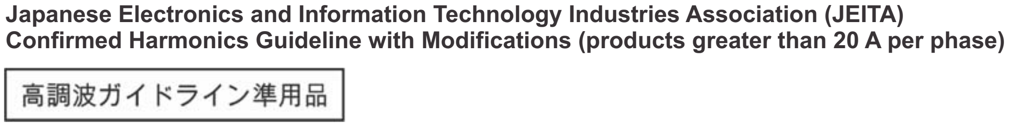
This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japanese Electronics and Information Technology Industries Association (JEITA) statement



Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)

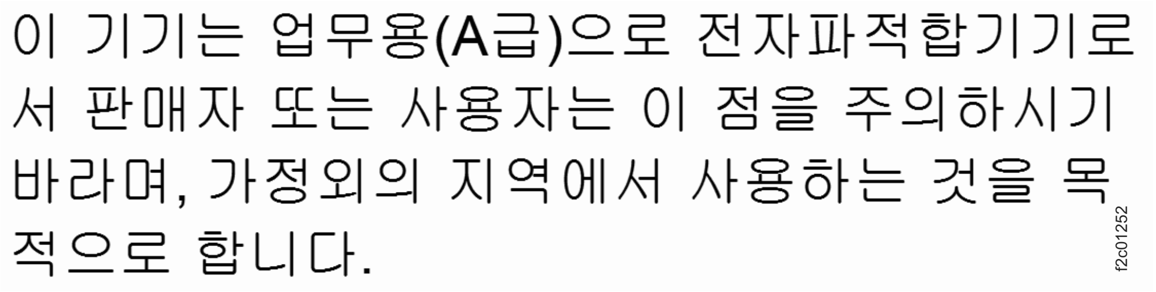
高調波ガイドライン適合品



Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)

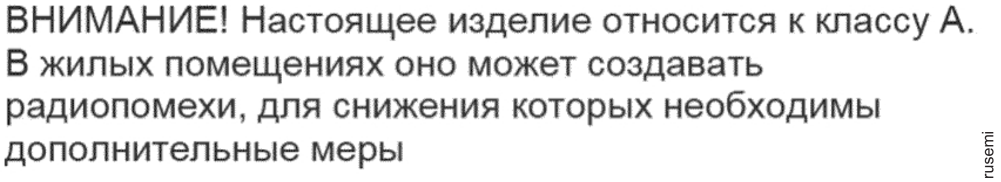
高調波ガイドライン準用品

Korea Communications Commission (KCC) Electromagnetic Interference (EMI) Statement

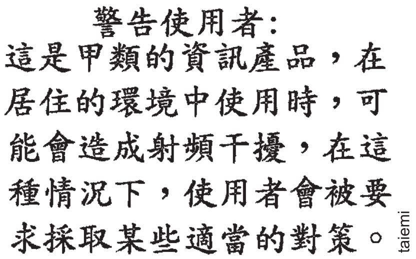


이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Russia Electromagnetic Interference (EMI) Class A Statement


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

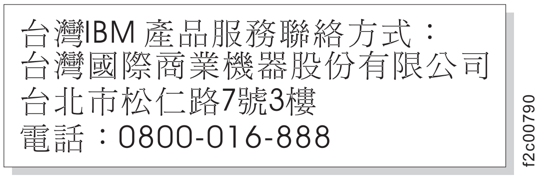
Taiwan Class A compliance statement


警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

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

Index

Printed in USA