ESCALA Power7

Installing and configuring the SDMC

ESCALA Power7

Installing and configuring the SDMC

The ESCALA Power7 publications concern the following models:

 - Bull Escala E5-700 (Power 750 / 8233-E8B)
 - Bull Escala M6-700 (Power 770 / 9117-MMB)
 - Bull Escala M6-705 (Power 770 / 9117-MMC)
 - Bull Escala M7-700 (Power 780 / 9179-MHB)
 - Bull Escala M7-705 (Power 780 / 9179-MHC)
 - Bull Escala E1-700 (Power 710 / 8231-E2B)
 - Bull Escala E1-705 (Power 710 / 8231-E1C)
 - Bull Escala E2-700 / E2-700T (Power 720 / 8202-E4B)
 - Bull Escala E2-705 / E2-705T (Power 720 / 8202-E4C)
 - Bull Escala E3-700 (Power 730 / 8231-E2B)
 - Bull Escala E3-705 (Power 730 / 8231-E2C)
 - Bull Escala E4-700 / E4-700T (Power 740 / 8205-E6B)
 - Bull Escala E4-705 (Power 740 / 8205-E6C)

References to Power 755 / 8236-E8C models are irrelevant.

Hardware

October 2011

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this book.

Contents

Configuring high availability 65

Notices 67

Safety notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the U.S. English publications.

German safety information

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Laser safety information

IBM® servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

IBM servers may be installed inside or outside of an IT equipment rack.

DANGER

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

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

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

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

  (D005)

DANGER

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

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

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

CAUTION

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

(R001)

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

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

(R002)

(L001)

(L002)
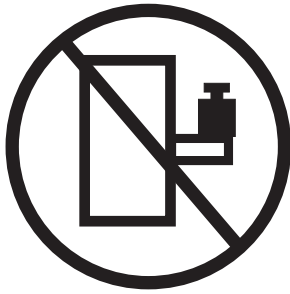
(L003)
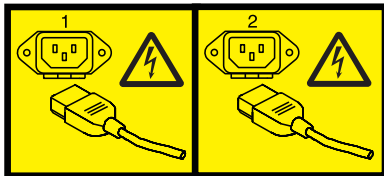
or

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:
- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

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

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

CAUTION:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do Not:
- ___ Throw or immerse into water
- ___ Heat to more than 100°C (212°F)
- ___ Repair or disassemble

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. (C003)

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:
- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

SDMC concepts

The IBM Systems Director Management Console (SDMC) is the next generation Hardware Management Console (HMC) that combines the functions of the HMC, the simplicity of the Integrated Virtualization Manager (IVM), and the value-add functions of the IBM Systems Director. The SDMC provides server management and PowerVM™ virtualization management.

The SDMC is a management console for managing IBM Power Systems™ servers and IBM BladeCenter® Power blade servers. The SDMC is an alternative and replacement for the current HMC with enhanced virtualization and hardware management capabilities. The SDMC is an x86-based console. The SDMC manages IBM AIX®, IBM i, or Linux operating systems on IBM Power Systems servers and IBM BladeCenter Power blade servers.

Comparing HMC and SDMC features

You need to understand the differences between the Hardware Management Console (HMC), Integrated Virtualization Manager (IVM), and IBM Systems Director Management Console (SDMC) environments including terminology, users and roles, supported features, high availability options, and command-line differences.

Comparing the HMC and SDMC

There are some important differences between the HMC and the SDMC.

With the SDMC, the scope of administered systems spans from POWER blade servers to high-end systems, providing a single, consistent approach to systems administration.

The characteristics of both the HMC and the SDMC, at a high level, follow:

HMC
- Is implemented as an external, independent appliance
- Can administer entry-level systems to high-end systems
- Can administer more than one managed system
- Allows for more than one VIOS per managed system

SDMC
- SDMC is offered as an appliance in two forms:
  - A hardware appliance similar to the HMC, using essentially the same hardware plus additional memory and disk.
  - A virtual appliance that runs in a VMware partition
- Can administer entry-level systems to high-end systems
- Can administer more than one managed system
- Allows for more than one VIOS per managed system
- Supports entry-level systems to high-end systems plus blades.

How the SDMC is used

SDMC represents the next generation of management appliances for POWER processor-based systems. The SDMC replaces both the HMC and IVM in POWER processor-based systems administration. Thus, the SDMC can manage POWER systems directly but can also work with the HMC and IVM side by side to ease transition.

SDMC is integrated into the administrative framework of IBM Systems Director. It provides a common interface for systems administration across the data center. If you have used an HMC or IVM, you will already be familiar with SDMC tasks and procedures. The Systems Director provides additional tasks that you might want to explore. Note that these additional Systems Director tasks and navigation options might make it more difficult to find familiar HMC tasks. For more information about navigating the SDMC GUI, see "Navigation differences between the HMC GUI and the SDMC GUI" on page 5.

The SDMC can unify platform management for IBM Systems, providing a consistent interface for common management tasks. By integrating POWER processor-based systems management into the IBM Systems Director framework, you can easily manage many systems of different types. The SDMC also enables the integration of POWER processor-based systems into data center management tools.

As a successor to both the HMC and IVM, the SDMC administrators can work with a high-level view of systems. It organizes tasks in a single window, instead of using different menus. This interface simplifies views on systems and provides faster access to day-to-day tasks.

As it was with older POWER processor-based systems, the transition to the SDMC requires that management for POWER5 and POWER5+ processor based systems continue with either the HMC or IVM. The SDMC can administer the HMC and IVM as well; however, this management console eases transition from older environments into new ones.

Virtualization enhancements

SDMC has made managing your virtualization environment significantly easier, while maintaining all of the HMC's existing functions.

The enhancements follow:

Virtual I/O management
  In addition to the HMC's Virtual Storage Management view, The SDMC brings similar simplification to the Create Virtual Server and Manage Virtual Server views. With SDMC, you can see the storage devices attached to a virtual server and need not be concerned about your virtual SCSI device pairs and the VIOS command-line.

Simplified Create Virtual Server wizard
  Create Virtual Server (known as logical partition on the HMC) wizard asks only what is needed to create the virtual server, and selects reasonable defaults for all other settings. Advanced users who want full control can change the profile after the wizard is completed to control all of their settings, such as min/max values. You can now create a virtual server by simply specifying the name and clicking **Finish**.

Managing virtual server
  A task called **Manage Virtual Server** displays virtual server properties and I/O device configuration information in one window. With this task, you control the resource assignments for a virtual server directly (whether the virtual server is powered on or off) without using a profile.

Terminology differences between HMC and SDMC

The HMC and SDMC environments use different terminology.

For integration into IBM Systems Director, SDMC introduces some synonyms that replace familiar HMC terms. The key ones to remember are the following:
- *Virtual Server* (formerly *Partition*)
- *Host* (formerly *Managed System* or *Server*)
- *Power Unit* (formerly *Frame*)

For detailed information about the terminology differences between the HMC and the SDMC, see the following tables.

Table 1. Networking terms

HMC	SDMC	Description
Open network	Standard network	The standard network can be connected to a firewall or router for connecting to the Internet.

Table 2. Objects

HMC	SDMC	Description
Hardware Management Console (HMC), Integrated Virtualization Manager (IVM)	Platform manager	A platform manager manages one or more hosts and their associated virtual servers and operating systems. For Power Systems servers, the platform managers are HMC and IVM.
Frame, bulk power assembly (BPA)	Power unit	The power assembly for processor, memory, FSP, and I/O enclosures.
Server, managed system, system, flexible service processor (FSP), central electronics complex (CEC)	Host	A physical server that contains physical processors, memory, and I/O resources. The physical server is often virtualized into virtual servers, also known as logical partitions.
Logical partition (LPAR), dynamic LPAR (DLPAR), partition	Virtual server	The collection of processor, memory and I/O resources defined to run an operating system and its applications.
Virtual I/O Server (VIOS)	Utility virtual server	A virtual server that provides virtualization capabilities for a particular environment.

Table 3. Tasks

HMC	SDMC	Description
Remove connection – systems	Remove host	The remove tasks removes the host from the directory database.

Table 4. Users and roles

HMC	SDMC	Description
hscroot	sysadmin	Predefined administrator user for the platform manager.
hscpe	pe	Predefined service and support user for the platform manager.
hmcsuperadmin	SMAdministrator (Administrator role)	The Administrator role has full authority to all resources and tasks, including security administration, product installation, and configuration.

Table 4. Users and roles (continued)

HMC	SDMC	Description
hmcoperator	SMManager (Manager role)	The Manager role can perform a subset of the tasks that an administrator can perform. Typically, system administration, system health management, and configuration tasks are available.
N/A	SMUser (User role)	The User role includes any authenticated user and allows only basic operations such as viewing resources and properties.
hmcviewer	SmMonitor (Monitor role)	The Monitor role can access those administrative functions that provide read-only access. Primarily, monitoring, notifications, and status tasks are available.
hmcservicerep	SMServiceRep (PE role)	The PE role includes the pe user and gives users the ability to perform only service operations, such as viewing resources, logs, and system status and health.

Table 5. Hosts and system states.
Note: SDMC states include operating states, detailed states, and health states.

HMC states	SDMC operating states	SDMC detailed states	SDMC health states
Operating	Started	N/A	OK
Standby	Standby	N/A	OK
Power off	Stopped	N/A	OK
Service processor failover	Started	Service processor failover	Degraded/warning
Power off in progress	Stopping	N/A	OK
Initializing	Starting	N/A	OK
No connection * (should be handled by Access Point state)	Not available	Unknown	Unknown
Pending authentication	Waiting for input	Password updates required	Degraded/warning
Failed Authentication * (Should be handled by Access Point state, that is, Failed Access)	Not available	Unknown	Unknown
Error	Error	Unknown	Critical failure
Error - terminated	Error	Terminated	Critical failure
Error - dump in progress	Error	Dump in progress	Critical failure
Recovery	Error	Recovery	Critical failure
Incomplete	Error	Incomplete	Critical failure
Version mismatch	Error	Version mismatch	Major failure

Table 6. Virtual server and partition states

HMC states	SDMC operating states	SDMC detailed states	SDMC health states
Running	Started	N/A	OK
Starting	Starting	N/A	
Not activated	Stopped	N/A	Unknown
Migrating - not activated	Relocating	N/A	OK
Migrating - running	Relocating	N/A	OK
Shutting down	Stopping	N/A	OK
Open firmware	Waiting for input	Open firmware	OK
Hardware discovery	Started	Performing hardware discovery	OK
Error	Error	Unknown	Major failure
Not available	Not available	Unknown	Unknown

Table 7. Power unit states

HMC state	SDMC Operating State	SDMC Detailed State	SDMC Health State
Standby	Standby	N/A	Degraded
Standby/starting	Standby	N/A	OK
Starting	Starting	N/A	
Pending frame number change	Standby	N/A	Degraded
Failed authentication	Not Available	Unknown	Unknown
Pending authentication	Waiting for input	Password updates required	Degraded / Warning
No connection	Not available	Unknown	Unknown
Incomplete	Error	Incomplete	Critical failure
Version mismatch	Error	Version mismatch	Major failure

Navigation differences between the HMC GUI and the SDMC GUI

This section describes the differences in navigating to commonly used Hardware Management Console (HMC) tasks on the HMC and on the Systems Director Management Console (SDMC).

Because IBM Systems Director manages many different types of objects, it has a generic navigation style. Systems Director groups managed objects and shows general properties for each object. The SDMC interface is quite similar to the HMC interface.

Below is a list of commonly-used HMC tasks, and where they can now be found in the SDMC interface:

Viewing host (server) properties by using the SDMC interface

The Properties task in SDMC is different from that of the HMC. The SDMC now calls a server a *host*.

To view server properties by using the HMC, complete the following steps:
1. In the navigation pane, select**Systems Management**.
2. Select the server.
3. In the contents pane, select **Tasks** > **Properties**.

To view host properties by using the SDMC, complete the following steps

1. From the Resources page, right-click the host.
2. Select **System Configuration** > **Edit Host**.

Viewing virtual server (partition) properties by using the SDMC interface

To view partition properties by using the HMC, complete the following steps:

1. In the navigation pane, select**Systems Management**.
2. In the contents pane, expand the server.
3. Select the logical partition.
4. Click **Tasks** > **Properties**.

The SDMC now calls a partition a *virtual server*.

To view virtual server properties using the SDMC, complete the following steps:

1. From the Resources page, select the virtual server.
2. Click **System Configuration** > **Manage Virtual Server**.

Discovering a system to manage using the SDMC interface

Discovery is a general Systems Director concept of finding a system or object to manage. You can use the SDMC interface to discover and manage the following objects:

- Host flexible service processors (FSPs) and host power units
- Bulk power controllers (BPCs) and frames
- Operating systems

If you are using the SDMC as a Dynamic Host Configuration Protocol (DHCP) server for your managed systems, the FSPs and BPCs are discovered automatically. If you are not using the SDMC as a DHCP server, you can discover the resource by entering a host name, an IP address, or a range of IP addresses in the **Discover** section of the GUI or the command-line interface (CLI).

To discover a system to manage by using the HMC, complete the following steps:

1. In the navigation pane, select**Systems Management**.
2. Select the server.

To discover a host to manage by using the SDMC, complete the following steps:

1. On the Resources page, click**Common Tasks** > **System Discovery**.
2. Select a discovery option, IP address, and the resource type to discover.
3. Click **Discover now**.

Powering a server (host) on or off by using the SDMC interface

To power a server on or off by using the HMC, complete the following steps:

1. In the navigation pane, select**Systems Management**.
2. Select the server.
3. In the contents pane, select **Tasks** > **Operations** > **Power On** or **Tasks** > **Operations** > **Power Off**.

The SDMC now calls a server a *host*.

To power a host on or off by using the SDMC, complete the following steps:

1. From the Resources page, right-click the host.

2. Select **Operations** > **Power on** or **Operations** > **Power off**.

Creating a logical partition (virtual server) by using the SDMC interface

To create a logical partition by using the HMC, complete the following steps:

1. In the navigation pane, select**Systems Management**.
2. Select the server on which you want to create a logical partition.
3. In the contents pane, select **Tasks** > **Configuration** > **Create logical partition**.

The SDMC calls a partition a *virtual server*. To create a virtual server by using the SDMC, compete the following steps:

1. From the Resources page, right-click the host.
2. Select **Create Virtual Server**.

Comparing HMC tasks and SDMC tasks

This section provides detailed task information for moving from Hardware Management Console (HMC) to Systems Director Management Console (SDMC) for each HMC task.

Server (host) tasks

This topic provides server task information for moving from HMC to SDMC. Servers are known as *hosts* on the SDMC.

The following task mapping information is available in this topic:

- Server (host) properties task mapping
- Server (host) operations task mapping
- Server (host configuration task mapping
- Server (host) connections task mapping
- Server (host) hardware information task mapping
- Server (host) updates task mapping
- Server (host) serviceability task mapping
- Server (host) Capacity on Demand task mapping

Table 8. Server (host) properties task mapping

HMC task	SDMC task	Is the task identical?	Notes
View Properties	System Configuration > Edit Host	Yes	The properties task on SDMC is different from that on the HMC. For more information about performing this task, see Changing host properties.

Table 9. Server (host) operations task mapping

HMC task	SDMC task	Is the task identical?	Notes
Power On and Power Off	Operations > Power On / Power Off	No	The function is the same, but the interface is different. For more information about performing this task, see Powering on the host.

Table 9. Server (host) operations task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Power Management	Operations > Power Management	No	The function is the same, but the interface is different. For more information about performing this task, see Performing POWER management operations.
LED Status > Deactivate Attention LED	Service and Support > Hardware > System Attention LED	Yes	For more information about performing this task, see Activating and deactivating the Attention LED.
LED Status > Identify LED	Service and Support > Hardware > Identify LED	Yes	For more information about performing this task, see Locating parts with the Identify LED.
LED Status > Test LED	Service and Support > Hardware > LED Lamp Test	Yes	For more information about performing this task, see Performing an LED lamp test.
Schedule Operations	Operations > Schedule Operations	No	The function is the same, but the interface is different. For more information about performing this task, see Scheduling host operations.
Launch Advanced System Management (ASM)	Operations > Launch Advanced System Management (ASM)	No	The function is the same, but the interface is different. For more information about performing this task, see Launching Advanced System Management.
Utilization Data > Change Sampling Rate	Operations > Utilization Data > Change Sampling Rate	Yes	For more information about performing this task, see Changing the sampling rate for utilization data.
Utilization Data > View	Operations > Utilization Data > View Utilization Data	Yes	For more information about performing this task, see Viewing host utilization data.
Rebuild	Operations > Rebuild Managed System	No	The function is the same, but the interface is different. For more information about performing this task, see Rebuilding a managed system.

Table 9. Server (host) operations task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Change Password	Operations > Change Password	No	The function is the same, but the interface is different. For more information about performing this task, see Changing host passwords

Table 10. Server (host) configuration task mapping

HMC task	SDMC task	Is the task identical?	Notes
Create Logical Partition	System Configuration > Create Virtual Server	No	The HMC has 3 separate tasks. The SDMC combines these tasks into one task. For more information about performing this task, see Creating virtual servers.
System Plans > Create/Deploy	System Configuration > Manage System Plans	Mostly	The SDMC task places all system plan function under the Manage System Plans task. For more information about performing this task, see Creating a system plan by using the SDMC.
View Workload Management Groups	System Configuration > View Workload Management Groups	Yes	
Manage Profile Data > Restore/Initialize/Backup/Delete	System Configuration > Manage Virtual Server Data > Restore/Initialize/ Backup/Delete	Yes	For more information about performing this task, see Managing profiles for virtual servers.
Manage System Profiles	System Configuration > Manage System Profiles	Yes	For more information about performing this task, see Managing system profiles.
Virtual Resources > Virtual Storage Management	System Configuration > Virtual Resources > Virtual Storage Management		
Virtual Resources > Virtual Network Management	System Configuration > Virtual Resources > Virtual Network Management	Yes	

Table 11. Server (host) connections task mapping

HMC task	SDMC task	Is the task identical?	Notes
Service Processor Status	System Configuration > Edit Host	Yes	

Table 11. Server (host) connections task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Reset or Remove Connection	Security > Revoke Access, Security > Request Access, Remove		Revoke access removes the connection. Request access reestablishes it. The remove operation is the equivalent to Remove Connection. For more information about performing this task, see Revoking connection access.
Disconnect Another Management Console	Service and Support > Reset Other Management Console Connection		
• Add Managed System • Update Password	• Common Tasks > System Discovery • Security > Request Access		Adding a system is a two-step process on SDMC. First, discover the system, and then request access. On the HMC it can be done in one step. For more information about performing this task, see Adding hosts to the SDMC.

Table 12. Server (host) hardware information task mapping

HMC task	SDMC task	Is the task identical?	Notes
Adapters > Host Ethernet	Hardware Information > Adapter > Host Ethernet	Yes	
Adapters > Host Channel	Hardware Information > Adapter > Host Channel	Yes	
View Hardware Topology	Hardware Information > View Hardware Topology	Yes	

Table 13. Server (host) updates task mapping

HMC task	SDMC task	Is the task identical?	Notes
Change Licensed Internal Code	Release Management > See notes	No	The HMC uses a wizard for updates, whereas the SDMC has separate steps for updates. Update tasks are under the Release Management menu. For more information about performing this task, see Updating the host.
Upgrade Licensed Internal Code	Release Management > See notes	No	Upgrade, change, and update operations have the same user flow on SDMC. For more information about performing this task, see Updating the host.

Table 13. Server (host) updates task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Check System Readiness	Release Management > Readiness Check	No	
View System Information	Release Management > Power Firmware Management	No	In SDMC, power-specific update tasks are under the **Power Firmware Management** task. For more information about performing this task, see Managing Power system firmware.

Table 14. Server (host) serviceability task mapping

HMC task	SDMC task	Is the task identical?	Notes
Manage Serviceable Events	Properties > Active Status > Category: Service Status	No	For more information about performing this task, see Managing serviceable problems by using Service and Support Manager.
Create Serviceable Event	Service and Support > Submit Service Request	No	For more information about performing this task, see Submitting service request using Service and Support Manager.
Reference Code History	Service and Support > Reference Code History	Yes	For more information about performing this task, see Reference Code History.
Control Panel Functions > (20) Type, Model, Feature	Service and Support > Control Panel Functions > (20) Type, Model, Feature	Yes	For more information about performing this task, see Control Panel Functions.
Hardware > Prepare For Hot Repair/Upgrade	Service and Support > Hardware > Prepare For Hot Repair/Upgrade	Yes	For more information about performing this task, see Preparing for Hot Repair or Upgrade.
Hardware > Exchange FRU	Service and Support > Hardware > Exchange FRU	Yes	For more information about performing this task, see Exchange FRU.
Hardware > Power On/Off Unit	Service and Support > Hardware > Power On/Off Unit	Yes	For more information about performing this task, see Power On/Off Unit.
Hardware > MES Tasks	Service and Support > Hardware > MES Tasks	Yes	For more information about performing this task, see MES tasks.
Manage Dumps	Service and Support > Support Files	No	For more information about performing this task, see Managing support files by using Service and Support Manager.

Table 14. Server (host) serviceability task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Manage Dumps > System Dump Parameters	Service and Support > Dump Settings	No	For more information about performing this task, see Managing support files by using Service and Support Manager.
Collect VPD	Inventory > View and Collect Inventory	No	
FSP Failover > Setup/Initiate	Service and Support > FSP Failover > Failover Initiate/Failover Setup	Yes	For more information about performing this task, see FSP Failover.

Table 15. Server (host) Capacity on Demand task mapping

HMC task	SDMC task	Is the task identical?	Notes
All Tasks	System Configuration > Capacity on Demand (CoD)	No	SDMC has combined all CoD functions into one Manage task. For more information about performing this task, see Capacity on Demand for SDMC.

Partition (virtual server) tasks

This topic provides partition task information for moving from HMC to SDMC. Partitions are known as *virtual servers* on the SDMC..

The following task mapping information is available in this topic:

- Partition (virtual server) task mapping
- Partition (virtual server) operations task mapping
- Partition (virtual server) configuration task mapping
- Partition (virtual server) hardware configuration task mapping
- Partition (virtual server) Dynamic Logical Partitioning (DLPAR) task mapping
- Partition (virtual server) console window task mapping
- Partition (virtual server) serviceability task mapping

Table 16. Partition (virtual server) task mapping

HMC task	SDMC task	Is the task identical?	Notes
Properties	System Configuration > Manage Virtual Server	No	SDMC has combined Properties and dynamic logical partitioning (DLPAR) tasks into the Manage Virtual Server task. For more information about performing this task, see Manage virtual server operations.
Change Default Profile	N/A		SDMC has removed this task.

Table 17. Partition (virtual server) operations task mapping

HMC task	SDMC task	Is the task identical?	Notes
Activate > Profile	Operations > Activate > Profile	Yes	For more information about performing this task, see Activating a virtual server based on its current configuration.
Activate > Current Configuration	Operations > Activate > Current Configuration	Yes	For more information about performing this task, see Activating a virtual server.
Restart	Operations > Restart	Yes	For more information about performing this task, see Shutting down and restarting virtual servers.
Shutdown	Operations > Shutdown	Yes	For more information about performing this task, see Shutting down and restarting virtual servers.
Deactivate Attention LED	Service and Support > Hardware > System Attention LED	Yes	
Schedule Operations	Operations > Schedule Operations	No	This task in SDMC is done on the server (host), not the partition (virtual server)
Delete	Operations > Delete	Yes	For more information about performing this task, see Deleting a virtual server profile.
Mobility > Migrate	Operations > Mobility > Migrate	Yes	For more information about performing this task, see Moving the virtual server with SDMC.
Mobility > Validate	Operations > Mobility > Validate	Yes	For more information about performing this task, see Validating the configuration for virtual server mobility.
Mobility > Recover	Operations > Mobility > Recover	Yes	
Suspend Operations > Recover	Operations > Suspend Operations > Recover	Yes	For more information about performing this task, see Recovering a suspended virtual server.
Suspend Operations > Suspend	Operations > Suspend Operations > Suspend	Yes	For more information about performing this task, see Suspending a virtual server.

Table 18. Partition (virtual server) configuration task mapping

HMC task	SDMC task	Is the task identical?	Notes
Manage Profiles	System Configuration > Manage Profiles	Yes	The Create Profile wizard has been removed and is replaced with the Copy Profile which launches into the edit profile function for changing the profile. For more information about performing this task, see Managing profiles for virtual servers.
Manage Custom Groups	Add To > Existing Group / Create Group System	No	For more information about performing this task, see Managing users.
Save Current Configuration	Configuration > Save Current Configuration	Yes	For more information about performing this task, see Saving the current configuration of a virtual server.

Table 19. Partition (virtual server) hardware configuration task mapping

HMC task	SDMC task	Is the task identical?	Notes
All Tasks	System Configuration > Manage Virtual Server	No	For SDMC, I/O adapter management is done under the **Manage Virtual Server** task. For more information about performing this task, see Manage virtual server operations.

Table 20. Partition (virtual server) dynamic logical partitioning (DLPAR) task mapping

HMC task	SDMC task	Is the task identical?	Notes
All Tasks	System Configuration > Manage Virtual Server	No	For SDMC, DLPAR tasks are done under the **Manage Virtual Server** task. Note that DLPAR Move tasks from the GUI are a two-step process (remove and add). For more information about performing this task, see Managing virtual servers.

Table 21. Partition (virtual server) console window task mapping

HMC task	SDMC task	Is the task identical?	Notes
Open Terminal Window	Operations > Console Window > Open Terminal Console	No	The TTY terminal applet requires you to authenticate to SDMC.

Table 21. Partition (virtual server) console window task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Close Terminal Connection	Operations > Console Window > Close Terminal Console	No	
Open Dedicated 5250 Console (Local Only)	Operations > Console Window > Open Dedicated 5250 Console (Local Only)	Yes	Launches x-Windows IBM 5250 emulator to the virtual server in dedicated mode.
Open Shared 5250 Console (Local Only)	Operations > Console Window > Open Shared 5250 Console (Local Only)	Yes	Launches x-Windows IBM 5250 emulator to the virtual server in shared mode.

Table 22. Partition (virtual server) serviceability task mapping

HMC task	SDMC task	Is the task identical?	Notes
Manage Serviceable Events	Properties > Active Status > Category: Service Status	No	For more information about performing this task, see Managing serviceable problems by using Service and Support Manager.
Reference Code History	Service and Support > Reference Code History	Yes	For more information about performing this task, see Reference Code History.
Control Panel Functions	Service and Support > Control Panel Functions	No	For SDMC, all functions are available in one task. For more information about performing this task, see Control Panel Functions.

Frame (power unit) tasks

This topic provides frame task information for moving from HMC to SDMC. Frames are known as *power units* on the SDMC.

The following task mapping information is available in this topic:
- Frame properties task mapping
- Frame connections task mapping
- Frame serviceability task mapping
- Frame operations task mapping

Table 23. Frame properties task mapping

HMC Task	SDMC Task	Is the task identical?	Notes
Frame Properties	Edit Power Unit	No	For more information about performing this task, see Changing power unit properties.

Table 24. Frame connections task mapping

HMC Task	SDMC Task	Is the task identical?	Notes
Bulk Power Assembly (BPA)	Connections > Bulk Power Assembly (BPA) Status	No	For more information about performing this task, see Viewing the bulk power assembly status.
Status Reset	Security > Revoke Access, Security > Request Access, Revoke	No	Revoke access removes the connection. Request access re-establishes it. For more information about performing this task, see Requesting connection access and Revoking connection access.

Table 25. Frame serviceability task mapping

HMC Task	SDMC Task	Is the task identical?	Notes
Manage Serviceable Events	Properties > Active Status > Category:	No	For more information about performing this task, see Managing serviceable problems by using Service and Support Manager.
Hardware > Exchange FRU	Service Status Service and Support > Hardware > Exchange FRU	Yes	For more information about performing this task, see Replace FRU.
Hardware > MES Tasks	Service and Support > Hardware > MES Tasks	Yes	For more information about performing this task, see Performing MES tasks.

Table 26. Frame operations task mapping

HMC Task	SDMC Task	Is the task identical?	Notes
Initialize	Operations > Initialize Power Unit	No	For more information about performing this task, see Initializing the power unit.
Launch Advanced System Management (ASM)	Operations > Launch Advanced System Management (ASM)	No	For more information about performing this task, see Launching Advanced System Manager.
Change Password	Operations > Change Password	No	For more information about performing this task, see Changing power unit passwords.
Rebuild	Operations > Rebuild	No	For more information about performing this task, see Rebuilding the power unit.
View VLAN Network Data	Service and Support > View VLAN Network Data	Yes	For more information about performing this task, see Viewing VLAN network data.

HMC and SDMC management tasks

This topic provides console or appliance task information for moving from HMC to SDMC.

The following task mapping information is available in this topic:
- Update the HMC (SDMC) task mapping
- HMC (SDMC) management: operations task mapping
- HMC (SDMC) management: administration task mapping

Table 27. Update the HMC (SDMC) task mapping

HMC task	SDMC task	Is the task identical?	Notes
Update HMC	Welcome > Settings > Update SDMC	No	If you do not have a connection to the Internet, click Stop, and manually import the updates from a local file system or from a File Transfer Protocol (FTP) server. For more information about performing this task, see Updating the SDMC.

Table 28. HMC (SDMC) management: Operations task mapping

HMC task	SDMC task	Is the task identical?	Notes
View HMC Events	System Status and Health > Event Log Welcome	No	
Shut Down or Restart	System Status and Health > Event Log Welcome > Settings > Restart SDMC	No	The Restart task has an option to simply shut down as well. For more information about performing this task, see Restarting the IBM Systems Director Management Console.
View Trace Logs (HSCPE Only)	Welcome > Settings > Serviceability Tasks > View Trace Logs (PE Only)	Yes	
Schedule Operations	Task Management > Active and Scheduled Jobs	No	
Format Media	N/A	No	There is no equivalent function in the SDMC

Table 28. HMC (SDMC) management: Operations task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Back Up HMC Data	CLI: backup(hardware appliance only)	No	The SDMC only has a CLI for backup. This task is available only on the hardware appliance. The virtual appliance can be backed up with hypervisor disk snapshots. For more information about performing this task, see Backing up and restoring the SDMC and Using the SDMC remote command line.
Restore HMC Data	CLI: restore(Hardware Appliance Only)	No	SDMC only has a CLI for restore. This task available only on the hardware appliance. The virtual appliance can be restored from hypervisor disk snapshots. For more information about performing this task, see Backing up and restoring the SDMC and Using the SDMC remote command line.
Save Upgrade Data	N/A	No	SDMC upgrades do not need a separate save upgrade step.
Change Network Settings	Welcome > Settings > Configuration Tasks > Configure Network	No	For more information about performing this task, see Configuring the network.
Test Network Connectivity	N/A	No	There is no equivalent UI function in SDMC. For ping and routing information, the user can the appropriate command. For more information about performing this task, see Using the SDMC remote command line.
View Network Topology	N/A	No	There is no equivalent function in SDMC.
Tip of the Day	N/A	No	There is no equivalent function in SDMC.
Change Default User Interface Setting	N/A	No	There is no equivalent function in SDMC.
Change Date and Time	Welcome > Settings > Configuration Tasks > Configure Date/Time	No	For more information about performing this task, see Configuring date and time.

Table 28. HMC (SDMC) management: Operations task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Launch Guided Setup Wizard	N/A	No	The setup wizard is only shown on initial configuration.

Table 29. HMC (SDMC) management: Administration task mapping

HMC task	SDMC task	Is the task identical?	Notes
Change User Password	Welcome > Settings > Change user account password	No	For more information about performing this task, see Changing user accounts and passwords.
Manage User Profiles and Access	Welcome > Settings > Create user accounts Welcome > Settings > View user accounts Security > Users	No	For more information about performing this task, see Managing users and passwords.
Manage Tasks and Resource Roles	Security > Roles	No	For more information about performing this task, see Managing users and passwords.
Manage Users and Tasks	Security > Users	No	In SDMC, you can view running tasks in the Task Management area of the GUI. For more information about performing this task, see Managing users and passwords.
Manage Certificates	CLI: mkcert and updcert	No	CLI only. For more information about performing this task, see Using the SDMC remote command line.
Configure KDC	Welcome > Settings > Security Tasks > Configure Kerberos Client	No	For more information about performing this task, see Configuring the SDMC as a Kerberos client.
Configure LDAP	Welcome > Settings > Security Tasks > Configure LDAP Client	No	For more information about performing this task, see Configuring the SDMC as an LDAP client.
Remote Command Execution	N/A	No	SDMC enables Secure Shell (SSH) by default. You can control this only by using the firewall. For more information about performing this task, see Using the SDMC remote command line.

Table 29. HMC (SDMC) management: Administration task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Remote Virtual Terminal	N/A	No	SDMC has removed the remote VTTY port, and requires SSH instead for remote console connections. The SDMC GUI vterm applet now uses SSH.
Remote Operation	N/A	No	SDMC enables remote access to the web interface by default. You can control this only by using the firewall. For more information about performing this task, see Configuring the network.
Change Language and Locale	CLI: `chconfig -l`	No	The SDMC GUI can be controlled with the web browser locale settings. The console can be controlled with only the CLI. For more information about performing this task, see Using the SDMC remote command line.
Create Welcome Text	N/A	No	There is no equivalent function in SDMC. For more information about performing this task, see Create welcome text.
Manage Data Replication	N/A	No	There is no equivalent function in SDMC.
Manage Install Resources	N/A	No	There is no equivalent function in SDMC.

Service management

This topic provides service management task information for moving from HMC to SDMC.

The following task mapping information is available in this topic:
- Service management task mapping
- Service management: connectivity task mapping

Table 30. Service management task mapping

HMC task	SDMC task	Is the task identical?	Notes
Create Serviceable Event	Welcome > Manage > Service and Support Manager > Open a service request	No	For more information about performing this task, see Submitting service request using Service and Support Manager.

Table 30. Service management task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Manage Serviceable Events	Welcome > Manage > Service and Support Manager > Serviceable Problems	No	For more information about performing this task, see Managing serviceable problems by using Service and Support Manager.
Manage Remote Connections	N/A	No	There is no equivalent function in SDMC.
Manage Remote Support Requests	N/A	No	There is no equivalent function in SDMC.
Format Media	N/A	No	There is no equivalent function in SDMC.
Manage Dumps	Welcome > Manage > Service and Support Manager > Manage Support Files	No	For more information about performing this task, see Managing support files by using Service and Support Manager.

Table 31. Service management: connectivity task mapping

HMC task	SDMC task	Is the task identical?	Notes
Transmit Service Information	Welcome > Manage > Service and Support Manager > Settings	No	For more information about performing this task, see Activating the service and support manager.
Enable Electronic Service Agent	Welcome > Manage > Service and Support Manager > Settings	No	For more information about performing this task, see Activating the service and support manager.
Manage Outbound Connectivity	Welcome > Manage > Service and Support Manager > Settings	No	For more information about performing this task, see Activating the service and support manager.
Manage Inbound Connectivity	Welcome > Settings > Configure VPN	No	
Manage Customer Information	Welcome > Manage > Service and Support Manager > Manage your system contacts	No	For more information about performing this task, see Managing serviceable problems by using Service and Support Manager.
Authorize User	Welcome > Manage > Service and Support Manager > Settings	No	For more information about performing this task, see Authorizing user.
Manage Serviceable Event Notification	Welcome > Manage > Service and Support Manager > Settings (click the **learn more about automation plans** link)	No	SDMC supports email notification only. SNMP trap notification is not supported.
Manage Connection Monitoring	N/A		There is no equivalent function in SDMC.
Manage POWER4 Service	N/A		There is no equivalent function in SDMC.

Table 31. Service management: connectivity task mapping (continued)

HMC task	SDMC task	Is the task identical?	Notes
Agent Electronic Service Agent Setup Wizard	Welcome > Settings > Serviceability Tasks > Service and Support Manager Getting Started Wizard		

Functional differences between the HMC, IVM, and SDMC

There are functional differences between the Hardware Management Console (HMC) and Integrated Virtualization Manager environments and the Systems Director Management Console (SDMC) environment.

The SDMC incorporates most functions of the HMC. This has been done through direct mapping of commands or by replacing functions that are present already in IBM Systems Director. Some functions are not currently available for the SDMC, such the ability to handle system plans. For a complete listing of functions, see Comparing HMC tasks and SDMC tasks

Although the SDMC retains most of the functions that are available in the HMC, a few functional differences exist between the SDMC and the HMC. These differences are directed toward adapting to the IBM Systems Director environment and also toward improving the user interface.

The command-line interface (CLI) is essentially the same. On the SDMC, most of the commands are just preceded by smcli. This might require changes to existing scripts that use the HMC.

Enhanced virtualization management

The following are some of the key enhancements in virtualization management that are available in the SDMC:
* SDMC offers a simplistic IVM kind of user interface for virtualization functions, such as creating a virtual server.
* The views of virtual server properties and dynamic logical partitioning (DLPAR) are combined to present a single view from where you can perform all virtual server operations.
* SDMC provides the ability to change the resource assignment of your virtual servers even when they are in the Stopped state.
* SDMC can manage virtual slots automatically.

Users and roles

The concepts of users and roles in the SDMC remain the same as in the HMC. The user interfaces for creating and managing users and roles are different in the SDMC. SDMC follows the IBM Systems Director way of creating and managing users and roles. SDMC supports the use of LDAP and Kerberos servers. You can create users who use Lightweight Directory Access Protocol (LDAP) or Kerberos for authentication. Resource roles in HMC are referred to as *groups*in SDMC. Also, the session time-out and the idle time-out settings are global and not configured per user.

For more information about user and roles in the SDMC environment, see Predefined user IDs and passwords and SDMC roles

User interface enhancements

SDMC provides a user interface that is integrated with the broader IBM Systems Director user interface. Most of the tasks in SDMC have the same flow as in the HMC with slight enhancements to present an IBM Systems Director appearance.

Redundancy model

The existing redundancy model available in HMC is available in the SDMC as well. You can connect two SDMCs to a managed system in which one of the SDMCs acts as the redundant SDMC. You can also use an HMC for redundant management. Apart from this redundancy model, IBM Systems Director provides an active-passive availability model that is optional for the SDMC users. In this model, two SDMC nodes can manage a single server, of which one node is used (active) and the other is not used (passive), waiting for a failover condition. The existing HMC active-active redundancy model is available in addition to the active-passive availability model, both provided by the IBM Systems Director.

Backup and Restore

SDMC provides the capability to back up the entire virtual machine to removable media or to a remote File Transfer Protocol (FTP) server. You can restore using the backup file from the removable media or from a remote FTP server. The restore operation is a full image deployment and all existing files are replaced from the backup file. Unlike the HMC, SDMC backs up the entire disk instead of individual files.

For more information about performing a backup and restore of the SDMC environment, see Backing up and restoring the SDMC

Additional functions

The SDMC includes the IBM Systems Director base management functions which offers you additional capabilities to manage your heterogeneous and large homogeneous infrastructure better. These capabilities include:
* Automation manager
* Update manager
* Status manager

SDMC supported and unsupported systems

Support for POWER processor-based systems with either software or hardware appliance depends on the type of POWER system you have. This topic provides a complete listing of which appliance is supported with which system.

Table 32. POWER7 support by SDMC

POWER7 models	Machine types	SDMC
795	9119-FHB	Hardware appliance only
780	9179-MHB	Hardware appliance only
770	9117-MMB	Hardware appliance only
755	8236-E8C	Hardware or software appliance
750	8233-E8B	Hardware or software appliance
720	8202-E4B	Hardware or software appliance
740	8205-E6B	Hardware or software appliance
710/730	8231-E2B	Hardware or software appliance
PS701	8406-71Y	Hardware or software appliance
PS700	8406-70Y	Hardware or software appliance

Table 33. POWER6 support by SDMC

POWER6 Models	Machine types	SDMC
595	9119-FHA	Hardware appliance only
575	9125-F2A	Hardware appliance only
570	9117-MMA	Hardware appliance only
570	9406-MMA	Hardware appliance only
560	8234-EMA	Hardware appliance only
550	8204-E8A	Hardware or software appliance
550	9409-M50	Hardware or software appliance
520	8203-E4A	Hardware or software appliance
520-SB (IBM Smart Cube)	8261-E4S	Hardware or software appliance
520	9408-M25	Hardware or software appliance
520	9407-M15	Hardware or software appliance
JS23/43	7778-23X	Hardware or software appliance
JS22	7998-61X	Hardware or software appliance
JS12	7998-60X	Hardware or software appliance

Supported configurations

You can connect your SDMC to host systems in a variety of ways.

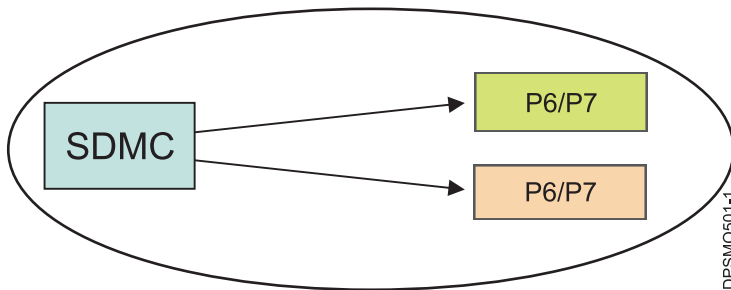The following topic describes the different ways you can manage host systems using the SDMC.

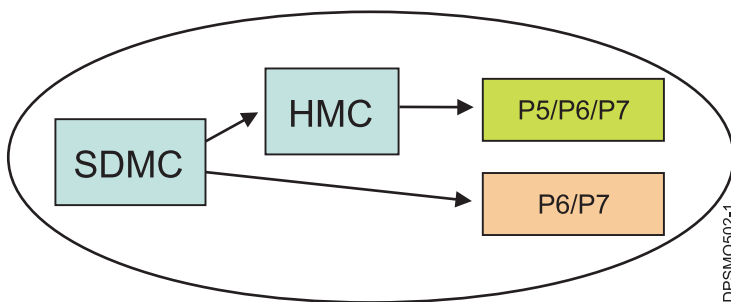*Figure 1. SDMC managing multiple Power Systems servers*

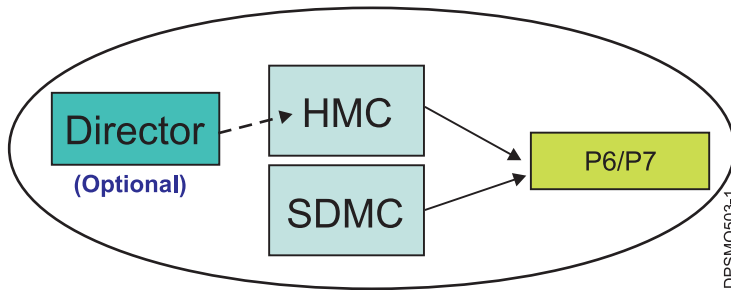*Figure 2. SDMC managing two different Power systems, where one is managed by an HMC*

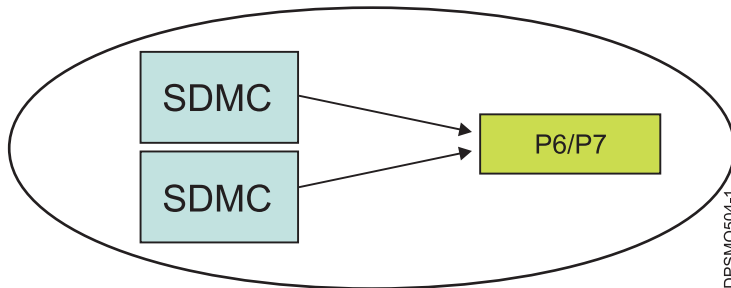*Figure 3. HMC and SDMC managing the same server at the same time*

Figure 4. Two SDMCs managing the same server at the same time

SDMC redundancy and high availability features

Implementing SDMC in a high availability (HA) or a redundant setup can provide improved serviceability to the SDMC appliance and provides backup to the system in case of a disaster.

SDMC HA versus redundant setup

If you are familiar with redundant HMC setup in your Power Systems environment, you can do the same with SDMC, because multiple SDMCs can connect to and actively manage a single host.

For more information about the tasks associated with SDMC redundancy and high availability, see SDMC installation and configuration scenarios and Configuring high availability.

You can also implement SDMC HA, which provides active/passive failover capability, with one active SDMC and one passive SDMC on standby to take over in case of failure.

In addition to providing the management capabilities currently in the HMC for the managed Power Systems hosts, the SDMC also can manage the operating systems of the hosts themselves by connecting to the Common Agent Services (CAS) agent on the managed systems through an agent manager. However, the CAS agent has the limitation of only a single connection to an agent manager and is not capable of a redundant connection. Therefore, the SDMC HA feature is provided to eliminate this limitation as a single point of failure if you require high availability for this functionality.

The choice between a redundant setup versus an active/passive HA implementation depends on your planned usage of the SDMC:
* In an environment where the SDMC is being used for HMC-like management functions, the redundant setup provides the most availability and is the easiest to set up and administrate. Both SDMCs will be

active and can continue to provide functions for the managed systems should one of them have a failure. The setup of a redundant SDMC environment only involves adding the managed system to both SDMCs.

- For an environment where the SDMC is being used for agent OS management and there is a high availability requirement for that function, SDMC HA is needed. If your active SDMC fails, the passive standby SDMC automatically takes over and management functions for the managed systems are restored in about 10 minutes. Some extra planning, setup, and administrative steps are required to implement SDMC HA. For more information about the planning tasks associated with implementing high availability, see Planning for high availability, redundancy, and failover.

The following table shows the differences between redundant HMCs and IBM Systems Director high availability setup.

Table 34. Differences between a redundant and a replication HA environment

	HMC	SDMC with redundancy	Systems Director or SDMC with HA
Type of environment	Redundant	Redundant	Replication
High availability topology	Active/active: Both consoles are active at the same time.	Active/active: Both consoles are active at the same time.	Active/passive: Only one console is active at a time.
Data	Data is not identical.	Data is not identical.	All data is identical on the two nodes.
Management console	HMC	Systems Director	Systems Director
Console versions	Can be different	Can be different	Must be the same

In a redundant setup, it is also possible to have one SDMC point to another SDMC's agent manager, which would allow both SDMCs to manage the agents at the same time. However, since the agent manager is running on only one of the SDMCs, this setup is a single point of failure. If this SDMC goes down, the other SDMC loses contact with the agents.

Active/passive HA overview

In a high availability environment, two SDMCs operate as synchronized nodes in an active/passive cluster. One node in the environment is kept active at all times, and a second passive node is kept in close synchronization. If your active node fails, the passive node (on standby, waiting for a failure of the active node) takes over in about 10 minutes.

The internal software components that make up SDMC HA are transparent to you and do not need to be directly configured. Floating IP addresses used to connect to the active SDMC can be moved between the nodes, by using the active node. The OS on the passive node is started, but the software stack is not.

Running the Guided Setup wizard or the command-line interface commands on the SDMC that is designated to be the primary node configures the internal HA components on both the primary and secondary SDMCs.

High availability terminology

Refer to this list of terms to help you better understand high availability concepts:

Node A node is an SDMC that is configured to be part of a high availability environment.

Active node

An active node manages your environment. Only one node is active at a time.

Passive node

The passive node is not currently active. Any changes you make to the active node are replicated to the passive node.

Primary node

This is the node you use to set up high availability. It is initially the active node. When you set up a high availability cluster, the IBM Systems Director data, remote authentication configuration settings, users, and firewall settings on this node are replicated to the secondary node.

Secondary node

This is the node that you set up to take over if the primary node fails. It is initially the passive node, but takes over as the active node if the primary node is detected to have failed.

Network status IP address

The cluster nodes use this IP address to determine which node is connected to the network. If they cannot contact each other, the node that can connect to this IP address becomes the active node.

Floating IP address

This address is always assigned to the active node. Always access this address so that you do not have to know which node is active. It also enables you to use IBM Systems Director Common Agent with high availability.

Active/passive HA mirrored directories

The following directories that are replicated and synchronized between the active SDMC and the passive SDMC in the HA cluster.

Table 35. Replicated and synchronized SDMC directories

Directory	Description
/opt/ibm/director/data	Director data
/home/db2inst1	DB2 data
/opt/ibm/director/keys	License keys
/opt/ibm/director/lwi/conf/overrides	Director property overrides
/opt/ibm/director/lwi/runtime/agentmanager/eclipse/ plugins/com.ibm.tivo li.cas.manager/config	CAS agent manager config
/opt/ibm/director/lwi/runtime/agentmanager/eclipse/ plugins/com.ibm.tivo li.cas.manager/certs	CAS agent manager certificates
/opt/ibm/director/lwi/runtime/core/DATABASE	CAS agent manager database
/opt/ibm/director/lwi/runtime/agentmanager/toolkit/ certs	CAS agent manager toolkit certificates
/opt/ibm/director/lwi/runtime/agentmanager/toolkit/ config	CAS agent manager toolkit configuration files
/var/lib/dhcp	Dynamic Host Configuration Protocol (DHCP) server
config /dump	Flexible service processor (FSP) dump files
/var/hsc/log	SDMC log files
/var/hsc/profiles	Profile files
/opt/hsc/data/utilization	Utilization files

SDMC HA synchronized data

The following data changes on the active SDMC are synchronized to the standby SDMC:

- User ID additions

- User ID modifications
- User ID deletions
- Firewall changes
- Network Time Protocol (NTP) configuration
- Kerberos and Lightweight Directory Access Protocol (LDAP) configuration
- Initial HA configuration
    - Distributed Replicated Block Device (DRBD) configuration
    - Users
    - Authentication files
    - LDAP and Kerberos
    - Firewall settings
    - Domain Name System (DNS) resolver
    - NTP configuration

SDMC HA processes monitored

The following processes are monitored by the SDMC HA for a redundant takeover:
- Director
- DB2
- DRBD
- CIM server
- HA MQ daemon – MQ server
- HA daemon – Processes MQ messages
- NTP server
- DHCP server

Active/passive HA: Log location

The locations of the HA log files follow:
- /opt/ibm/director/ha/logs/daemon0-x.log

Table 36. daemon0-x.log file description

Log file	Description
daemon0-x.log	HA daemon log
mq0-x.log	ActiveMQ log
smha.log	TSA monitor log
init0-x.log	Initial configuration initiated from outside the Director process

- /opt/ibm/director/lwi/logs

    HA task logs captured in the Systems Director HA configuration task.
- The daemon log and mq log are rolling logs with up to five log files, where *x* is the log file number. Each log file can contain approximately 10 MB of data.

SDMC and HMC command-line differences

There are differences between the HMC commands and the SDMC commands.

Commands used to manage the Power Systems servers such as lssyscfg, lshwres, and chhwres that are all supported and virtually identical to the commands in the HMC. Any scripts that you may have that use these commands should continue to work with no changes.

To see all of the HMC commands that are supported on the SDMC, run the smcli lsbundle command. The commands that have been carried over from the HMC are in the psm bundle.

The following topic describes how to run SDMC commands. Commands for managing Power Systems resources can be run in exactly the same way as on an HMC. However, to integrate into the Systems Director way of doing commands, there are additional ways to issue commands. The following commands are all equivalent:

- lssyscfg –r sys
- smcli lssyscfg –r sys
- smcli psm lssyscfg –r sys
- The commands that have been carried over from the HMC are aliased. Therefore, you can run the command in three ways from the command line: lssyscfg, smcli lssyscfg,, or smcli psm lssyscfg .
- Add managed system (mksysconn) in SDMC has been replaced by the smcli discover and smcli accesssys Systems Director commands.
- Two attributes, **primary_state** and **detailed_state**, are introduced to the lssyscfg and lssysconn commands to indicate the respective Systems Director state mapping. The **state** field is deprecated. It is only shown when the **-F** option is used.
- Man pages for the SDMC commands can be displayed by running either man command_name or man psm.command_name.

The following tables compare HMC command-line interface (CLI) function with SDMC CLI function. These tables display only the changes, and all functions not shown can be assumed to be similar.

Table 37. Power Systems management commands

HMC tasks and commands	SDMC commands	Notes
Add Managed System: mksysconn –r sys/frame	smcli discover –H smcli accesssys	Discover and access are two separate steps on SDMC. Make sure you specify the IP or hostname in SDMC; otherwise, by default, it discovers everything on your subnet. If SDMC is acting as the DHCP server, systems must be automatically discovered. You must request access.
Remove Managed System: rmsysconn –o remove	smcli rmsys	You can disconnect by using the smcli revokeaccesssys command; however, to completely remove the system, you must use smcli rmsys.
List system or partition states: lssyscfg –r sys/lpar –F state	lssyscfg –r sys/lpar –F primary_state,detailed_state	Although the HMC state option is supported, to view the states as the SDMC GUI displays them, you need to view the primary_state and detailed_state.
List serviceable events: lssvcevents	smcli lssvcproblem	

Table 38. Appliance (SDMC) management commands

HMC tasks and commands	SDMC commands	Notes
List and change HMC information such as version and locale: lshmc / chhmc	lsconfig / chconfig	

Table 38. Appliance (SDMC) management commands (continued)

HMC tasks and commands	SDMC commands	Notes
List and change HMC network settings: `lshmc -n / chhmc`	`lsnetcfg / chnetcfg`	
Backup and restore console data: `bkconsdata`	`backup / restore`	Hardware appliance only
LDAP configuration: `chhmcldap / lshmcldap`	`cfgldap / lsldap`	
Shut down and restart HMC; `hmcshutdown`	`smshutdown`	
Create and list HMC users: `ls/mk/ch/rmhmcuser`	`mksmusr / chsmusr / rmsmusr / smcli lsuser`	
Save and restore upgrade data: `saveupgdata / rstupgdata`	N/A	This is not needed on SDMC because the save/restore process happens automatically as part of an upgrade.
Manage password policies: `mk/ch/ls/rmpwdpolicy`	N/A	SDMC does not support password policy profiles.
Manage access control: `mk/ch/ls/rmaccfg`	`smcli mk/ch/ls/rmrole`	
Monitor HMC: `monhmc`	N/A	

Systems Director Management Console limitations

Learn about IBM Systems Director Management Console (SDMC) limitations.

Consider the following limitations when you plan to migrate from Hardware Management Console (HMC) to SDMC:

- Replication of user data, groups data, LDAP or Kerberos configuration data, and outbound connectivity configuration data is not supported in SDMC.
- Management of POWER5™ technology-based systems is not supported in SDMC.
- Modem or VPN support for Call home function is not available in SDMC. The Call home function is supported only on a network connection over SSL.
- Users cannot disconnect and reconnect to old sessions of SDMC.
- No Advanced Manager support in SDMC.

Accessibility features for *SDMC*

This topic provides information about the accessibility features of *SDMC*

The SDMC is used for managing virtual servers and other hardware management tasks. The hardware accessibility features of the SDMC are the same as for other IBM hardware. The graphical user interface for SDMC software offers full keyboard accessibility, but is not currently accessible with screen readers or other assistive technology. You can access the SDMC software remotely to take advantage of assistive technologies available in the Windows environment. However, full screen reader support is not currently available.

A partial command-line interface is available for the SDMC. See Accessibility features for SDMC for more information about which functions are available through the command line, and how to use the command-line interface.

SDMC installation and configuration scenarios

Learn about the tasks associated with different SDMC installation and configuration scenarios.

This section describes, at a high level, the tasks you must perform when you install and configure your SDMC. There are different ways you can install and configure your SDMC. Find the scenario that best matches the task you want to perform.

Installing and configuring a new SDMC to manage a new host

Learn more about the high-level tasks you must perform when installing and configuring a new SDMC with a new host.

Table 39. Installing and configuring a new SDMC to manage a new host

Task	Where to find related information
1. Gather information and complete planning.	Planning for installation
2. Unpack the hardware appliance.	
3. Install the SDMC software or hardware appliance.	"Installing the SDMC software appliance" on page 33 "Installing the SDMC hardware appliance" on page 37
4. Power on the SDMC hardware appliance by pressing the power button.	
5. Log in and launch the SDMC.	
6. Use the Guided setup wizard to configure the SDMC.	"Configuring the SDMC using the Guided Setup wizard" on page 47
7. Attach the server to the SDMC.	
8. Power on the managed server.	
9. Set managed server passwords using SDMC.	Setting passwords for the managed system

Installing and configuring a new SDMC to manage an existing host

Learn more about the high-level tasks you must perform when installing and configuring a new SDMC to work with an existing host.

Table 40. Installing and configuring a new SDMC to manage an existing host

Task	Where to find related information
1. Gather information and complete planning.	Planning for installation
2. Unpack the hardware appliance (if applicable).	
3. Install the SDMC software or hardware appliance.	"Installing the SDMC software appliance" on page 33 "Installing the SDMC hardware appliance" on page 37
4. Power on the SDMC hardware appliance (if applicable) by pressing the power button.	
5. Log in and launch the SDMC.	
6. Use the Guided setup wizard to configure the SDMC.	"Configuring the SDMC using the Guided Setup wizard" on page 47

Table 40. Installing and configuring a new SDMC to manage an existing host (continued)

Task	Where to find related information
7. Transition from using the HMC or IVM to using the SDMC to manage your hosts.	If your existing host is managed by the HMC, see "Moving from HMC to SDMC" on page 59. If your existing host is managed by the IVM, see "Moving from IVM to SDMC" on page 58.

Installing and configuring an SDMC to work with an existing HMC or SDMC

Learn more about the high-level tasks you must perform when installing and configuring an SDMC to work with an existing HMC.

Table 41. Installing and configuring an SDMC to work with an existing HMC

Task	Where to find related information
1. Gather information and complete planning.	Planning for installation
2. Unpack the hardware appliance (if applicable).	
3. Install the SDMC software or hardware appliance.	"Installing the SDMC software appliance" on page 33 "Installing the SDMC hardware appliance" on page 37
4. Power on the SDMC hardware appliance (if applicable) by pressing the power button.	
5. Log in and launch the SDMC.	
6. Use the Guided setup wizard to configure the SDMC.	"Configuring the SDMC using the Guided Setup wizard" on page 47

Installing the SDMC software appliance

Describes how to install the SDMC software appliance option.

The SDMC Software Appliance can be installed in your existing x86 virtualized infrastructure. For more information about the SDMC software appliance requirements, see SDMC software appliance requirements. Virtualization hypervisor options include VMware (vSphere server and ESXi version 4 or later--at least 4.1 required if USB support is desired) and Red Hat Enterprise Linux (RHEL) Enterprise KVM version 5.5 or later.

You can choose to install your software appliance by using one of the two installation media options:
* By downloading the installation media from an IBM web site.

  The web download option for VMware will contain an Open Virtualization Archive (OVA). In addition to disks, OVA contains an Open Virtualization File (OVF) describing the appliance (e.g. disk names, disk sizes, number of CPUs to allocate) and a manifest with checksums of each disk. This web download will contain just the single OVA.

  The web download option for KVM will contain a gzipped tar file containing seven virtual disk images in the IMG file format.
* By installing from DVD media.

  Multiple DVDs contain disk images, OVF, and manifest files.

For more information about each Hypervisor installation option, read the following sections.

Installing and configuring hypervisors

Provides information to help you select the hypervisor software to use with your SDMC appliance.

Installing the SDMC software appliance for VMware ESX and ESXi 4

Describes the SDMC deployment methods used for VMware ESX and ESXi 4.

Two different methods are available to install the SDMC software appliance for VMware ESX and ESXi 4. You can choose one of the following methods:
* Download and install the VMware OVF tool using the command line
* Use the graphical interface on the VMWare Virtual Infrastructure Client

Note: To use the command line method of deployment for VMware, you must first install the VMware OVF Tool on a Windows or Linux machine. Download the VMware OVF Tool here: Open Virtualization Format Tool

Note: If using thin provisioning as in the below examples, ensure that you have the space needed to contain the SDMC data. Using thick provisioning would guarantee the storage required.

Note: Ensure that the virtual machine created by your hypervisor supports both a public and a private network.

After performing either of the above steps to deploy the OVA file and create the SDMC appliance, you must configure the public and private network interfaces on the VM client within VMware. You can then map the logical adapters in the SDMC image to the VMnetworks defined in VMware as part of the Setup Wizard process. For more information about using the Setup Wizard to configure your SDMC, see "Configuring the SDMC using the Guided Setup wizard" on page 47.

Downloading and installing the VMware OVF tool using the command line

Note: In the below examples for the CLI install, the thin provisioned format is selected as the format to store the virtual machines virtual disks. Using this format, the storage is allocated on demand as data is written to the virtual disks. This is only supported on VMFS3 and newer datastores. Otherwise, the thick format (in which the storage is allocated immediately) can also be used.

To download and install the VMware OVF tool using the command line, do the following:
1. Download the VMWare OVF tool, available at the following Website:
   - http://communities.vmware.com/community/vmtn/vsphere/automationtools/ovf

   Note: vSphere Client is only available for Windows and can be downloaded from the web address of the ESX or ESXi Server.
2. Obtain the OVA file that contains the SDMC Virtual Machine.
3. Because all files and images needed are contained within the OVA, you can simply deploy the package. Note that the descriptive syntax within and including the <> should be replaced with the appropriate user-specified string:
   - If you are using Linux, use the following command to deploy the package:

     ```
     /usr/bin/ovftool --name=SDMC –ds=<datastore name on ESX>
     [-dm=thin] <OVA filename> vi://<user>:<password>@<ESX hostname>
     ```
   - If you are using Windows, use the following command to deplaoy the package:

     ```
     "Program Files\VMware\VMware OVF Tool\ovftool.exe" --name=SDMC
     –ds=<datastore name on ESX> [-dm=thin] <OVA filename>
     vi://<user>:<password>@<ESX hostname>
     ```

     Here is an example of the output from the OVF TOOL CLI using an OVA file on Windows:

     ```
     C:\>"Program Files\VMware\VMware OVF Tool\ovftool.exe" --name=sdmc
     -ds=datastore1 -dm=thin "c:\sdmc\SDMC_1046A_730_1117.ova"
     "vi://root:passw0rd@172.16.20.20"

     Output:
     Opening OVA source: c:\sdmc\SDMC_1046A_730_1117.ova
     Opening VI target: vi://root@172.16.20.20/
     Target: vi://172.16.20.20/
     ```

Downloading and installing the VMware OVF tool using the VMWare Vsphere Client with OVA

Note: The Vsphere client is only available for Windows and can be downloaded from the web address of the ESX(i) Server. If you choose this deployment method, fully allocated disk files representing the disks are created.

To download and install the VMware OVF tool using the VMWare Vsphere Client with OVA, do the following:
1. Obtain the OVA file that contains the SDMC Virtual Machine.
2. Click **File > Deploy OVF Template...**.
3. Click **Deploy from file** and then click **Browse**.
4. Navigate to the directory where you saved the OVA file, select the OVA file, and then click **Next**.
5. Continue through the wizard to complete the installation and start the deployment of the SDMC.

Installing configuring KVM

Describes how to install and configure KVM for the SDMC software appliance.

You can install the SDMC software appliance on KVM by using the pre-installed virtual disks. To install the SDMC software appliance on KVM, do the following:

1. Verify that virtualization software is installed on RHEL. You must have KVM, libvirt and VM manager installed. Run the command **virsh** as the root user to determine whether you can see the virsh shell.

2. Download `<SDMC Installation filename>.tar.gz` to the host system.

3. Extract virtual disk images from **CSDA.tar.gz** using the following command: `tar -xzvf SDMC_1046A_730_1117.tar.gz` This will extract the following disk images:
   - **dvmdisk1.img**
   - **dvmdisk2.img**
   - **dvmdisk3.img**
   - **dvmdisk7.img**

4. Create the domain XML file. You have to provide custom values for the following fields:
   - MAC addresses (by using the **mac address** tag). You can use the following script to generate the MAC address:

     ```
     echo -n 00:1A:64 ; for i in `seq 1 3` ; do echo -n `echo
     ":$RANDOM$RANDOM" | cut -n -c -3` ;done; echo \n
     ```

     (If you prefer, you can replace the **00:1A:64** with any other prefix).
   - Bridge name (**source bridge** tag). To get available bridges on your host, run the command **brctl show**. A second bridge will also be needed for the private management network.
   - VM name, source files for hard disks and CDROM. Update memory and CPU values, if necessary.

   ```
   <domain type="kvm">
   <name>VM1</name>
   <uuid/>
   <memory>6144000</memory>
   <vcpu>2</vcpu>
   <os>
   <type arch="x86_64">hvm</type>
   <boot dev="hd"/>
   </os>
   <features>
   <acpi/>
   </features>
   <clock offset="utc"/>
   <on_poweroff>destroy</on_poweroff>
   <on_reboot>restart</on_reboot>
   <on_crash>destroy</on_crash>
   <devices>
   <disk type="file" device="disk">
   <source file="/vdisk1/vm1/dvmdisk1.img"/>
   <target dev="vda" bus="virtio"/>
   </disk>
   <disk type="file" device="disk">
   <source file="/vdisk1/vm1/dvmdisk2.img"/>
   <target dev="vdb" bus="virtio"/>
   </disk>
   <disk type="file" device="disk">
   <source file="/vdisk1/vm1/dvmdisk3.img"/>
   <target dev="vdc" bus="virtio"/>
   </disk>
   <interface type="bridge">
   <source bridge="virbr1"/>
   <mac address="00:1A:64:27:30:19"/>
   <target dev="vnet0"/>
   <model type="e1000"/>
   </interface>
   <interface type="bridge">
   <source bridge="virbr1"/>
   <mac address="00:1A:64:27:30:20"/>
   <target dev="vnet1"/>
   <model type="e1000"/>
   ```

```
</interface>
<interface type="bridge">
<source bridge="virbr1"/>
<mac address="00:1A:64:27:30:21"/>
<target dev="vnet2"/>
<model type="e1000"/>
</interface>
<interface type="bridge">
<source bridge="virbr1"/>
<mac address="00:1A:64:27:30:22"/>
<target dev="vnet3"/>
<model type="e1000"/>
</interface>
<serial type="file">
<source path="/vdisk1/vm1/boot.log"/>
<target port="1"/>
</serial>
<input type="mouse" bus="ps2"/>
<graphics type="vnc" autoport="yes" listen=""/>
<video>
<model type="cirrus" vram="9216" heads="1"/>
</video>
</devices>
</domain>
```

5. Define VM. Use the following command: `virsh define <domain>.xml`

6. Start VM. Use the following command: `virsh start VM_name`

Go through Setup Wizard on KVM virtual machine console to customize the VM. For more information, see Creating a virtual server.

Installing the SDMC hardware appliance

You must install the SDMC hardware appliance.

The IBM Systems Director Management Console (SDMC) hardware appliance is required for the midrange and higher classes of POWER processor-based servers. The hardware appliance can also manage entry-level systems. The hardware appliance is preinstalled on the IBM x86 hardware (a 7042-CR6). The hardware appliance consists of a virtual image that resides on a Red Hat Linux configured host system. Unlike the software appliance, you cannot log into the host system or access the hypervisor.

For the hardware appliance, you must have at least one network connection to connect to the service processor of your POWER processor-based system. To configure a private and an open network, you need at least two network connections, one in an open network (over which you can reach the SDMC via a web browser), and one private network for connecting the SDMC with the service processor of your POWER system. .

Installing the SDMC into a rack

This section describes how to install the SDMC into a rack.

Complete a parts inventory. The following illustration shows the items that you need to install the server in the rack cabinet. If any items are missing or damaged, contact your place of purchase.
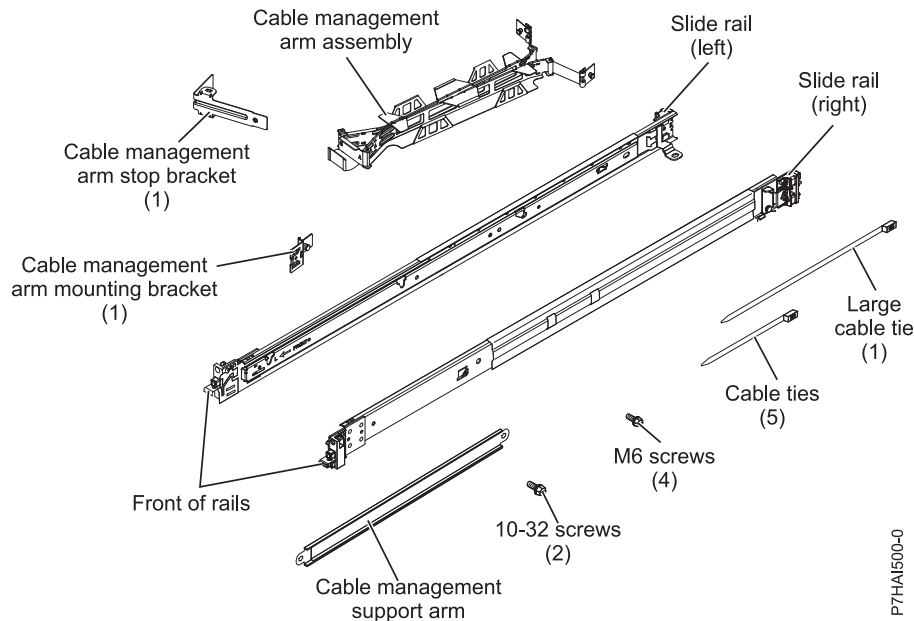

Figure 5. Parts inventory

Note: Screws can be used for shipping, or for additional stabilization in high-vibration areas.

To install the SDMC into a rack, complete the following steps:
1. Each slide rail is marked with either an R (right) or an L (left). Select one of the slide rails and push up on the front movable tab **(1)**; then, pull out the front latch **(2)** to slide out the front side rail. If a

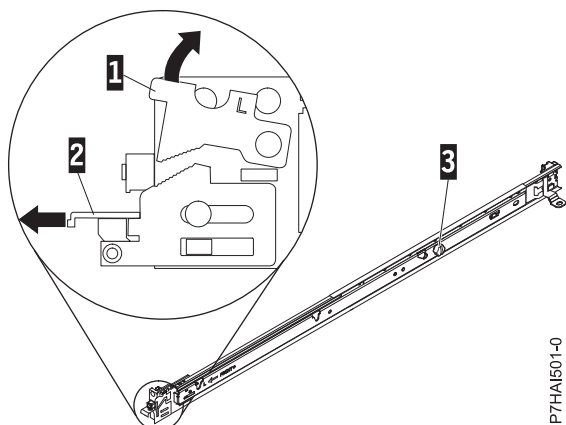thumbscrew is installed in the slide rail **(3)**, remove it.

Figure 6. Slide rail and movable tab

> **Note:** Make sure that the movable tab remains extended and does not click back into place.

2. Align the three pins on the rear of the slide rail with the three holes in the selected U on the rear of the rack. Push the rails so that the pins go into the holes **(1)**, and drop the slide rail down **(2)** until it latches into place.
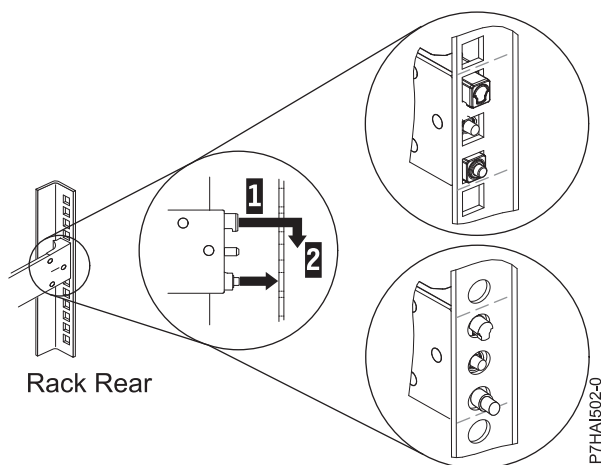

Figure 7. Align the pins with the holes in the rear of the rack

3. Pull the slide rail forward and insert the two pins **(1)** on the front of the rail into the two lower holes in the U on the front of the rack. Drop the rail into place until it clicks into place. Push the front latch **(2)** in all the way. Repeat steps 1 through 3 to install the other rail into the rack. Make sure that each front latch is fully seated.
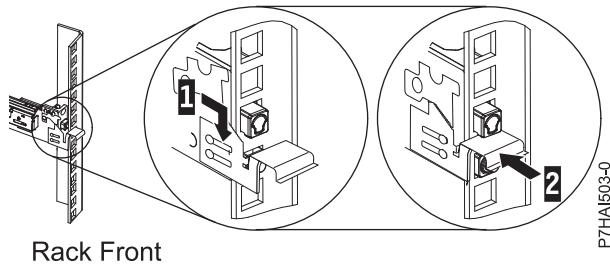
Figure 8. Rack front rail and pins

4. Pull the slide rails forward **(1)** until they click, twice, into place. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads **(2)** on the server line up with the rear slots **(3)** on the slide rails. Slide the server down until the rear nail heads slip into the two rear slots, and then slowly lower the front of the server **(4)** until the other nail heads slip into the other slots on the slide rails. Make sure that the front latch **(5)** slides over the nail heads.
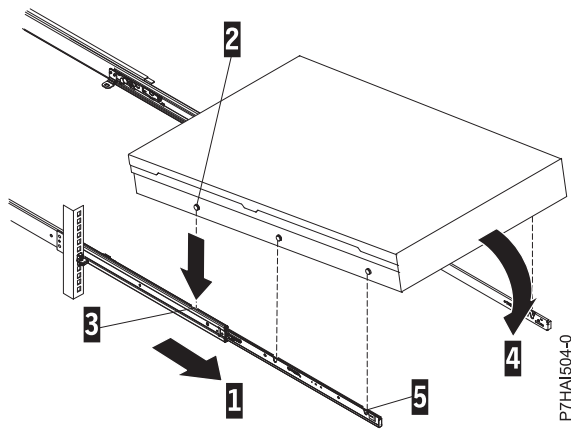

Figure 9. Slide rails extended, server nail heads aligned with slots in rail

5. Lift the blue release latches **(1)** on the slide rails and push the server **(2)** all the way into the rack until it clicks into place.
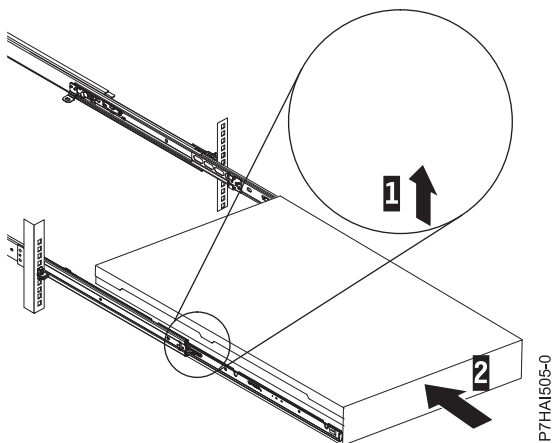

Figure 10. Release latches and server

6. Slide the server into the rack until it snaps into place.

Installing the cable-management arm

You might need to install the cable-management arm. Use this procedure to perform this task.

To install the cable-management arm, complete the following steps:

Note: The procedure for installing the cable-management arm involves the assembly of the following parts:

A	Support arm
B	Cable-management stop bracket
C	Mounting bracket
D	Cable-management arm
E	Extension bracket

The following figure shows the parts of the cable-management arm in relative position to each other before their assembly.
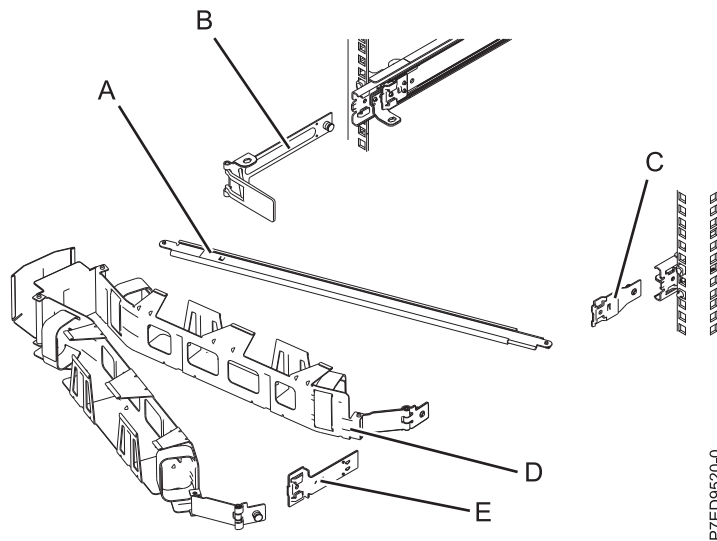

Figure 11. Relative positions of cable-management arm parts before assembly

1. The cable-management arm must be installed on the right side of the server, when you are facing it from the rear. The following figure shows it being installed on the right side. Connect one end of the support arm **(A)** to the right slide rail **(1)** so that you can swing the other end of the support arm **(2)** toward the left side of the rack.
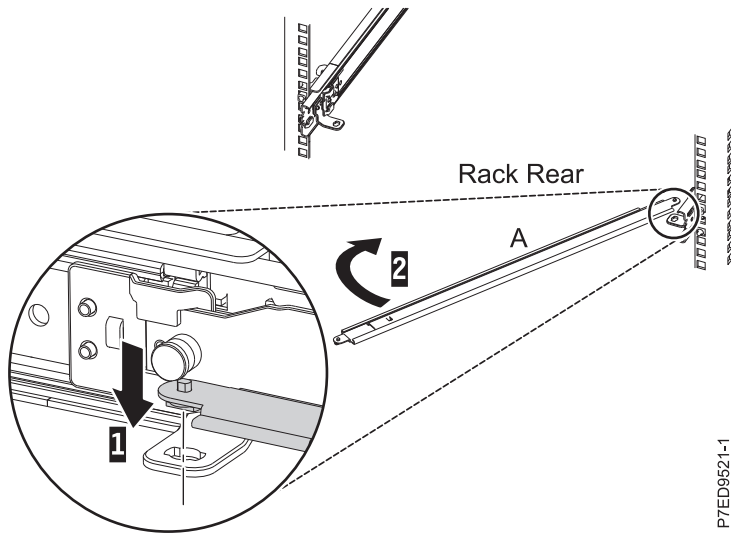
Figure 12. Support arm connection

2. Locate the hole at the bottom inside corner of the L-shaped cable-management stop bracket **(B)**. Position the unattached end of the support arm so that the locking tab on the underside of its tip aligns with the bracket hole. Insert the tab into the hole **(1)** and turn the bracket **(2)** to secure it to the support arm.
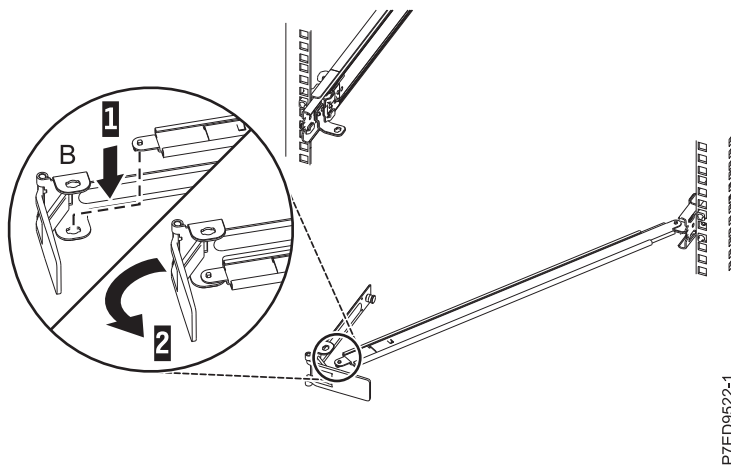

Figure 13. Cable-management stop bracket secured to the support arm

3. To attach the other side of the support arm to the backside of the slide rail, pull the pin out **(1)**, and then slide the bracket **(B)** into the left slide rail **(2)**.
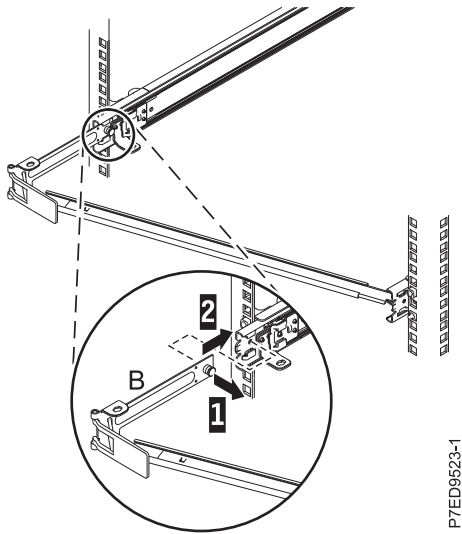
Figure 14. Pin extended, bracket installed into slide rail

4. Slide the extension bracket **(E)** into the right slide rail **(2)**. Push the bracket into the slide rail until the spring-loaded latch snaps into place.

Figure 15. Extension bracket installed into slide rail

5. Attach the mounting bracket **(C)** to the slot on the inside of the right slide by pulling the pin out **(1)**, and sliding the mounting bracket **(C)** into the slide rail until the spring-loaded pin snaps into place **(2)**.
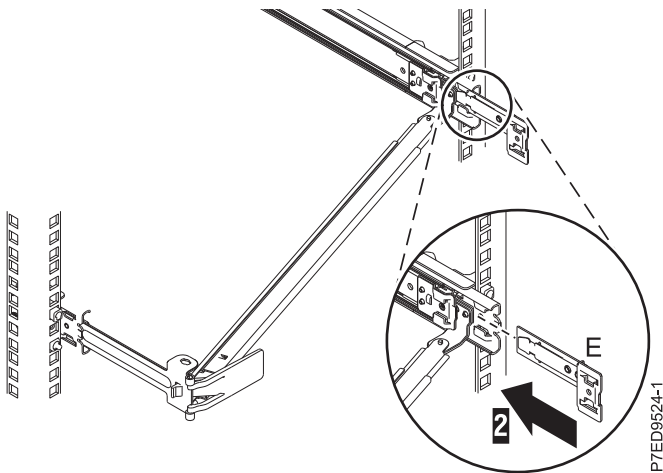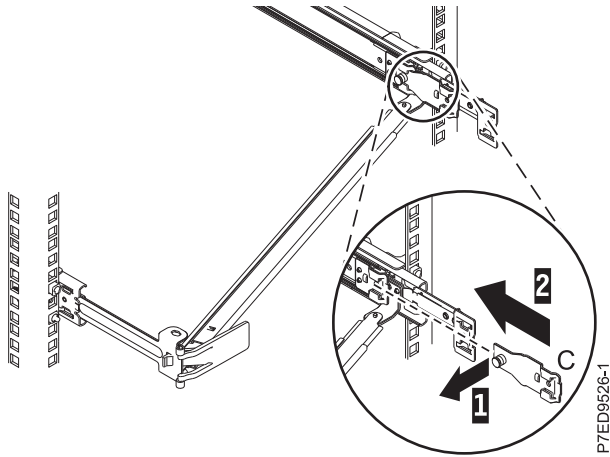
Figure 16. Mounting bracket installed into slide rail

6. Place the cable-management arm **(D)** on the support arm **(A)**. Pull out the cable-management arm pin **(1)**, and then slide the cable-management arm tab **(2)** into the slot on the mounting bracket **(C)**. Push the tab until it snaps into place. Pull out the other cable-management arm pin **(3)**, and then slide that cable management arm tab into the extension bracket **(E)** slot **(4)** on the outside of the right slide rail. Push the tab until it snaps into place.

Figure 17. Cable-management arm connection
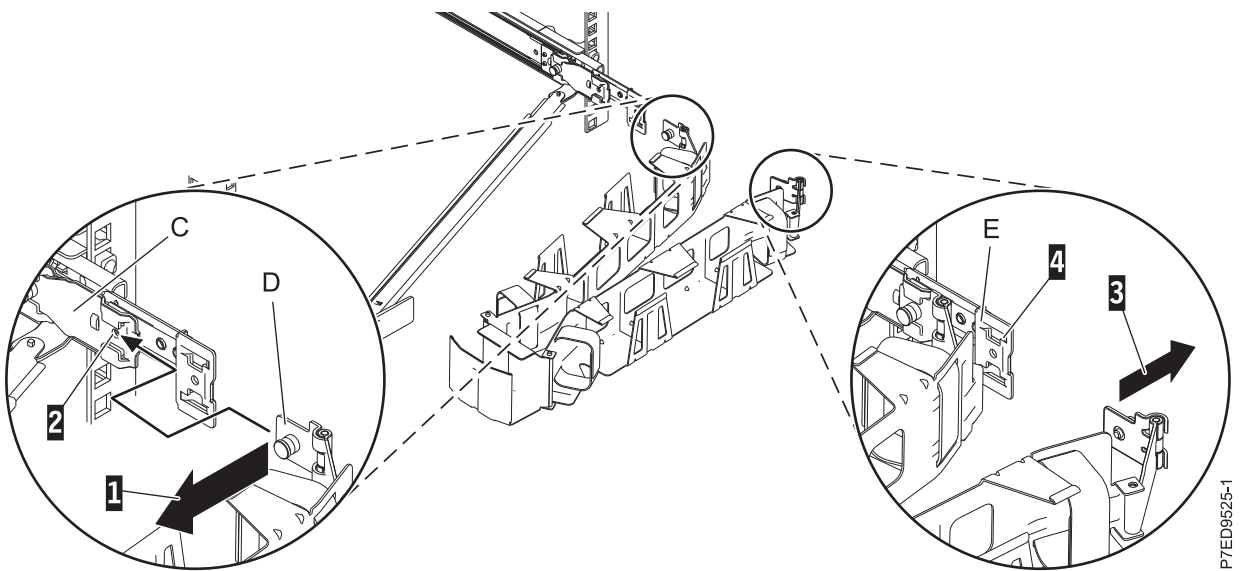
7. Route the power cords and other cables (including keyboard, monitor, and mouse cables, if required) on the cable-management arm **(1)**. Attach all cables to the rear of the server except for the power cord. Secure the cord and cables with cable ties or hook-and-loop fasteners.

   Note: Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.
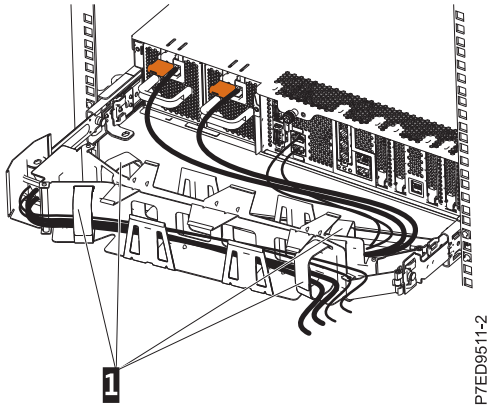
Figure 18. Power cord attachment and routing

8. Slide the server into the rack until it snaps into place.

Cabling the Systems Director Management Console

Connect the IBM Systems Director Management Console (SDMC) cables, connect the Ethernet cable, and connect the SDMC to a power source.

If the physical SDMC is not located within 8 meters (25 feet) away from the server, you must supply a separate system that can access the Internet using a browser. This system must be within 8 meters (25 feet) of the server. This setup allows service personnel remote access to the SDMC and manually perform removal and replacement procedures on the server. The SDMC must also be configured to allow for this remote access.

DANGER

Electrical voltage and current from power, telephone, and communication cables are hazardous.

To avoid a shock hazard:
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described below when installing, moving, or opening covers on this product or attached devices.

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

  To Connect:
  1. Turn everything OFF (unless instructed otherwise)
  2. Attach all cables to devices.
  3. Attach signal cables to connectors.
  4. Attach power cords to outlet.
  5. Turn device ON.

  (D005)

Use the following instructions to help you cable your rack-mounted SDMC.

Attention: *Do not* plug the power cords into the electrical outlet until you are instructed to do so.
1. Ensure that you position the SDMC in the correct location.
2. Perform the following steps to install the cables on a rack-mounted SDMC:
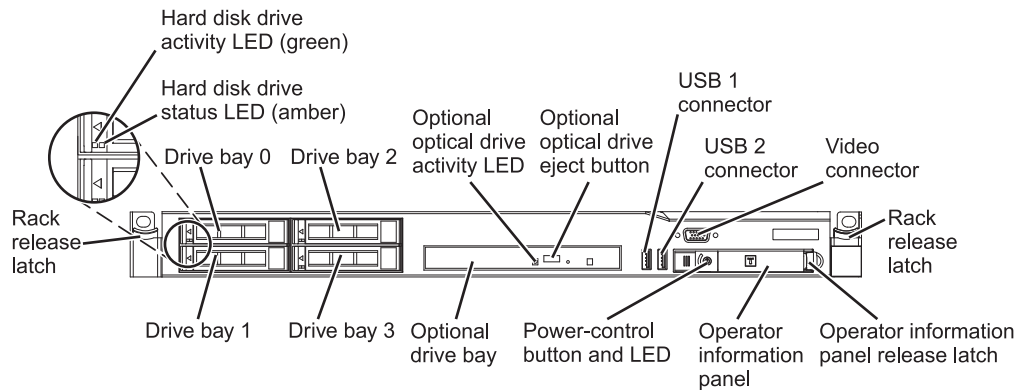   a. Use the following illustration to identify the location of the connectors described in these instructions:

Hard disk drive
activity LED (green)

Hard disk drive
status LED (amber)

Drive bay 0   Drive bay 2

Optional   Optional
optical drive optical drive
activity LED   eject button

USB 1
connector

USB 2   Video
connector   connector

Rack
release
latch

Rack
release
latch

Drive bay 1   Drive bay 3   Optional   Power-control   Operator   Operator information
                              drive bay   button and LED information   panel release latch
                                                             panel

P7EAV502-0

Figure 19. Back view of 7042-CR6 model

b. To install your SDMC into a rack, see the Installing and configuring the SDMC topic collection. When you are finished installing the SDMC into a rack, continue with the next step.

c. Connect the keyboard, display, and mouse using the USB conversion option cable.

3. Connect the Ethernet (or crossover) cable from the SDMC to the managed server.

   Note:

   - In general, connect your SDMC to the managed server in a private service DHCP network. If you have not installed any additional Ethernet adapters in the PCI slots on your SDMC, use the primary integrated Ethernet port. Use the previous illustrations to identify the location of the SDMC ports.

   - You can verify that the Ethernet cable connection is active by observing the green status lights at both the SDMC and server Ethernet ports while your installation progresses.

   - Connect the Ethernet port on the SDMC to the Ethernet port that is labeled **HMC1** on the managed server.

     If you are connecting a second SDMC to your managed server, connect to the Ethernet port that is labeled **HMC2** on the managed server.

4. Plug the power cords for the monitor and the SDMC into the electrical outlets.

   Note: Do not connect the server to a power source at this time.

5. If you are setting up the SDMC to manage an existing server, continue with Preparing for Systems Director Management Console configuration.

   Note: For a complete list of SDMC supported external cables, see the Serial attached SCSI cable planning topic.

Configuring the SDMC using the Guided Setup wizard

You must use the Guided Setup Wizard to configure your SDMC the first time you start the interface.

To configure your SDMC, do the following:
 1. Start the SDMC inferface.
 2. Click the **Console** tab.
 3. Select the locale.
 4. Accept the license agreement. The Welcome window opens.
 5. Set the date and time. Click **Next**.
 6. Set the passwords. Click **Next**.

    Note: Record these passwords. You might need them later.
 7. Create additional users. Click **Next**.
 8. Perform the following network configuration tasks:
    * Select an available LAN address
    * Select the network type
    * Configure the IP address
    * Configure the firewall settings
    * Configure a second LAN adapter (if applicable) and configure the network settings for this second network adapter
    * Configure the host and gateway

      Note: If you choose to not use a public network connection, provide default information in the short name and domain name fields.
    * Configure DNS
 9. Configure Agent Manager (for IBM Systems Director). Click **Next**.
10. Review the summary, then click **Finish**.
11. Click **Close**. Wait for all post-processing tasks to complete.
12. Next, complete any required postconfiguration tasks. For more information, see "Postconfiguration steps" on page 49.

Postconfiguration steps

After you have installed and configured the SDMC, back up SDMC data as necessary.

Setting up Electronic Service Agent

This topic describes how to set up Electronic Service Agent.

Electronic Service Agent can run on your host or on an SDMC. If Electronic Service Agent is installed and activated on your SDMC, the SDMC can monitor all the managed hosts. If a problem occurs and the application is enabled, Electronic Service Agent can report the problem to your service and support organization. If your host has virtual servers, Electronic Service Agent reports serviceable events and associated data to your service and support organization, either automatically or manually, under your authorization.

To set up and configure Electronic Service Agent, do the following:
1. From the Welcome page, click **Settings**,
2. Click **Support Manager Getting Started Wizard**.
3. Complete the steps in the wizard to set up and configure Electronic Service Agent.

Updating the SDMC

You can use the Update IBM Systems Director Management Console option to obtain and install updates for the SDMC.

To update the SDMC, complete the following steps:
1. Ensure that you have collected the latest inventory for the SDMC by clicking the **Inventory** → **View and Collect Inventory** in the IBM Systems Director application.
   a. On the View and Collect Inventory page, click **Browse**, and then click **Add** to add the selected target system in the Context Chooser window.
   b. Click **Collect Inventory**.
2. Use the **Import update** function to copy one or more updates from a directory on the management server to the update library. For more information, see "Importing host updates manually" on page 51.
3. To see a list of updates needed by a system and to install the updates, complete the following steps:
   a. From the Update Manager summary page, locate the Updates section.
   b. Click **Show needed updates**. The Show Needed Updates page is displayed.
   c. Select a system or system group in the Selected systems field. Click **Browse** to see a list of systems to choose from.
   d. Click **Show Needed Updates**. A table of needed updates is displayed.
   e. Examine the table. There is one line for each update and details about the update.

      Notes:
      - If you do not see an update that you expected to see, you can view all updates that are available for a system by selecting Show all available updates
      - Certain listed updates, for example UpdateXpress System Pack updates for a IBM BladeCenter blade server or chassis, are actually update collections that contain one or more member

updates that are combined into one installable image. To view the member updates within the update collection, right-click on the update collection and select "Update". For more information, see your product documentation.

   f. Select the updates that need to be installed and then click **Install**.

   g. Complete the steps in the install wizard to install the updates.

4. After installing the SDMC update, restart the SDMC. For more information, see Restarting the IBM Systems Director Management Console.

View available hosts

View the hosts that are available in your environment.

To view available hosts, do the following:

1. From the Welcome page, click the **Resources** tab. Your hosts are listed under Power Systems Resources if you set up the SDMC as a DHCP server-based private network.
2. If you do not see your hosts, from the Welcome page, click the **Resources** tab, then click **Common tasks** > **System Discovery**.

Request access to hosts

Request access to resources so that the SDMC can manage them.

To request access to managed systems, do the following:

1. From the Welcome page, click the **Resources** tab.
2. Click **No Access** next to a discovered system.

Checking and updating system firmware

Determine the firmware level on your host systems and update that firmware, if necessary.

Viewing and collecting inventory

You can view and collect inventory for the selected host by using the Systems Director Management Console (SDMC).

To view and collect inventory for the SDMC host, complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host for which you want to view and collect inventory.
3. Right-click and select **Inventory** → **View and Collect Inventory**.
4. Select the profile that you want to use for inventory collection from the **Manage Profiles** drop-down menu.
5. Click **Collect Inventory**.
6. Select **Run now** to start the inventory collection immediately, or select **Schedule** to start the inventory collection later.
7. Click **OK**.

Checking host updates

You can check and download the latest updates that are available for your environment and import the updates. By running a check for updates, new updates are loaded into the update manager.

This task contacts IBM Systems through an Internet connection and downloads information about the latest available updates. After updates are loaded, the update manager automatically compares this information to system inventories to determine whether your systems need updates.

To check for host updates by using the IBM Systems Director Management Console (SDMC), complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host for which you want to view updates.
3. Right-click and select **Release Management** → **Check for Updates**.
4. Select the update type from the **Available update types** list.
5. Click **Add** to add the selected update type in the **Selected** list.
6. Select **Run now** to check for updates immediately, or select **Schedule** to check for updates later.
7. Click **OK**.

Importing host updates

The updates for any IBM hardware managed by the Systems Director Management Console (SDMC) including IBM Power Systems servers and the SDMC appliance, can be downloaded from the IBM Fix Central website.

You can manually import host updates, or you can use File Transfer Protocol (FTP) to import them.

To download the updates from the IBM Fix Central website, go to Downloading and importing updates manually.

Notes:
- Run the following commands if you are importing host updates from a CD drive or a USB flash drive to get the path to import from:

  ```
  lsmediadev
  mount path_returned_from_lsmedadev
  ```
- Run the umount command after the import to unmount the path that was mounted.

Importing host updates manually

You can import updates that are available for the selected host by specifying the local directory path in the Systems Director Management Console (SDMC).

The updates can be manually downloaded or ordered on DVD media and then imported into the SDMC.

To import host updates by specifying a local directory path to the update files on the SDMC, complete the following steps:

1. Before importing the firmware updates, mount the media device (CD-ROM or USB) containing the firmware by completing the following steps:
   a. On the Welcome page, click the **Manage** tab.
   b. Select **Remote Access**, and then select **Remote Command Line**.
   c. In the Task Launch Dialog window, select the hostname of the SDMC, click **Add>**, and then click **OK**.
   d. Log in by using the sysadmin user ID and its password. The command-line interface (CLI) will be started.
   e. In the CLI, enter the lsmediadev command to list the installed media devices.
   f. Mount the media device by entering one of the following commands depending on the type of media:

      CD-ROM: `mount /media/cdrom`

USB: `mount /media/vdhX`, where X is the resource number that is displayed in the lsmediadev command.

2. Import the firmware updates by completing the following steps:

   a. On the Welcome page, click the **Manage** tab.

   b. Select **Update Manager**.

   c. Select **Import Updates** from the **Common tasks** list on the **Update Manager** page.

   d. Enter the directory path that contains the updates to be imported in the **Path** field. The directory path is the path of the media that you mounted in step 1 on page 51.

   e. Select **Run now** to import the updates immediately or select **Schedule** to import the updates later.

   f. Click **OK**.

   Note: After updating the firmware, unmount the media device by using the following command:

   CD-ROM: `umount /media/cdrom`

   USB: `unmount /media/vdhX`, where X is the resource number that is displayed in the lsmediadev command.

Importing system firmware updates by FTP

You can import system firmware updates by using File Transfer Protocol (FTP) by from the Systems Director Management Console (SDMC).

You require an active network connection to import host updates by FTP.

To import system firmware updates by using FTP from the SDMC, complete the following tasks:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host.
3. Right-click and select **Release Management** → **Import Updates by FTP**.
4. Enter the path on the remote server that contains the updates being imported in the **Path** field.
5. Enter the system host name or IP address in the **System hostname or IP** field.
6. Enter the user name in the **Username** field.
7. Enter the password in the **Password** field, if you are using a secure FTP.
8. Click **OK**.
9. Select **Run now** to import the updates immediately, or select **Schedule** to import the updates later.
10. Click **OK**.

Viewing and installing host updates

You can view and install the current updates that are needed for the selected host by using the Systems Director Management Console (SDMC).

To view and install the updates needed for the selected host, complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host for which you want to view and install needed updates.
3. Right click and select **Release Management** → **Show needed updates**.
4. Click **Show Needed Updates** to view the updates needed for the selected system.
5. Select the update, and select **Install** from the **Actions** drop-down menu.
6. Navigate through the installation wizard, select the target system, and click **Add** to add the target systems to the **Selected** list.
7. Click **Next** → **Finish**.

8. Select **Run now** to install the updates immediately, or select **Schedule** to install the updates later.
9. Click **OK**.

Moving to the SDMC

Transition is a new feature available to move systems from the HMC or IVM environment to the SDMC environment. This feature helps you to bring in one or more systems that are currently being managed by HMC or IVM to being managed by SDMC.

SDMC supports the following two types of transition:
- IVM to SDMC
- HMC to SDMC

You can use either the command line interface or the graphical user interface to perform an interactive transition or an offline transition. Use interactive transition when your HMC is running and offline transition when your HMC is shutdown. During transition, SDMC discovers the managed systems and you have to request access to each managed system by supplying the password. Transition is complete only after successful authentication to the managed system. The state of the managed system changes to Available and you can start managing your system and its virtual servers which gets reconstructed automatically.

The SDMC transition process does not remove the managed systems connection from the HMC. The managed systems stay connected to the HMC even after transition. You have to ensure that the maximum connections to the managed systems are not exhausted and there is a free connection available that SDMC can use during request access.

Upgrading from HMC to SDMC

Use this procedure to upgrade the Hardware Management Console (HMC) to the IBM Systems Director Management Console (SDMC). You should be able to complete the upgrade in less than two hours.

Prerequisites:
1. One hard disk drive (HDD)
2. Two dual inline memory modules (DIMMs)
3. Three *SDMC code* DVDs (The MES kit includes these DVDs)
4. Optional: DVD-R DVDs for backing up profile data on the existing HMC.

   Note:
   You can also back up the profile data to a file server that is accessible to the HMC or on a Universal Serial Bus (USB).
1. Back up the profile data on the existing HMC.
   a. Select the managed system from the **Contents** area.
   b. From the menu, select **Configuration > Manage Partition Data > Backup**.
   c. Type the name you want to use for the backup file.
   d. Click **OK**. Ensure that you save the backup data on an external drive.
2. Install the Dual Inline Memory Module (DIMM).
   a. Turn off the HMC and peripheral devices.

      Note: You can leave all the managed servers on.
   b. Slide the HMC into the service position.
   c. Disconnect the power cables.

Note: You can leave all other cables attached.

   d. Remove the service cover.

   e. Remove the memory air duct.

   f. Install DIMMs into connectors 2 and 9. (For more information, refer to the system service label located inside of the top service cover).

      Note: DIMM connectors 3 and 6 already have the DIMMs installed.

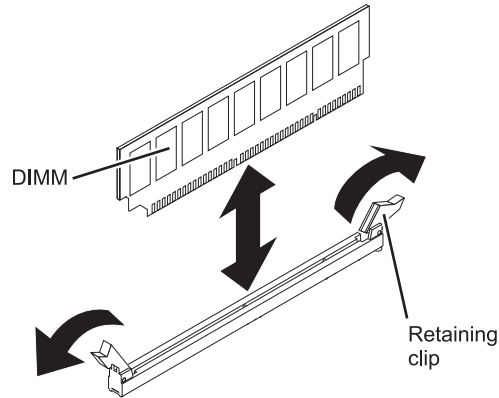   1) Open the retaining clips on each end of DIMM connectors 2 and 9.

Figure 20. Installing the DIMM

      2) Touch the static-protective package that contains the DIMM and touch any unpainted metal surface. Remove the DIMM from the package.

      3) Hold the DIMM and align the DIMM keys correctly with the connector.

      4) Insert the DIMM into the connector by aligning the edges of the DIMM with the slots at the ends of the DIMM connector.

      5) Firmly press the DIMM straight down into the connector by applying pressure on both ends of the DIMM simultaneously.

         The retaining clips snap into the locked position when the DIMM is firmly seated in the connector. If there is a gap between the DIMM and the retaining clips, the DIMM has not been correctly inserted. Open the retaining clips, remove the DIMM, and then reinsert it.

      6) Repeat steps 1) through 5) to install the second DIMM.

   g. Replace the memory air duct.

   h. Replace the service cover.

   i. Reconnect the power cables.

   j. Slide the HMC back into the rack.

3. Install the hard disk drive (HDD) as follows:
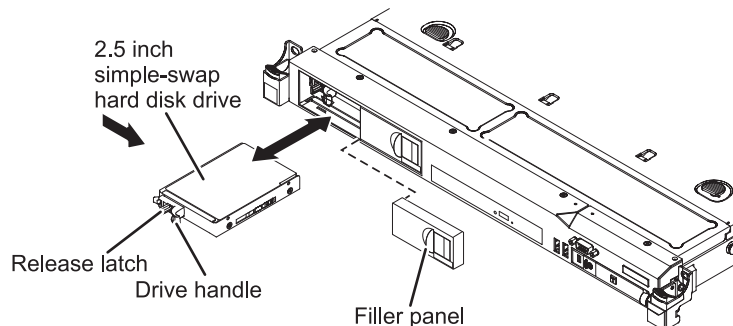
Figure 21. Installing the HDD

   a. Remove the bay filler from bay 1.

      Note: An HDD is already installed in bay 0.

   b. Touch the static-protective package that contains the HDD and touch any unpainted metal surface. Hold the HDD by the side edges and remove the HDD from the package.

   c. Hold the HDD by its side and press the terracotta release button to release the drive handle.

   d. Align the HDD with bay 1 and gently push the drive assembly into the bay until the drive stops.

   e. Close the handle on the HDD assembly to seat the drive until the handle is retained back into the release button.

4. Perform the following steps to configure RAID 0 for the Systems Director Management Console (SDMC):

   a. Power on the SDMC appliance.

   b. After the selection window is shown during the restart operation, press F1 to go to **Setup**.

   c. Select **System Settings**.

   d. Select **Adapters and UEFI Drivers**.

      Note: If the **Compile the List of Drivers** menu is shown, press **Enter**.

   e. Select **LSI Logic Fusion Adapter** in the **LSI Logic MPT Setup Utility** menu.

   f. Select **Create IS Volume**.

      Note: This step lists the two HDDs that are installed in the SDMC appliance. Check for the HDD listings and ensure that the two HDDs are correctly installed.

   g. Use the arrow keys to move to the **RAID DISK** column and press the space bar to toggle the value to **Yes**, for each HDD listed. Set the RAID DISK column value to **Yes**.

   h. Press **C** to create the RAID array.

   i. From the **Create and Save New Array** menu, Select **Save Changes**.

   j. Exit the menu and press **Enter**.

   k. Press **Esc** to exit **LSI MPT setup utility**.

   l. Press **Esc** to exit the previous menu.

   m. Select **Exit the Configuration Utility and Restart**.

   n. Enter **Yes**, when a prompt displays the message `The action required is stop controller`.

   o. Press **Esc** three times to exit setup.

   p. Press **Y** to exit setup completely.

5. Install the SDMC from the DVD media:

   a. Power on the SDMC appliance, and insert the first DVD disk into the DVD device.

   b. At the prompt, Select **Install SDMC**.

   c. After the system shutdown, power on the system and remove the first DVD.

   d. Insert the second and remaining DVDs, and press **Enter** when prompted.

   e. The system restarted and a wizard displays and prompts for locale information.

   f. When system displays the **License panels and Configuration** wizard, follow the wizard to configure SDMC.

   g. The SDMC appliance restarts, once the configuration is complete. You can access SDMC either locally by using the window manager or remotely by using a browser.

6. Download and install the updates for SDMC. For more information, see Updating the SDMC.

Moving from IVM to SDMC

The following information describes how you can transition a managed system from an IVM to an SDMC.

You have to perform the transition process manually for IVM to SDMC transition. You cannot use the transition wizard to transition managed systems from IVM to SDMC. The managed system has to be in an IVM Managed state. Once the transition is complete, you will not be able to use the IVM user interface as the Virtual Management Channel (VMC) is deactivated. The VMC is the device which exists on the VIOS to enable a direct Hypervisor configuration. This device is activated only when the VIOS detects that the environment has to be managed by IVM.

Note: When you transition managed systems from IVM to SDMC, only the following information are transitioned:

- Managed system information.
- Virtual server information is reconstructed from the managed system post successful request access to the managed system.

This transition will perform the following operations internally:

- Fetch the virtual server configuration information from the hypervisor.
- Update the SDMC with the managed system information restored from the hypervisor.
- The virtual slots range from 2 to 10 is reserved in SDMC. The IVM does not have such restrictions and it is possible that you were using some virtual slots in the reserved range in the IVM environment. The transition process looks for such virtual slots and dynamically adjusts the virtual slots range to a new available range within the maximum slots value specified.

  Note: If the automatic re-adjustment of reserved virtual slot range is unsuccessful, then you have to shutdown and activate the VIOS again to use the advanced PowerVM features. The shutdown and reboot will be needed only when you want to use the advanced PowerVM features. But the virtual servers will continue to run normally even without the shutdown and reboot.

- Create default profiles based on virtual server current configuration read from PHYP as IVM does not support profiles.

1. Discover the managed system in SDMC using the **System Discovery** page.
2. Request access to the managed system. The Request access task fails and the **Operating State** of your managed system changes to `Waiting for Input` and the **Detailed State** is `Pending Authentication - Password updates required`.
3. Update the ASM general and ASM admin passwords for the managed system using the **Update Password** task. The **Access** state of the system changes to OK and additional tasks are now available on the context menu of managing the system. The virtual servers hosted by the system get reconstructed and are listed on the **Welcome** page.

By default all success and failure messages are listed in the **Event Log** page. The **Event Log** page is available under **System Status and Health** category in the navigation area. Check the **Event Log** page for the success or failure of the transition process. When the transition completes successfully, the following message is posted on the **Event Log**.

When the IVM to SDMC transition completes successfully, you will see the appropriate Alert and the Resolution messages displayed in the Status Manager. The **Health and Summary** link under the **System Status and Health category** shows the messages in the Status Manager. An Alert message (error) is displayed first, followed by a Resolution event. The Alert event is removed when the Resolution event is logged in the Status Manager. The following table shows the **Alert** and **Resolution** events related to IVM to SDMC transition.

Table 42. Status Manager Alert (error) and Resolution messages

Alert	Resolution
VIOS Slot Range Adjustment Failed (Error)	The VIOS Slot adjustment did not complete successfully. You have to reactivate the VIOS virtual server before attempting LPM or AMS operations.
VIOS Reactivated & Slot Adjustment Completed Successfully. (Resolution)	The VIOS Slot Adjustment completed successfully.

Moving from HMC to SDMC

The following information describes several procedures on how to transition a managed system from an HMC to an SDMC from the GUI and command line using interactive or offline mode.

* Ensure that the HMC you are transitioning is version 7.1 or later.
* For interactive environment transition, ensure that you know the correct username, password, and the IP address/host name of the HMC.
* For interactive environment transition, ensure that you have the SSH access to the HMC.
* For offline environment transition, ensure that you export the HMC data before running the wizard.

The following data will be transitioned:

* List of managed systems along with their information such as MTMS name, IP address.
* Virtual server and profile information are not lost during transition and are reconstructed from the managed system after transition.

The following data will not be transitioned:

* Dump data, system and error logs stored on the HMC.
* Custom users and roles created on the HMC.

Note: The information in the following procedures only applies when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to the following information Transition in a private network .

Moving from HMC to SDMC using the graphical user interface

You can transition a managed system from HMC to SDMC interactively or non-interactively using the graphical user interface.

Moving from HMC to SDMC interactively using the graphical user interface.

SDMC provides you a wizard for interactive transition.

* Ensure that the HMC you are transitioning is version 7.1 or later.
* For interactive environment transition, ensure that you know the correct username, password, and the IP address/host name of the HMC.
* For interactive environment transition, ensure that you have the SSH access to the HMC.
* For offline environment transition, ensure that you export the HMC data before running the wizard.

The following data will be transitioned:

* List of managed systems along with their information such as MTMS name, IP address.
* Virtual server and profile information are not lost during transition and are reconstructed from the managed system after transition.

The following data will not be transitioned:

- Dump data, system and error logs stored on the HMC.
- Custom users and roles created on the HMC.

Note: The information in the following procedures only applies when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to the following information Transition in a private network .

Using the wizard, you can connect to a live HMC and stream in the configuration data directly from it.

1. Launch the Transition wizard from the Common Tasks pull-down in the SDMC welcome page as shown: (insert image here)
2. Click **Next** on the **Welcome** page of the transition wizard.
3. Select the option **Connect to the HMC to interactively transition to SDMC**. Enter the user name, password and the IP Address or host name of the HMC and click Next.
4. You should now see a list of managed systems that are available in the HMC that can be transitioned to your SDMC. Select the managed systems that you want to transition and click **Next**. If the SDMC is already managing some managed systems that are being managed by the HMC currently, those managed systems will not be listed for transition.
5. You should now see the summary page of the transition wizard. It shows you the IP Address or the host name of the HMC and the managed systems that you have selected for transition. Click **Finish** to complete the transition.
6. You can see the transitioned managed systems in the **Welcome** page in the No Access state. Request access to the managed system. The user ID field in the **Request Access** page will be pre-populated and disabled. You only need to enter the password.

After successful authentication, the **Access** state of the managed system changes to OK. The tasks for managing the system are now available on the context menu of the system. And the virtual servers hosted by the managed system gets retrieved automatically and can be seen in the **Welcome** page or the **Navigate Resources** page.

Moving from HMC to SDMC non-interactively using the graphical user interface.

The following information describes how you can transition a managed system from an HMC to an SDMC in offline mode using the GUI.

- Ensure that the HMC you are transitioning is version 7.1 or later.
- For interactive environment transition, ensure that you know the correct username, password, and the IP address/host name of the HMC.
- For interactive environment transition, ensure that you have the SSH access to the HMC.
- For offline environment transition, ensure that you export the HMC data before running the wizard.

The following data will be transitioned:

- List of managed systems along with their information such as MTMS name, IP address.
- Virtual server and profile information are not lost during transition and are reconstructed from the managed system after transition.

The following data will not be transitioned:

- Dump data, system and error logs stored on the HMC.
- Custom users and roles created on the HMC.

Note: The information in the following procedures only applies when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to the following information Transition in a private network .

Perform the following procedure to transition a managed system from HMC to SDMC.

1. Execute the expdata command with the option given below on the HMC: expdata -f <file>

    file   The name of the file where the HMC configuration data is to be written on the HMC. If file is not fully qualified, file will be written to the /dump/expdata directory on the HMC.

    If the file already exists, this command will fail unless the --force option is specified. To export the data to removable media, the media must be present in the removable media device and the device must be mounted with the mount command before you issue this command.

    All serviceable events must be closed before you can execute this command. If there are any open serviceable events at the time of issuing this command, you will get a warning message and you have to close all of them before executing the command again.

    Note: The expdata command only exports HMC configuration information that is required for transition. The exported data cannot be used as HMC backup data.

2. Launch the transition wizard. Note that the export is run on the HMC, and the wizard is launched on the SDMC. The SDMC imports the data from the HMC export.

3. Click on Next to go to the Transition Method page in the wizard.

4. Select the option **Use an exported data file** in the **Transition Method** page.

5. Browse to select the exported configuration data file from step 1 as shown. You can also select a file that is available on a connected system in the network. Click **Next**.

6. You should now see the summary page of the transition wizard. It shows you the IP Address or the host name of the HMC and the managed systems that you have selected for transition. Click Finish to complete the transition.

7. You can see the transitioned managed systems in the welcome page in the `No Access` state. Request access to the managed system.The user ID field in the Request Access page will be pre-populated and disabled. You only need to enter the password.

After successful authentication, you can start managing the system. The virtual servers hosted by the managed system get retrieved automatically.

Moving from HMC to SDMC using the command line interface.

You can transition a managed system from HMC to SDMC either interactively or on-interactively using the command line interface.

Moving from HMC to SDMC interactively using the command line interface.

The following information describes how you can transition a managed system from an HMC to an SDMC using interactive mode from the command line interface.

- Ensure that the HMC you are transitioning is version 7.1 or later.
- For interactive environment transition, ensure that you know the correct username, password, and the IP address/host name of the HMC.
- For interactive environment transition, ensure that you have the SSH access to the HMC.
- For offline environment transition, ensure that you export the HMC data before running the wizard.

The following data will be transitioned:

- List of managed systems along with their information such as MTMS name, IP address.
- Virtual server and profile information are not lost during transition and are reconstructed from the managed system after transition.

The following data will not be transitioned:

- Dump data, system and error logs stored on the HMC.
- Custom users and roles created on the HMC.

Note: The information in the following procedures only applies when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to the following information Transition in a private network .

Perform the following steps to transition a managed system from HMC to SDMC.

1. Execute the impdata command with the options given below on the SDMC: smcli impdata -h <system_name> -u <user>

   system_name
   > host name or IP address of the remote HMC to import configuration data

   user   name of the remote HMC

2. Enter the name of the remote HMC user

3. Enter the password for the name of the remote HMC user when prompted. SDMC identifies the managed systems to transition and discovers them.

4. The transitioned systems are in the No Access state. Request access to the managed systems using the accesssys command.

After successful authentication, you can start managing the system with the tasks available on the context menu of the system and the virtual servers hosted by the managed system get retrieved automatically.

Moving from HMC to SDMC non-interactively using the command line interface.

The following information describes how you can transition a managed system from an HMC to an SDMC in offline mode using the command line interface.

- Ensure that the HMC you are transitioning is version 7.1 or later.
- For interactive environment transition, ensure that you know the correct username, password, and the IP address/host name of the HMC.
- For interactive environment transition, ensure that you have the SSH access to the HMC.
- For offline environment transition, ensure that you export the HMC data before running the wizard.

The following data will be transitioned:

- List of managed systems along with their information such as MTMS name, IP address.
- Virtual server and profile information are not lost during transition and are reconstructed from the managed system after transition.

The following data will not be transitioned:

- Dump data, system and error logs stored on the HMC.
- Custom users and roles created on the HMC.

Note: The information in the following procedures only applies when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to the following information Transition in a private network .

Perform the following procedure to transition a managed system from HMC to SDMC.

1. Execute the expdata command with the option given below on the HMC: expdata -f <file>

2. Execute the impdata command with the options given below in the SDMC: smcli impdata -f file

   file   The name of the file containing the HMC configuration data imported from your HMC in step 1.

   This will carry out a discovery process of the managed systems that are eligible for transition from your HMC. The managed systems gets discovered by the SDMC and will be in No Access state.

3. Request access to the managed systems using the accesssys command: smcli accesssys <managed system name>
4. Enter the user ID and password for the managed system when prompted.

After successful authentication, you can start managing the system. The virtual servers hosted by the managed system get retrieved automatically.

Moving from HMC to SDMC in a private network

Describes how to perform transition of managed systems which are in the private network. In this scenario, either the SDMC or the HMC can be the DHCP server. The steps for transitioning when the SDMC is the DHCP server is different from the steps when the HMC is the DHCP server.

SDMC as the DHCP server

Follow the steps given below to perform a transition of managed systems in the private network with the SDMC as the DHCP server:

1. Disconnect the HMC from the private network.
2. Connect the SDMC to the private network.
3. Configure the network interface of the SDMC with the correct DHCP range. The IP addresses of the managed systems may change after renewal of the DHCP leases from the SDMC. SDMC then auto-discovers the managed systems.
4. Request access to the managed systems.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The virtual servers hosted by the managed system get retrieved automatically.

HMC as the DHCP server - method 1

When the existing HMCs are currently the DHCP servers and SDMC will replace one HMC as the DHCP server on the same DHCP range used by the HMC, you have two methods of transitioning systems.

he following steps perform a transition of managed systems using the first method:

1. Connect the SDMC to the HMC2 port of the managed system. Leave the other HMC connected to the HMC1 port of the managed system. Now, the HMC is the DHCP server for the managed systems on the network to which the HMC1 port is connected. The SDMC will be the DHCP server for those systems on the network to which the HMC2 port is connected, replacing the other HMC that used to perform this function.
2. Configure the network interface with the same DHCP range as the HMC that used to be attached to the HMC2 of the managed system. The IP addresses of the managed systems may change after renewal of the DHCP leases from the SDMC. SDMC then auto-discovers the managed systems.
3. Request access to the managed systems.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The virtual servers hosted by the managed system get retrieved automatically.

HMC as the DHCP server - method 2

The following are the steps to perform a transition of managed systems using the second method:

1. Connect the SDMC to the private network.
2. Configure the SDMC to be a DHCP client of the HMC.
3. Discover the HMC managed system using the IP address or the host name of the managed system.

4. Request access to the managed system.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The virtual servers hosted by the managed system get retrieved automatically. Since the resulting environment will remain dependent on the HMC to be the DHCP server and hinder complete transition to an SDMC-only setup, this should only be used as a temporary solution.

Configuring high availability

A high availability environment minimizes your enterprise's downtime.

To set up a high availability environment, you will configure two Systems Director Management Consoles (SDMCs) to be kept in close synchronization. These consoles are then considered nodes in a high availability cluster. One node in the environment is kept active at all times. If your active node fails, the passive node takes over in about 10 minutes. You must be assigned to the SMAdministrator role to configure high availability.

Note: If you are using IPv6, the discovery process must be done manually. For Internet Protocol version 6 (IPv6), there is no automatic discovery.

Consider an example of a redundant SDMC environment with two managed systems. The first SDMC is connected to the first port on each flexible service processor (FSP), and the redundant SDMC is connected to the second port on each SDMC. Each SDMC is configured as a Dynamic Host Configuration Protocol (DHCP) server, using a different range of IP addresses. The connections are on separate private networks. As such, it is important to ensure that an FSP port is connected to only one SDMC.

Each managed system's FSP port that is connected to an SDMC requires a unique IP address. To ensure that each FSP has a unique IP address, use the SDMC's built-in DHCP server capability. When the FSP detects the active network link, it issues a broadcast request to locate a DHCP server. When correctly configured, the SDMC responds to that request by allocating one of a selected range of addresses.

If you have multiple FSPs, you must have your own LAN switch or hub for the SDMC-to-FSP private network. Alternatively, this private segment can exist as several ports in a private virtual LAN (VLAN) on a larger managed switch. If you have multiple private VLANs, you must ensure that they are isolated and that there is no crossover traffic.

If you have more than one SDMC, you must also connect each SDMC to the virtual server and to each other on the same open network.

Assume that two SDMCs connected to a single managed server on a private network and to three virtual servers on a public network. You can have an additional Ethernet adapter for the SDMC to have three network interfaces. You can use this third network as a management network or connect it to the Cluster Systems Manager (CSM) Management Server.

To configure a high availability cluster in your environment, complete the following steps. You must be assigned to the SMAdministrator role to configure high availability. After completing the wizard, configuration will take 20 - 60 minutes.

1. On the **Welcome** page, select the **Settings** tab.
2. Click **High availability setting** → **Set Up High Availability**.

   Note: If you do not see the **Set Up High Availability** button, high availability is already configured.
3. Complete the wizard as directed.
4. After configuration, use the floating IP address to connect to the IBM Systems Director server on the primary node.

Notices

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED "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. The manufacturer 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 websites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this product and use of those websites is at your own risk.

The manufacturer 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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

67

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.

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

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer's computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the manufacturer's support websites for updated information and fixes applicable to the system and related software.

Ethernet connection usage restriction

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

Trademarks

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER7® processor and its features unless designated as electromagnetic compatibility (EMC) Class B in the feature information.

Federal Communications Commission (FCC) statement

Note: 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, may 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 may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Community Compliance Statement

This product is in conformity with the protection requirements of 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.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M456
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2937
email: tjahn@de.ibm.com

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

VCCI Statement - Japan

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

The following is a summary of the VCCI Japanese statement in the box above:

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) 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

Electromagnetic Interference (EMI) Statement - People's Republic of China

声　　明
此为 A 级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

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。

The following is a summary of the EMI Taiwan statement above.

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

IBM Taiwan Contact Information:

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

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

Germany Compliance Statement

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 von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich
Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene
Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

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

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

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

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15-2937
email: tjahn@de.ibm.com

Generelle Informationen:

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

Electromagnetic Interference (EMI) Statement - Russia

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

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC)
Class B in the feature installation information.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a Class B digital device,
pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against
harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

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

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of 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.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M456
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15-2937
email: tjahn@de.ibm.com

VCCI Statement - Japan

この装置は，クラスB情報技術装置です。この装置は，家庭環境で使用
することを目的としていますが，この装置がラジオやテレビジョン受信機に
近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　　　VCCI－B

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

IBM Taiwan Contact Information

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

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 가정용(B급)으로 전자파적합기기로
서 주로 가정에서 사용하는 것을 목적으로 하
며, 모든 지역에서 사용할 수 있습니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B 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 B 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 von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

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 B

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 M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15-2937
email: tjahn@de.ibm.com

Generelle Informationen:

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THESE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.