

Managing Hosts using the SDMC

ESCALA Power7



REFERENCE
86 A1 09FH 01

ESCALA Power7

Managing Hosts using 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

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 09FH 01

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 2011

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

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

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Contents

Discovering and managing hosts	1
Adding hosts to the SDMC	1
Discovering hosts.	1
Requesting access.	1
Changing host properties	2
Managing host operations	2
Powering on the host	2
Powering off the host	2
Performing power management operations	2
Activating and deactivating the attention LED	3
Locating parts with the identify LED	3
Performing an LED lamp test.	3
Scheduling host operations	4
Launching Advanced System Management	5
Changing the sampling rate for utilization data.	5
Viewing host utilization data	5
Rebuilding a managed system	6
Changing host passwords	6
Managing host connections	7
Changing host connection information.	7
Requesting, revoking, and resetting host connections	7
Requesting connection access	7
Revoking connection access	7
Resetting a management console connection	7
Discovering and requesting access to a host	8
Discovering a system	8
Requesting access to a host	8
Managing hardware	8
Viewing a host Ethernet adapter.	8
Viewing a host channel adapter	9
Viewing hardware topology	9
Managing host updates.	9
Updating the host	9
Viewing and collecting inventory	10
Checking host updates	10
Importing host updates	10
Importing host updates manually	11
Importing system firmware updates by FTP	11
Viewing and installing host updates	12
Managing Power system firmware.	12
Managing POWER blades	13
Discovering and managing POWER blades with the advanced management module	13
Notices	15
Trademarks	16
Terms and conditions	16

Discovering and managing hosts

Managed hosts (formerly known as managed systems or servers) can be discovered and multiple life-cycle management operations can be performed by using the IBM® Systems Director Management Console (SDMC).

Discovery is the process by which the IBM Systems Director identifies and establishes connections with the network-level resources that the SDMC can manage. You can use system discovery or advanced system discovery to identify resources within your environment, to collect data about the resources, and to establish connections with the resources. The SDMC uses the Service Location Protocol (SLP) for discovering resources in the network. The SDMC supports the discovery of hosts, power units, and operating systems.

You must request access to a host to which your SDMC has not yet authenticated. Ensure that you have the correct authorization to access the host.

You can manage a host only after you discover the host and request access to the host. After a host has been discovered, the host is displayed under **Hosts** on the **Resources** tab of the Welcome page. The hosts are also listed on the **Navigate Resources** page.

Adding hosts to the SDMC

To add hosts to the IBM Systems Director Management Console (SDMC), you must discover hosts and then request access to the hosts.

Discovering hosts

To discover hosts, complete the following steps:

1. On the SDMC navigation pane, expand **Inventory** and click **System Discovery**.
2. Select a discovery option from the **Select a discovery option** drop-down menu.
3. Enter the IP address in the **IP address** field.
4. Select the resource type from the **Select the resource type to discover** drop-down menu.
5. Click **Discover Now** to discover hosts immediately, or click **Schedule** to discover hosts later.

The discovered resources are displayed in the **Discovered Manageable Systems** table. The **Discovered Manageable Systems** table displays only the manageable resources that are discovered during the current discovery. System discovery discovers only systems and other types of resources that can be managed by SDMC.

Requesting access

The discovered systems are listed on the **Resources** tab of the **Welcome** page and the **Navigate Resources** page with an access state of Unknown. The access state changes to No Access, you can perform a Request Access State task on the discovered host.

To request access, go to “Requesting connection access” on page 7

When the request access is successful, the access state of the system changes to OK, which means you have access to the host. After you access a host, additional tasks for managing the system are available.

Changing host properties

You can use the IBM Systems Director Management Console (SDMC) to view and change the properties of a host, such as processor, memory, I/O, migration, power-on parameters, and capabilities.

To change the host properties, complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and click the host for which you want to change the properties.
3. Right-click and select **System Configuration** → **Edit Host**. This action launches the **Edit Host** page.

Managing host operations

You can use the IBM Systems Director Management Console (SDMC) to perform host operations.

You can perform the following actions on hosts by using the SDMC:

- Edit host configuration
- Power on and power off the host
- Perform power management operations
- Activate and deactivate the attention LED
- View the current identity LED
- Perform LED lamp test
- Schedule host operations
- Launch Advanced System Management (ASM)
- View and change the sampling rate of host utilization data
- Rebuild a managed system
- Change host passwords

Powering on the host

You can use the IBM Systems Director Management Console (SDMC) to power on the host.

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

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and click the host you want to power on.
3. Right click and select **Operations** → **Power On**.
4. Click **OK**.

Powering off the host

You can use the IBM Systems Director Management Console (SDMC) to power off the host. Powering off the host makes all the virtual servers unavailable until the host is powered on.

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

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and click the host you want to power off.
3. Right click and select **Operations** → **Power Off**. You can select to perform a normal power off, or a fast power off on the **Power off options** page.
4. Click **OK**.

Performing power management operations

You can enable the power saver mode on the host to reduce the power consumption of the processors.

Important: Enabling the power saver mode on a host might affect the accuracy of performance monitoring tools that are running on the host.

To configure the power management settings for a 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 configure the power management settings.
3. Right-click the host and select **Operations** → **Power Management**.
4. From the **Desired Power Server Mode** drop-down list, select **Enabled**.
5. Click **OK**.

Note: Changes to the power saver mode take effect immediately, without requiring a restart of the host system.

Activating and deactivating the attention LED

You can view system attention LED information, light specific LEDs to identify a system component, and test all LEDs on a managed system. The system provides several LEDs that help you to identify various components, such as enclosures or field replaceable units (FRUs), in the system. Hence, they are called identify LEDs.

To activate or deactivate the system attention LED by using the IBM Systems Director Management Console (SDMC), complete the following tasks:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host on which you want to activate and deactivate the attention LED.
3. Right click and select **Service and Support** → **Hardware** → **System Attention LED**.
4. Click **OK** to continue with activation or deactivation of the **System Attention LED**.

Locating parts with the identify LED

You can view the current identify LED states for all the location codes that are contained in the selected enclosure.

To locate parts with the identify LED by using the Systems Director Management Console (SDMC), complete the following tasks:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host for which you want to view the current Identify LED.
3. Right click and select **Service and Support** → **Hardware** → **Identify LED**.
4. Click **OK** to continue with deactivation of the **System Attention LED**.
5. Select an enclosure from the table and either operate against its identify LED or display the selected enclosure's FRUs and operate against those identify LEDs.

Performing an LED lamp test

You can perform an LED lamp test against the selected system. All LEDs are activated for several minutes.

To perform an LED lamp test against the selected system by using the Systems Director Management Console (SDMC), complete the following tasks:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host on which you want to perform an LED lamp test.
3. Right click and select **Service and Support** → **Hardware** → **LED Lamp Test**.
4. Click **OK** to initiate the LED lamp test against the selected system.

Scheduling host operations

You can schedule operations for the host when automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance.

Perform the following steps to create schedules for operations:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts**, and select the host for which you want to create scheduled operations.
3. Right-click the host, and select **Operations** → **Schedule Operations**.
4. From the **Operations** drop-down list, select the operation that you want to schedule. The possible operations that can be scheduled are:
 - Activate system profile
 - Backup profile data
 - Power off
 - Power on
 - Manage utility CoD
 - Modify power saver mode
5. Click **OK**.
6. Specify the required details for the selected operation as shown in the table below.

Option	Description
Operation	Required detail
Activate System Profile	The system profile to activate
Backup Profile Data	The name of a backup file
Power Off	the type of power-off operation. The possible options are: <ul style="list-style-type: none">• Normal Power Off• Fast Power Off
Power On	The type of power-on operation. The possible options are: <ul style="list-style-type: none">• Normal• Hardware Discovery <p>Note: If you are scheduling a system profile power on operation, select the system profile to use.</p>
Manage Utility CoD	The following details: <ul style="list-style-type: none">• Number of utility CoD processors• Processor usage limit
Modify Power Saver Mode	Enable or disable power saver mode for the host

7. Click **OK**.
8. In the **Task Launch Dialog** window, specify the details of the schedule as shown in the table below.

Option	Description
Schedule	Select: <ul style="list-style-type: none">• Run now to run the operation immediately.• Schedule to run the operation at the specified date and time, and at the required frequency.

Option	Description
Notification	Specify the following details: <ul style="list-style-type: none"> • The progress of the operation when you want to receive the notification. Select the required check box. • The email address at which you want to receive the notification. • The name of the email server. • The port number for the email server.
Options	Specify the following details: <ul style="list-style-type: none"> • The system time according to which the scheduled operation is to run. You can select the management server time or your local system time. • The action to be taken for unavailable systems. • The maximum job instances in history.

9. Click **OK** to save the schedule.

Launching Advanced System Management

The Systems Director Management Console (SDMC) can connect directly to the Advanced System Management (ASM) interface for a selected system. ASM is an interface to the service processor that allows you to manage the operation of the host, such as the automatic power restart function, and to view information about the host, such as the error log and vital product data.

To launch ASM by using the SDMC, complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host on which you want to launch ASM.
3. Right-click and select **Operations** → **Launch Advanced System Management (ASM)**.
4. Select the service processor IP address from the **Service Processor IP Address** drop-down menu.
5. Click **OK** to launch ASM.

Changing the sampling rate for utilization data

You can set the Systems Director Management Console (SDMC) to collect resource utilization data for a specific host that the SDMC manages.

Use this task to enable, set, and change the sampling rate, or disable sampling collection.

To change the sampling rate for utilization data by using the SDMC, complete the following tasks:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host for which you want to change the sampling rate.
3. Right click and select **Operations** → **Utilization Data** → **Change Sampling Rate**.
4. Select the sampling rate from the **Sampling rate** drop-down menu.
5. Click **OK** to change the sampling rate for utilization data.

Viewing host utilization data

The Systems Director Management Console (SDMC) collects utilization data for memory and processor resources. You can use this data to analyze trends and make resource adjustments. The data is collected into records called events.

Events are created at the following times:

- At periodic intervals (30 seconds, 1 minute, 5 minutes, 30 minutes, hourly, daily, and monthly).

- When you make host-level state and configuration changes that affect resource utilization.
- When you start, shut down, and change the local time on the SDMC.

You must set the SDMC to collect resource utilization data for a specific host or several hosts that the SDMC manages before utilization data can be displayed for the host.

To view the host utilization data by using the 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 the utilization data.
3. Right click and select **Operations** → **Utilization Data** → **View Utilization Data**.
4. Select **Snapshot** or **Hourly** or **Daily** or **Monthly**.
5. Enter the beginning time and date in the **Beginning Time** and **Date** fields.
6. Enter the ending time and date in the **Ending Time** and **Date** fields.
7. Select the event type from the **Event type** drop-down menu.
8. Click **Show** to view the host utilization data.

Rebuilding a managed system

You can extract the configuration information from the managed system and rebuild the information about the Systems Director Management Console (SDMC). Rebuilding the managed system updates the information about the SDMC managed systems. This task does not disrupt the operation of the running host. Rebuilding the managed system is useful when the state of the managed system is Incomplete. The Incomplete state means that the SDMC cannot gather complete information from the managed system about virtual servers, profiles, or resources. You cannot start other tasks while the SDMC rebuilds the managed system. This process can take several minutes.

To rebuild a managed system by using the SDMC, complete the following steps:

1. On the Welcome page, click the **Resources** tab.
2. Expand **Hosts** and select the host.
3. Right click and select **Operations** → **Rebuild Managed System**.
4. Click **Yes** to rebuild the managed system. The process of rebuilding the managed system starts immediately. No other tasks can be performed while rebuilding the managed system.

Changing host passwords

You can change the IBM Systems Director Management Console (SDMC) access password on the selected managed system. After the password is changed, you must update the SDMC access password for all other SDMCs from which you want to access this managed system.

To change the host password by using the 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 change the password.
3. Right click and select **Operations** → **Change Password**.
4. Enter your current password in the **Current System Access password** field.
5. Enter your new password in the **System Access password** field.
6. Enter your new password in the **Verify System Access password** field to verify your new password.
7. Click **OK** to change the password.

Managing host connections

You can view and change the host connection information, request connection access, revoke connection access, reset a management console connection, and discover and request access to another host by using the Systems Director Management Console (SDMC).

Changing host connection information

You can change the host connection information by using the Systems Director Management Console (SDMC).

To change the host connection information, 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 change the connection information.
3. Right click and select **System Configuration** → **Edit Host**.
4. Under the **General** tab, select the service virtual server from the **Service virtual server** field.
5. Select the **Power off the system** check box if you want to power off the system after all the virtual servers are powered off.
6. Click the **Processors, Memory, I/O, Migration, Power-On Parameters, Capabilities, and Advanced** tabs, and enter the required details.
7. Click **OK** to activate the changes.

Requesting, revoking, and resetting host connections

You can request host connection access, revoke host connection access, reset a management console connection, and discover and request access to another host through the Systems Director Management Console (SDMC).

Requesting connection access

You can request connection access to a target system by using the Systems Director Management Console (SDMC).

To request the connection access, 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 request connection access.
3. Right click and select **Security** → **Request Access**.
4. Enter your password in the **Password** field.
5. Click **Request Access** to grant all authorized IBM Systems Director users access to the target system.

Revoking connection access

You can revoke host connection access by using the Systems Director Management Console (SDMC).

To revoke the host connection access, 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 revoke connection access.
3. Right-click and select **Security** → **Revoke Access**.
4. Click **OK** when you are prompted to revoke access.

Resetting a management console connection

You can reset a management console connection by using the Systems Director Management Console (SDMC). Management consoles are connected to the host.

Resetting a management console connection resets the connection between the selected console and the host. After the task is performed, the disconnected console attempts to reconnect to the system. If the disconnected console has a lock on the system, this task forces the release of the lock so other tasks can be performed from this console.

Note: This task is recommended for advanced users only.

To reset a management console connection, complete the following tasks:

1. On the **Welcome** page, click the **Resources** tab.
2. Expand **Hosts** and select the host on which you want to reset the management console connection.
3. Right click and select **Service and Support** → **Reset Other Management Console Connection**.
4. Select a management console from the table, and click **OK**.

Discovering and requesting access to a host

You can discover and request access to a host by using the Systems Director Management Console (SDMC).

Discovering a system:

Use system discovery to discover manageable resources now or schedule your discovery to run later. You can discover a resource for a single IP address or host name, discover resources of the same type for a range of IP addresses, or use a discovery profile. Discovery profiles enable you to customize discoveries, including importing IP addresses, requesting access to discovered resources, and collecting inventory for the discovered resources.

To discover a system, complete the following steps:

1. On the Welcome page, click the **Manage** tab.
2. Select **System Discovery** from the **Common Tasks** drop-down menu.
3. Select a discovery option from the **Select a discovery option** drop-down menu.
4. Enter IP address in the **IP address** field.
5. Select the resource type from the **Select the resource type to discover** drop-down menu.
6. Click **Discover Now** to discover the system immediately, or click **Schedule** to schedule your discovery to run later.

Requesting access to a host:

To request access to a host, go to “Requesting connection access” on page 7:

Managing hardware

You can view Host Ethernet Adapters (HEA), Host Channel Adapters (HCA), and the Remote I/O (RIO) topology using the hardware tasks of the Systems Director Management Console (SDMC).

Viewing a host Ethernet adapter

A Host Ethernet Adapter (HEA) allows multiple virtual servers to share a single physical Ethernet adapter.

You can view a list of the HEAs for the managed system. You can select an HEA from a list to display the current virtual server use for the HEA.

To view an HEA, 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 the HEA.

3. Right click and select **Hardware Information** → **Adapter** → **Host Ethernet**.
4. Select an HEA from the table to display the current virtual server use of the adapter.

Viewing a host channel adapter

A host channel adapter (HCA) provides a managed system with port connections to other devices. The port can be connected to another HCA, to a target device, or to a switch that redirects the data coming in on one of its ports out to a device that is attached to another of its ports.

You can view a list of the HCAs for the managed system. You can select an HCA from a list to display the current virtual server use for the HCA.

To view an HCA, 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 the HCA.
3. Right click and select **Hardware Information** → **Adapter** → **Host Channel**.
4. Select an HCA from the table to display the current virtual server use of the adapter.

Viewing hardware topology

You can view the current hardware topology for the selected managed system and any discrepancies between the current topology and the last valid topology.

High-speed link (HSL), also known as remote I/O (RIO), resources provide the connection between system I/O busses and the system processor. HSL/RIO resources are normally configured in loops with the system unit having an HSL/RIO controller resource that handles routing of the data between the system processor and the system I/O busses. System I/O busses connect to the loop with HSL I/O adapter resources or with RIO adapter resources.

To view the current hardware topology and the last valid hardware topology, 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 the hardware topology.
3. Right-click and select **Hardware Information** → **View Hardware Topology**.
4. Click **Save** to save the topology details.

Managing host updates

Use the *Update Manager* in Systems Director Management Console (SDMC) to do update, installation, and maintenance operations in the SDMC managed system environment.

Updating the host

You can perform all the update operations from the *update manager* page of the Systems Director Management Console (SDMC). Alternatively, you can do individual update operations from the **Action** drop-down menu on the **Resources** page of the SDMC.

The update manager compares information about the updates loaded into it with system inventories to determine whether updates are needed. If an Internet connection is available, the update manager can automatically discover information about available updates. Alternatively, you can manually import the update information.

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

The updating process for the host includes the following tasks:

1. “Viewing and collecting inventory”
2. “Checking host updates”
3. “Importing host updates”
4. “Viewing and installing host updates” on page 12

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_lsmediadev
```

- 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.
 - 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: umount /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**.

Managing Power system firmware

Use this task to manage firmware on Power systems.

1. On the **Welcome** page, under the **Resources** tab, select the server.
2. Click **Actions** > **Release Management** > **Power Firmware Management**.
3. i
4. Click **Gather Target Info** to gather the target information, which populates the table with selected target system information.

Note: The **Readiness** state of the system must show **Passed** in order to proceed with firmware management operations.

5. Click **Action** and select the operation you want to perform.

Note: When the target information is gathered, available operations are **Accept/Reject**, **Disruptive Activate**, **Synchronize**, **Remove and Activate**, and **Set Next IPL Side**. The availability of the **Accept** menu option is side-dependent, for example, if the P-side of the flexible service processor (FSP) is active, **Accept** is not available (likewise, if T-side is active, **Reject** is not available).

6. Click **Start** (the operation you want to perform)**Task**.
7. On the **Task Launch** dialog box, run the selected operation now or schedule it to run at a later time. Click **OK** to run the task now and the **Active and Scheduled Jobs** page shows task progress. Status is shown as **Complete** when the task is successfully run.

Managing POWER blades

A POWER® blade can be managed in the same way that a rack-mounted Power Systems server is managed from a Systems Director Management Console (SDMC). That is, the blade server gets managed directly through the Flexible Service Processor (FSP).

By default, the FSP is not available on the network. You must enable the advanced management module (AMM) and ensure that you have the latest AMM firmware and blade firmware. Select **Blade Tasks** → **Configuration** → **Management Network Configuration**. Enable the FSP on your network.

Note: Ensure that you remove all objects associated with the blade, including the Virtual I/O Server (VIOS) operating system object, all the virtual server objects, and the server objects from the SDMC.

To discover a blade server and request access to it, complete the following steps:

1. On the SDMC navigation pane, expand **Inventory** and select **System Discovery**.
2. Enter the IP address or the host name of the blade server, and select the resource type as **Server**. The discovery process discovers the blade server as a **Server**.
3. Request access to the blade server with correct credentials.

The blade server is now connected to the SDMC and is listed in the **Resources** tab on the Welcome page. The model type and serial number of the server indicates that it is a blade server. You can perform all management tasks on the blade server.

Discovering and managing POWER blades with the advanced management module

Advanced management module (AMM) is a management console that provides system management functions and keyboard/video/mouse (KVM) switching for all the blade servers in an IBM BladeCenter® chassis that supports KVM. The Systems Director Management Console (SDMC) can also manage the blade servers that are connected to an AMM.

To discover and manage POWER blades by using the AMM, complete the following steps:

1. On the SDMC navigation pane, expand **Inventory** and select **System Discovery**.
2. Select a discovery option from the **Select a discovery option** drop-down menu.
3. Enter the IP address in the **IP address** field.
4. Select the resource type from the **Select the resource type to discover** drop-down menu to discover the **AMM**.
5. Request access to the **AMM** by using the credentials for AMM. The blade servers that are managed by the AMM are now listed as servers on the **Navigate Resources** page.

The blade servers that are discovered directly and the blade servers that are discovered through an AMM can co-exist in the SDMC environment. SDMC can manage both of these blade servers at the same time.

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.

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

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the

same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning 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.

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

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

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

Trademarks

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

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

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.

