ESCALA POWER5

Hardware Information

Solution planning

REFERENCE
86 A1 06EW 00

BLANK

ESCALA POWER5

Hardware Information

Solution planning

Hardware

July 2006

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

REFERENCE
86 A1 06EW 00

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

Table of Contents

Solution planning

Solution planning is the process of verifying that all your server equipment meets or exceeds the operational requirements of your solution. Before installing the hardware, software, and other equipment needed to run your hardware solution, consult this information to create a plan.

Each of the following topics can help you develop your plan. The topics are intended to be used in a modular way. You can develop sub-plans for each topic and plug them into the appropriate place in your overall plan as your solution demands.

At the end of your solution planning, plan to meet the following requirements:

- Create a plan for a solution that meets your current and future business needs.
- Create a plan for a solution that is physically and operationally set up to perform the tasks, and to respond in a way that you expect.
- Know your responsibilities and have a list of tasks associated with these responsibilities. This could include tasks that a service provider can work with you on (for a fee).
- Understand the importance of carefully documenting a plan with all of its details.
- Understand the importance of communicating plan details, especially physical configuration requirements and plans, with your installers, such as electricians and movers.
- Understand the importance of, and your responsibility for, evaluating and testing the solution, such that the solution is considered fully operational. This occurs after installation, configuration, setup, and functional setup are completed. Testing ensures that the solution performs according to your plans and expectations.

- **What's new**
  See what is new and what has changed in Solution planning since the last edition of this topic.
- **Printable PDF**
  See this information to print the entire Solution planning topic collection.
- **Planning for software**
  The success of your solution will depend on the applications running on your server and on its clients. Your software plan needs to include the operating systems you want to load on your server and how you want to integrate them, and the software that you want in order to facilitate your solution.
- **Planning for consoles, interfaces, and terminals**
  Managing the connection to your server and related systems requires a critical piece of preparation. This information helps you understand your console, interface, and terminal options and plan accordingly.
- **Planning for logical partitions**
  Server hardware architectures allow you to create logical partitions to distribute resources within a single server, and make it function as if it were two or more independent servers. Before creating logical partitions, you will need to plan for several variables specific to your solution. It is especially important to understand how you can reconfigure partitions to respond to future needs.
- **Planning for workloads**
  Planning for workloads involves planning for capacity, including sizing, and planning for performance and availability. Workload planning tools differ according to the operating systems you run on your servers. This topic collection offers capacity and performance planning checklists for each supported operating system.
- **Planning for availability**
  To minimize downtime and maximize availability, you need to prepare for hardware failures, power outages, server transitions, and disaster recovery.
- **Planning for service processor failover**
  The ESCALA PL 850R/PL 1650R/R+ models support redundant service processor configurations that allow you to plan for dynamic failover. It is important to understand the considerations and requirements for a redundant service processor configuration to prepare for enabling the failover capability.
- **Planning for networking communications**
  How you configure your server to connect servers and other systems through local area networks, wide area networks, and to the Internet requires careful planning before successful implementation.
- **Planning for InfiniBand Networks**
  Learn about clustering systems using InfiniBand (IB) hardware.
- **Planning for hardware**
  Before installation, you will need to ensure that you have all the required upgrade hardware. You will also need to plan for power, environmental needs, and server placement. Finally, you need to prepare for unique configurations based on how you plan to use the server, including data storage and cabling.

- **Planning for service and support**
  Understanding the different functions and features of your service environment can help you prevent server problems. Understanding the applications that you can use to provide those functions can help you plan for regular preventive maintenance.
- **Planning for testing**
  Testing can help validate that your new system is functioning as planned. Based on your system requirements and needs, your test can range from covering the basics to an in-depth analysis.

What's new

See what is new and what has changed in Solution planning since the last edition of this topic.

Planning for logical partitions
: This section contains updates to the logical partition planning tasks. The updates discuss working with a system plan to deploy partitions.

Planning for service processor failover
: This new section discusses how to plan for service processor failover in your systems.

Planning for consoles, interfaces, and terminals
: This topic has been updated.

Planning for an Enterprise Storage Server environment
: This topic has been revised to include information about a new boot option for ESS servers.

Planning for performance with AIX
: This topic has been revised to include information about planning for huge page memory support.

Parent topic: Solution planning

Printable PDF

See this information to print the entire Solution planning topic collection.

To view or download the PDF version of this document, select Solution planning (about 1,787 KB).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link to the PDF file in the preceding paragraph).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you would like to save the PDF.
4. Click Save.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html).

Parent topic: Solution planning

Planning for software

The success of your solution will depend on the applications running on your server and on its clients. Your software plan needs to include the operating systems you want to load on your server and how you want to integrate them, and the software that you want in order to facilitate your solution.

Software planning is perhaps the most critical aspect of solutions planning. It is important to know which applications best fit your solution, and under which operating systems those applications run. server hardware and server hardware allows you to run multiple operating systems on multiple partitions on the same server. This enables you to run the best applications in each class without concern for the operating systems under which they run. But it also increases the complexity of your solution, which makes software planning all the

more important. Follow this planning guide to help ensure that your operating systems and applications work together.

- **Planning for operating systems**

Parent topic: Solution planning

Planning for operating systems

Installing or upgrading an operating system requires careful planning. This topic collection guides you through installation planning if your operating system is AIX, or Linux

- **Planning for AIX**
- **Planning for Linux**

Parent topic: Planning for software

Planning for AIX

Before you install your AIX operating system on your server, perform a number of recommended planning tasks. Follow the checklist to obtain the detailed information that you need to complete the planning tasks for your operating system. Before you begin your planning tasks, complete the items in the checklists that follow.

Before you begin

__ Read the AIX Release Notes.

AIX planning tasks

__ Evaluate your current and future server configuration

Know where your operating system currently resides on your server and whether that should change according to the needs of your business.

__ Understand performance issues

The size and location of the disk on which you select to install AIX can affect the performance of your system. For more information about the impact of your choice of

boot disk on your system's performance, including tuning, performance monitoring, and diagnosis, see the Performance Management Guide.

__ Determine the type of installation

Decide which type of installation, including new and complete overwrite, migration, or preservation, is correct for your situation. See How-To's for AIX Installation Tasks in the AIX installation guide for more information.

__ Identify how the partitions will communicate with the HMC

If you plan to run AIX partitions, this information can help ensure that your partitions are communicating with the HMC. For more information about setting up and communicating with the HMC, see Setting up the HMC.

__ **Ensure that your system meets all requirements to run AIX**

An installation of AIX requires a minimum amount of memory and physical disk space. The installation might also require that hardware units

be turned on or configured, and that network information be readily available. For more information about prerequisites for your AIX installation, see the installation guide.

__ Configure virtual I/O

If you want to use virtual I/O with your AIX partition you must first install and configure a virtual I/O server partition. See Installing the Virtual I/O Server. For more information about using the Virtual I/O Server, see Using the Virtual I/O Server.

Parent topic: Planning for operating systems

Planning for Linux

Before you install your Linux operating system on your server, use this checklist to obtain the detailed information that you need to complete the planning tasks for your operating system.

If you need more information to help you decide whether or not to partition, see the list of topics under Partitioning for Linux with an HMC.

Before you begin

__ If you are planning to upgrade an existing server, document your current environment.

__ If you are migrating from another operating system to Linux, document your migration path.

Linux planning tasks

__ **Identify the hardware requirements for your Linux system**

The server hardware and

server hardware systems require a Linux for POWER distribution, that is, Linux distributions designed to run on POWER technology-based systems. For information, see the Linux on Power Web site.

__ **Identify installation media (CD or Network)**

__ Identify the Linux distribution (for example, SUSE Linux Enterprise Server or Red Hat Enterprise Linux) and the release to be installed

For information, see the Linux on Power Web site.

After you finish

__ Identify and record the hardware requirements for your solution.

__ Identify and record the appropriate Linux distribution for your solution.

__ Ensure that the hardware requirements for your configuration have been met.

__ Record a complete hardware feature placement plan, which includes your post installation strategy for moving features to match your configuration.

Parent topic: Planning for operating systems

Planning for consoles, interfaces, and terminals

Managing the connection to your server and related systems requires a critical piece of preparation. This information helps you understand your console, interface, and terminal options and plan accordingly.

You can communicate with your server and the other systems in your environment in many ways. The appropriate console interface, and terminal solution enables you to manage system resources in the most efficient and effective way. This topic describes prerequisites, features, and scenarios for each console, interface, and terminal. The purpose of this topic is to help you determine the best console, interface or terminal choice for your solution and to direct you to the resources that you need to implement those choices.

Adequate console, interface, and terminal planning also ensures that you have the necessary access for service and support personnel. Consoles, interfaces, and terminals need to be carefully configured and placed in order to give service providers access to important service functions. For more information on the configuration and placement of consoles, interfaces, and terminals for service and support purposes, see the Planning for consoles, interfaces, and terminals for your service environment topic.

When you are finished planning for your consoles, interfaces, and terminals, see Managing consoles, interfaces, and terminals.

- **Types of consoles, interfaces, and terminals**
- **Solutions with the Hardware Management Console (HMC)**
- **Solutions without the HMC**
- **Planning for consoles, interfaces, and terminals for your service environment**

Parent topic: Solution planning

Types of consoles, interfaces, and terminals

Depending on your server model and business environment, you have several console, interface, and terminal options. Some options are required by the model; others are optional. In some cases you can integrate multiple consoles, interfaces, and terminals. Read these topics to understand your options and decide which options to investigate further through subsequent research in this topic collection.

- **The Advanced System Management Interface**
- **The Hardware Management Console**
- **o/p interfaces and terminals**

Parent topic: Planning for consoles, interfaces, and terminals

The Advanced System Management Interface

The Advanced System Management Interface (ASMI) is the interface to the service processor that is required to perform general and administrator-level service tasks, such as reading service processor error logs, reading vital product data, setting up the service processor, and controlling system power. The ASMI also might be referred to as the service processor menus.

- You can access the ASMI through a Web browser, an ASCII terminal, or the Hardware Management Console (HMC).
- The ASMI provides an interface to service processor functions, such as remote power-on and other system management functions.
- The ASMI can be used for some system management functions for nonpartitioned servers that are not managed by an HMC and can also be used with HMC-managed systems.
- The ASMI is designed to complement other consoles specifically for service functions like remote power management and error log access.
- The ASMI is the required interface to the service processor on all servers server models.
-

For more information on accessing the ASMI, see Managing the ASMI. For more information on the functions that are available on the ASMI, see Managing your server using the ASMI.

Parent topic: Types of consoles, interfaces, and terminals

The Hardware Management Console

The Hardware Management Console (HMC) is a system that controls managed systems, including the management of logical partitions and the use of Power On Demand. Using service applications, the HMC also communicates with managed systems to detect, consolidate, and send information to your systems integrator for analysis.

Considerations for choosing the HMC:

- The HMC is the only console that enables you to configure server partitions.
- The HMC can control multiple partitions without needing a separate connection and adapter for each partition.
- A version of the HMC also can be used in server models with pre-POWER5 processors. However, previous versions of the HMC are not compatible with the version used to manage POWER5 servers. So you cannot manage pre-POWER5 servers and POWER5 servers with the same HMC.
- You must use an HMC to manage your servers if you plan to create or reconfigure logical partitions, or to enable Power On Demand.

- You also can use the HMC in conjunction with other consoles, interfaces, or terminals for specific management needs.
- You must use an HMC if you plan to manage your InfiniBand network using the Network Manager.
- You must use an HMC to perform concurrent maintenance tasks on systems that support part replacement and feature upgrades without server downtime.
- You must use an HMC to enable your system for service processor failover on systems equipped with redundant service processors.

For more information on the HMC, see Solutions with the Hardware Management Console (HMC).

Parent topic: Types of consoles, interfaces, and terminals

o/p interfaces and terminals

In addition to the Hardware Management Console (HMC) and the Advanced System Management Interface (ASMI), additional terminals and interfaces can be used to manage the systems in your data center. Use these topics to find out if you need additional interfaces and terminals for your solution.

- **ASCII terminal**
- **Graphics terminal**
- **System Management Services menus**
- **Virtual terminal**

Parent topic: Types of consoles, interfaces, and terminals

ASCII terminal

The ASCII terminal is the original servers terminal; the ASCII terminal is connected to the server using a serial link. It can be used with or without an HMC. The ASCII interface to the ASMI provides a subset of the ASMI functions that are available using the Web interface, and the ASCII interface is only available when the server is in the platform standby state. The ASCII interface to the ASMI is not available during initial program load or runtime. See Accessing the ASMI using an ASCII console for more information on the ASCII terminal.

Note that the ASMI can also be accessed using a web browser. For information, see Accessing the ASMI using a Web Browser. Both of the ASMI topics can be found in the Managing the Advanced System Management Interface (ASMI) topic.

Parent topic: o/p interfaces and terminals

Graphics terminal

The graphics terminal is available to servers customers who want to use a graphical user interface to their AIX or Linux servers. Users plug the graphics adapter into a PCI slot in the back of the server. Customers connect a standard monitor, keyboard, and mouse to use the terminal. It is primarily used for specialized applications, including animation programs and product lifecycle management solutions such as CATIA. The graphics terminal can be used with or without an HMC.

Parent topic: o/p interfaces and terminals

System Management Services menus

System Management Services (SMS) menus provide access to low-level functions through the firmware console on servers servers. Linux and AIX servers customers must use the SMS menus to specify from which device or Network Information Management (NIM) server to install the operating system on the system or logical partition.

After the operating system is installed, the SMS menus can be used to change the boot sequence. You can do this if you want to boot a diagnostic CD instead of the operating system, or if you want to try booting another hard disk drive with a different version of the operating system, for example. For some models on which the ASMI is not supported, additional options are available on the SMS menus. See Using the system management services for additional information.

The console that is used to access the SMS menus is usually referred to as the firmware console. On a system that is managed by a Hardware Management Console (HMC), the firmware console is usually a virtual terminal on the HMC. On a system that is not managed by an HMC, the firmware console can be a graphics terminal attached to a graphics adapter, or an ASCII terminal attached to one of the system ports on the server.

The SMS menus are not related to the Advanced System Management Interface (ASMI), to the operating system, or to configuring partitions on the HMC. For more information on the SMS menus, see the Using the system management services topic.

Parent topic: o/p interfaces and terminals

Virtual terminal

The virtual terminal is used for some system management functions on servers servers running AIX or Linux. The virtual terminal is an HMC function that emulates a standard terminal window. It can be used locally from the HMC console, or from Web-based system manager remote clients.

See Virtually accessing AIX or Linux using the virtual terminal for more information on the virtual terminal.

Parent topic: o/p interfaces and terminals

Solutions with the Hardware Management Console (HMC)

The HMC is a system that controls managed systems, including the management of logical partitions and the use of Power On Demand. Using service applications, the HMC also communicates with managed systems to detect, consolidate, and send information to your systems integrator for analysis.

See this information to determine if the HMC is the right choice for your solution.

- **HMC capabilities**
- **HMC specifications**
- **HMC requirements and benefits**
- **HMC configurations**
- **Scenarios: HMC for servers servers**

Parent topic: Planning for consoles, interfaces, and terminals

HMC capabilities

The HMC is a system management appliance. For the purposes of stability and security, the HMC is a closed system; that is, no other software can be loaded on it. When powered on and connected to the server through its dedicated Ethernet port, the graphical user interface gives the administrator control over all hardware resources, including all partitions and capacity settings.

The Ethernet port connects the HMC to the service processor, which enables you to perform various service functions.

The HMC's primary functions include the following:

- Remote power management enables you to power on and off your server remotely through the HMC's user interface.

- Logical partition (LPAR) configuration allows you to manage partition resources as your business changes.
- Service focal point provides error routing, error analysis, and error reporting to your systems integrator.
- Power On Demand enables you to activate additional unused resources as your business changes.
- Virtual terminal support allows you to manage your systems using the virtual ASCII terminal.
- Concurrent maintenance enables you to perform concurrent maintenance tasks on models that allow for feature upgrades without server downtime.

See Implementations of HMCs for more information on what you can do with the HMC.

Parent topic: Solutions with the Hardware Management Console (HMC)

HMC specifications

The Hardware Management Console (HMC) is available in two forms, a desktop version and a rack-mounted version. See these specification sheets to help you determine which model is right for your solution.

- Desktop Hardware Management Console
- Rack-Mounted Hardware Management Console

Parent topic: Solutions with the Hardware Management Console (HMC)

HMC requirements and benefits

Some solutions require the use of the Hardware Management Console (HMC). Other solutions might not require the HMC, but the HMC might still help you manage your solution more effectively. Use this information to help you determine if the HMC is the best choice for your solution.

When the HMC is required

The HMC is required for:

- All systems running multiple logical partitions.
- All systems that come in 24-inch racks with bulk power assemblies.
- All systems with redundant (active/standby) service processors.
- servers, o/p and server clusters with CSM hardware controls that are in 24-inch rack systems.
- Systems connected in an InfiniBand switch network with GX 4x/12x IB HCA adapters that you plan to manage using the Network Manager.

When the HMC is beneficial

Logical Partitioning

Logical partitioning enables you to consolidate multiple workloads into one server. For example, if you have 10x86 Linux servers in your data center, you can assign a logical partition on your POWER5 server for each Linux server and migrate all your Linux workloads into your POWER5 system.

LPAR also enables you to consolidate workloads from multiple operating systems into one server. By logically isolating the operating system and its associated workload to one partition, you can ensure that its availability and performance are unaffected by other workloads, while saving overall system and administrative costs.

For servers, server and o/p, the Integrated Virtualization Manager will provide similar basic logical partitioning capability without an HMC.

Note: The Virtual Partition Manager and Integrated Virtualization Manager offerings only provide a subset of the HMC's LPAR management function and flexibility, so you may still benefit from the additional capability of the HMC.

Centralized Hardware Management

One HMC can manage up to 32 systems. This number is expected to increase in subsequent releases.

Note: You will need a separate Ethernet switch to connect more than one server to an HMC. Switches are preferred over hubs.

The HMC provides a graphical interface to control servers, including powering up and down, and setting up and managing partitions running on the managed servers. On AIX or Linux partitions, this is accomplished through the HMC graphical user interface (GUI) and through the virtual terminal. The following tasks can be managed through the HMC GUI:

- ◊ Adding and removing managed systems.
- ◊ Authentication: The HMC gives you control over the passwords required to access the HMC and the managed systems connected to the HMC.
- ◊ Managed system properties: The HMC enables you to view or change system properties of managed systems. You can view general system properties (system type, system model, serial number, and capabilities), power-on properties, processor, I/O, and memory information (current usage), and system reference codes. You can change the managed system's name or power-off policy.
- ◊ Partition management: The HMC enables you to manage partition resources with its GUI.
- ◊ Remote scripting capability: The HMC provides you with a set of commands that can be used to build scripts to manage your managed systems.

See Working with the HMC for more information on configuring and using the HMC to manage your systems.

Managing Power On Demand

You can use the HMC to activate unused processor and memory resources as your business grows. The HMC provides full support for managing all Power On Demand (POD) and Function on Demand (FoD) capabilities. These functions ensure that you have the processor and memory capacity that you need when you need it, either on a regular growth curve or on a seasonal basis. By allowing you to pay for only the capacity that you need, it improves your cost/performance ratio.

See the Planning for Power On Demand topic for more information on how to order and configure Power On Demand.

Advanced Service Functions

The Service Focal Point (SFP) functions* are only available with an HMC. These advanced service functions include:

- ◊ Service event collection
- ◊ Platform dump collection
- ◊ Call home
- ◊ SNMP traps
- ◊ Guided/concurrent repair procedures

The HMC also supports concurrent firmware maintenance, which allows you to apply fixes to your system firmware without any disruption to the operation of the system and partitions.

* The Integrated Virtualization Manager also contains a limited subset of SFP functions, but they only apply to the system on which the Virtual I/O Server is running.

Redundant and remote system management

You can integrate multiple HMCs into one data center. In some cases, one HMC can manage multiple systems. In other cases, two or more HMCs can manage one system. In still other cases, multiple consoles and interfaces can manage systems remotely using the HMC as a gateway device.

See Redundant HMCs for more information on redundant HMC configurations. See Remote HMCs and clients for more information on remote HMC configurations.

Security

For a number of reasons, the HMC is a more secure console option than many available for your system. First, a reliable security system is built into the machine code. Second, it is tied to specific PC hardware and is not supported or functional on vendor PCs. This guarantees that the HMC includes all the security hardware and software that your systems integrator includes. Finally, the HMC is closed and dedicated, which means users are not able to install their own software onto an HMC. For all these reasons, the HMC is a highly secure console.

See Working with users, roles, and passwords for more information on HMC security.

Parent topic: Solutions with the Hardware Management Console (HMC)

HMC configurations

You can connect multiple administrators in a variety of ways. Learn more about how to connect multiple administrators in your distributed environment.

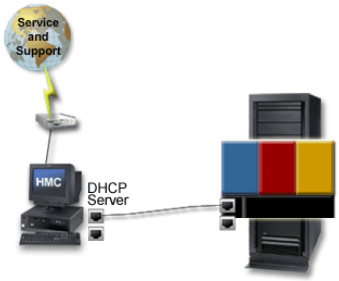
- **Local HMC with ASMI and SMS**
- **Redundant HMCs**
- **Remote HMCs and clients**

Parent topic: Solutions with the Hardware Management Console (HMC)

Local HMC with ASMI and SMS

A local Hardware Management Console (HMC) is directly connected to the server it manages using a private network. The HMC can launch the Advanced System Management Interface (ASMI) using a Web browser. The HMC can display the System Management Services (SMS) menus using the virtual terminal.

Figure 1. A local HMC connection



Parent topic: HMC configurations

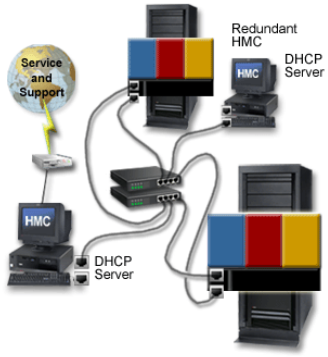
Redundant HMCs

Multiple Hardware Management Consoles (HMCs) can manage one server. When there are two or more HMCs managing one system, the HMCs are peers. To set up a redundant HMC, follow the instructions in Setting up an HMC.

In a DHCP environment, both HMCs must be configured as DHCP servers, and the HMCs must be on separate subnets. For instructions about setting up a DHCP server, see Configuring the HMC as a DHCP server. In a redundant HMC environment, configure only one HMC for service and support.

The following figure depicts a redundant HMC configuration in a DHCP environment. In this configuration, both HMCs are connected to the server using private networks.

Figure 1. Redundant HMC connections

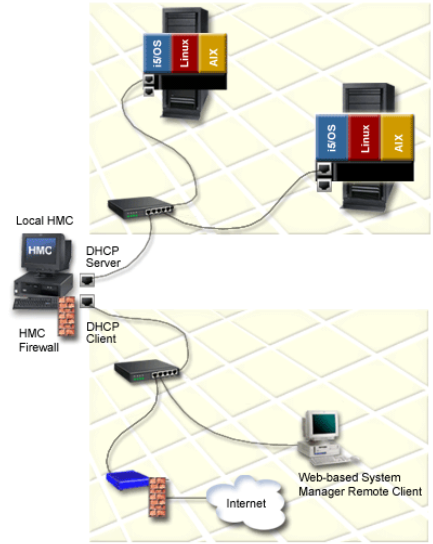


Parent topic: HMC configurations

Remote HMCs and clients

The local HMC needs to be configured to allow remote access because, in the default settings, remote access is disabled. The local HMC can also enable remote access with other types of clients. You can configure the HMC as a Web-based System Manager Remote Server, with clients accessing the HMC's server through the Web-based System Manager Remote Client. The HMC can also provide remote secure shell access for command-line and script-based management.

Figure 1. Remote HMC connections



- **Remote secure shell access for UNIX and Linux**

Parent topic: HMC configurations

Remote secure shell access for UNIX and Linux

The Hardware Management Console (HMC) allows Linux and AIX users to run commands and scripts through remote secure shell access to the managed system. This is useful if you need consistent results and you need to automate the administration of managed systems. You can accomplish consistency by storing the command sequence in scripts and running them remotely. You can automate management by calling the

scripts from batch-processing applications from the remote systems.

See Scenario: HMC with remote UNIX secure shell access for more information on this configuration on AIX systems.

Parent topic: Remote HMCs and clients

Scenarios: HMC for servers servers

Learn more about how users integrated the Hardware Management Console (HMC) into distributed servers server environments with other consoles, interfaces, and terminals.

- **Scenario: HMC with remote UNIX secure shell access**
- **Scenario: HMC and graphics with ASCII terminals in an integrated environment**

Parent topic: Solutions with the Hardware Management Console (HMC)

Scenario: HMC with remote UNIX secure shell access

Customer has multiple remote administrators

In this scenario, the user has a large data center of servers with multiple administrators. Rather than forcing the administrators to go to the data center every time they want to manage the systems, the administrators can access the Hardware Management Console (HMC) and manage their systems remotely. The remote administrators enter a user ID and password to access the HMC. This shell access is restricted to a set of commands that can be used to manage the HMC and the servers managed by the HMC. The user can also use the remote scripting capability of SSH to run scripts on a local system that issues HMC management commands to the HMC, thus giving the user access to a full range of commands on the managed systems.

For more information on using the HMC remote command line and setting up secure script execution between SSH clients, refer to Using the HMC remote command line.

Parent topic: Scenarios: HMC for servers servers

Scenario: HMC and graphics with ASCII terminals in an integrated environment

Multiple servers server models of various ages

The user has an existing data center running servers servers and continues to add servers to the data center as the business grows. The user connects to the older servers using ASCII terminals and graphics terminals, and to server servers through the Hardware Management Console (HMC).

Parent topic: Scenarios: HMC for servers servers

Solutions without the HMC

Although choosing not to use the Hardware Management Console (HMC) limits your ability to flexibly handle business changes, you may choose not to use the HMC. Read the topics relevant to your server families to understand your console, interface, and terminal options outside of the HMC.

- **server and server AIX or Linux**

Parent topic: Planning for consoles, interfaces, and terminals

server and server AIX or Linux

For server and server AIX or Linux models, you have several console, interface and terminal options outside of the Hardware Management Console (HMC). Refer to o/p interfaces and terminals for details.

Parent topic: Solutions without the HMC

Planning for consoles, interfaces, and terminals for your service environment

During service activity, it is likely that the service provider will need to use one or more of the following: a Hardware Management Console (HMC), a system console, or a PC capable of connecting to the Advanced System Management Interface (ASMI). Take the following actions in preparation for the service provider:

1. Provide a supported HMC, a system console, a PC capable of connecting to the ASMI, or any appropriate combination that is capable of accessing the ASMI connected to the service processor over Ethernet.
2. Load and configure all current, supported software and software fixes.
3. Locate the consoles in the same room and within 8 meters (26 feet) of the system being serviced.
4. Make sure the devices are connected to the system, operational, and communicating with the service processor prior to the service representative's arrival.

Failure to meet the requirements stated above will result in delays to service providers. These delays may be billable at current hourly rates.

Parent topic: Planning for consoles, interfaces, and terminals

Planning for logical partitions

Server hardware architectures allow you to create logical partitions to distribute resources within a single server, and make it function as if it were two or more independent servers. Before creating logical partitions, you will need to plan for several variables specific to your solution. It is especially important to understand how you can reconfigure partitions to respond to future needs.

Creating logical partitions on your server enables you to integrate multiple operating systems and consolidate several servers into one. Consolidation helps you reduce maintenance and administration costs while improving performance. Planning for logical partitions is a multistep process. This topic directs you to the recommended tasks for logical partition (LPAR) planning for AIX and Linux logical partitions.

See this checklist for information about preparing to partition your server. Before you begin your planning tasks, be sure you have completed the items in the following checklist.

Before you begin

__ Learn about available tools

The available tools include:

Hardware Management Console
: Managing your server using the Hardware Management Console
The Hardware Management Console (HMC) is a system that controls managed systems, including server hardware, logical partitions, and Power On Demand.

Integrated Virtualization Manager
: Partitioning with Integrated Virtualization Manager
Integrated Virtualization Manager is a browser-based system management interface that you can use to manage a single managed system that uses Virtual I/O Server on a managed partition.

Virtual I/O Server

Using the Virtual I/O Server
The Virtual I/O Server is an appliance that resides in a POWER5 logical partition that facilitates the sharing of physical I/O resources between AIX and Linux client logical partitions within the server.

__ Check prerequisites

Use the following resources to check prerequisites:

- Hardware resources

Logical partition planning tasks

__ Take inventory of your current environment, and what is available through Power On Demand

Refer to Working with Power On Demand.

__ Perform capacity planning

Determine the number of partitions needed and the size of each.

__ Identify the console you will use to interact with the server and its operating systems

Refer to the topic Console options for logical partitions to help you determine which console helps you to connect and communicate with the server and your operating systems.

__ Determine how the partitions will communicate with other partitions, servers, or workstations

Refer to the topic Communications options for logical partitions to help

you select the communication option you prefer to use for your logical partition. Determine which communication option allows you to communicate with other partitions, servers, and workstations.

__ Identify how the partitions will communicate with the HMC

Refer to Hardware Management Console (HMC) topic to help you determine how you will implement a network connection on the HMC.

__ Determine a service and support strategy

Refer to service, support, and troubleshooting to understand how your server will communicate to your service provider if you have hardware or software errors. Determine how you will apply fixes to your server and how you will identify problems that need to be reported to your service provider.

__ Decide if you want your operating systems to share I/O resources with each other

Refer to Using the Virtual I/O Server to understand how your OS can provide I/O resources to other logical partitions.

__ Plan for software licensing in a partitioned

environment Use the following information to understand how many software licenses you might need depending on your logical partition configuration. Software licensing considerations for Power BackUP	

Parent topic: Solution planning

Planning for workloads

Planning for workloads involves planning for capacity, including sizing, and planning for performance and availability. Workload planning tools differ according to the operating systems you run on your servers. This topic collection offers capacity and performance planning checklists for each supported operating system.

- **Planning for capacity**
  Planning for capacity is related to several other planning actions, including sizing, planning for performance, and availability. By calculating your initial capacity needs and projecting future business activity, you can improve your server performance and availability while minimizing costs. Many of the capacity planning tools and the steps you take can also be used to capture performance and availability data. Capacity planning tools differ according to the operating systems you run on your servers. This topic collection offers capacity planning checklists for each supported operating system.
- **Planning for performance**
  Effective performance management requires thorough planning to ensure that you have the necessary server resources for your business needs. By ensuring that you are prepared for business contingencies, effective planning also reduces the time involved in managing your system performance when you need to add resources.

Parent topic: Solution planning

Planning for capacity

Planning for capacity is related to several other planning actions, including sizing, planning for performance, and availability. By calculating your initial capacity needs and projecting future business activity, you can improve your server performance and availability while minimizing costs. Many of the capacity planning tools and the steps you take can also be used to capture performance and availability data. Capacity planning tools differ according to the operating systems you run on your servers. This topic collection offers capacity planning checklists for each supported operating system.

Regardless of operating environment, your capacity planning might include planning for Power On Demand. Power On Demand allows you to purchase a server with excess capacity and only pay for the capacity you need. You can activate the standby processors or memory units temporarily or permanently as your business grows or on a seasonal basis. If you build Power On Demand into your capacity plan, you will ensure that you have the capacity you need when you need it.

See the following information to plan for capacity on your servers:

- **Planning for capacity with AIX**
- **Planning for capacity with Linux**

Parent topic: Planning for workloads

Planning for capacity with AIX

Capacity planning for AIX involves using several tools that are also used for performance management and system accounting. Some of these tools are built-in AIX commands and others are supplemental tools such as the Performance Toobox. Still other tools help you plan to add Power On Demand. This topic enables you to develop a plan that includes all these elements in the proper order.

Before you begin your AIX capacity planning, you need to answer the following questions:

Before you begin

__ Which type and size of database will your company use?
__ What other software applications are involved?
__ How many users will use these applications?
__ How much data will the server handle?
__ What are the inputs and outputs for the data?
__ What are your company's future growth plans both in the short and long terms?

Capacity planning tasks

__ **Use AIX commands to establish a current workload estimate**

The first step in determining your capacity needs is to capture data about existing workloads using standard AIX commands. Several commands within AIX can help you quantify various aspects of server usage. They include:

iostat
The **iostat** command generates quick reports that you can use to determine if there is an imbalanced I/O load

between physical disks and adapters. It also reports on CPU usage.

ipcs
: The **ipcs** command reports status information about active interprocess communication (IPC) facilities.

ps
: The **ps** command monitors memory usage between processors and partitions.

sar
: The **sar** command gathers data about system performance.

svmon
: The **svmon** command captures a current view of virtual memory usage.

topas
: The **topas** command enables you to perform broad-spectrum performance analysis.

vmstat
: The **vmstat** command reports statistics about kernel

threads in the run queue and wait queue, memory, paging, disks, interrupts, system calls, context switches, and CPU activity.

__ Use the Performance Toolbox to gather additional workload data

The purpose of the Performance Toolbox is to collect and graphically display data from various systems in your current configuration. The Performance Toolbox can give you a better understanding of how all your systems work together than screens of ASCII numbers generated by AIX commands. For more information on using the performance toolbox to determine current workloads, see the Performance Toolbox Version 2 and 3 Guide and Reference topic.

__ **Optimize current usage with AIX workload manager**

After you have a good picture of how your systems are being used, you can deploy the AIX Workload Manager to improve system usage. The AIX

Workload Manager is a part of AIX that gives system administrators control over many system resources, either manually or automatically. It also generates graphical reports, including graphs of capacity usage over time. The result will give you a better understanding of your capacity needs. To learn more about the AIX Workload manager, see the Workload Manager topic.

__ Estimate future server usage

Estimating future server usage is more of an art than a science, yet it is a crucial step in the process of planning for future capacity. Start by charting capacity and workload usage over the past year and extrapolate the growth curve for the coming year. This will give you a good short-term estimate of next year's capacity needs. For longer term estimates, use capacity data from the past five years to develop a capacity curve for the next five years. When extrapolating, increase the growth curve for new initiatives that will affect server usage.

__ Plan for logical partitions

You might need to

shift logical partition (LPAR) resources as your business needs dictate. How your partition resources are allocated will affect your capacity plan. For more information on LPAR planning on your AIX servers, see the Planning for logical partition topic.

__ Plan for Power On Demand

With Power On Demand, you can acquire excess capacity and pay for only the capacity that you use. This will help you adjust your capacity plan for unexpected server usage. Understanding how you can upgrade only what you need is a critical aspect of your capacity planning. See Planning for Power On Demand for more information on developing that plan.

When you have completed the tasks identified in this topic, you should have a plan for capacity that identifies the following elements:

After you finish

__ Record your current configuration with all standby capacity listed.
__ Record a list of hardware you will need to upgrade dynamically.
__ Record a timetable for short-term or seasonal upgrades.
__ Record a timetable for long-term upgrades.

Parent topic: Planning for capacity

Planning for capacity with Linux

Capacity planning for Linux involves using several tools related to sizing your current workloads and planning for future workloads. Much of the data you gather to complete your plan is also used to plan for performance and availability. Therefore, the tools involved in planning for capacity are similar to those used in the two related planning processes. Complete the following checklist to ensure that you have adequately planned for the capacity that your business needs.

Before you begin your capacity planning checklist, answer the following questions.

Before you begin
__ Which type and size of database will your company use?
__ What other software applications are involved?
__ How many users will use these applications?
__ How much data will the server handle?
__ What are the inputs and outputs for the data?
__ What are your company's future growth plans both in the short and long terms?

Linux capacity planning tasks	
__	**Identify capacity considerations for Linux distribution requirements** Each Linux distribution has unique requirements that need to be understood as part of your understanding of how much capacity your Linux server can handle. Also, each distribution is tuned differently with different workload and simulation tools that help you develop a plan for current and future capacity. To learn more about capacity planning within your Linux

distributions, see the following resources.

- Red Hat Linux service offerings.
- Novell SUSE LINUX.

__ Measure current workloads

The first step in your Linux capacity plan is to assess existing workloads assigned to your Linux partitions. Several tools exist to measure these workloads.

__ Plan to simulate the environment

The second step in your Linux capacity plan involves modeling current and future capacity to ensure that you have adequate resources for your workloads. There are several capacity simulation tools available.

__ Plan for logical partitions

You might need to shift logical partition (LPAR) resources as your business needs dictate. How your partition resources are allocated will affect your capacity plan. For more information on LPAR planning on your Linux servers, see the Planning for logical partitions topic.

__ Plan for Power On Demand

If your simulations show that you will need seasonal or permanent capacity upgrades, you need to be prepared to address these needs. For more information about planning for, activating, and ordering additional processors for your hardware system, see the Planning for Power On Demand topic.

When you have completed the tasks identified in this topic, you should have a plan for capacity that identifies the following elements:

After you finish

__ Record your current configuration with all standby capacity listed.
__ Record a list of hardware you will need to upgrade dynamically.
__ Record a timetable for monthly or seasonal upgrades.
__ Record a timetable for long-term upgrades.

Parent topic: Planning for capacity

Planning for performance

Effective performance management requires thorough planning to ensure that you have the necessary server resources for your business needs. By ensuring that you are prepared for business contingencies, effective planning also reduces the time involved in managing your system performance when you need to add resources.

See the following information to plan for performance on your server:

- **Planning for performance with AIX**
- **Planning for performance with Linux**

Parent topic: Planning for workloads

Planning for performance with AIX

To get the performance that your business needs from your AIX server, perform the planning tasks listed below. Follow each task in the list to get the information that you need to help you complete your planning. Before you begin your planning tasks, complete the items in the following checklist.

Before you begin

__ Read the AIX Release Notes.

AIX performance planning tasks

__ Build a plan for performance

The Planning and Implementing for Performance chapter of the Performance Management Guide guides you through the complete process of setting performance objectives and using those objectives to plan a performance management strategy. Refer to the Performance Toolbox Guide and Reference for additional information about the tools available to you in the Performance Toolbox.

__ Understand the tools available to you

The Performance Toolbox Version 2 and 3 Guide and Reference explains tools available to you in the Performance Toolbox for monitoring your systems performance. Additional information on tools available to you can be

found at this reference as well.

__ Identify performance considerations for AIX release requirements

Refer to the AIX Release Notes or the guide to Installing AIX to identify the disk storage, CPU, memory, and other requirements of your AIX release. Identify any implications for your performance planning.

When you have completed the tasks identified in this topic, you should have a plan for AIX performance that identifies the following elements:

After you finish

__ Identify and record any necessary changes to the server's operating environment, such as adding a large number of users or a significant software product.
__ Identify and record any considerations for upgrading to a new AIX release, such as requirements for disk storage, CPU, and memory.
__ Identify and record interactive CPU requirements.
__ Identify and record memory requirements, including huge-page memory requirements if applicable.
__ Identify and record communications performance requirements.
__ Identify and record database accessibility requirements as they relate to disk and disk device requirements.
__ Identify and record the components of the workload.
__ Identify and record all performance requirements.
__ Identify and record the estimated resource requirements of the workload.
__ Record a complete strategy for meeting the performance requirements of projected workloads.

Parent topic: Planning for performance

Planning for performance with Linux

To get the performance that your business needs from your server running Linux, perform the planning tasks listed below. The links under each task in the list can help you get the information that you need to help you complete your planning. Before you begin your planning tasks, complete the items in the following checklist.

Before you begin

__ Read the Optimizing Linux environments for performance and scalability white paper to get a good overview of the tasks involved in planning for Linux performance.

Linux performance planning tasks

__ Identify performance considerations for Linux distribution requirements

Each Linux distribution has unique requirements that need to be met in order to get desired performance. Also, each distribution is tuned differently with different shell scripts or performance-enhancement tools. To get the most out of your distributions, see the following resources:

- Red Hat Linux service offerings
- Novell SUSE LINUX

__ Plan to create a performance baseline

The first step in your Linux performance plan is to assess existing workloads assigned to your Linux partitions. Several tools exist to measure these workloads. See the Linux on POWER applications Web site for more information on available applications, including those that can help you establish a baseline and perform other performance-related tasks.

__ Plan to simulate the environment

The second step in your Linux performance plan involves modeling current and future capacity to ensure that you have adequate resources for your workloads. There are several capacity simulation tools available.

__ Plan for Power On Demand

If your simulations show that you will need seasonal or permanent capacity upgrades, you need to be prepared to address these needs. So it is a good idea to add Power On Demand planning to your performance planning checklist. For more

information about planning for, activating, and ordering additional processors for your hardware system, see the Planning for Power On Demand topic.

__ Plan to test your solution's performance

Testing your solution's performance before running it in a production environment is a key step. Testing validates that your simulations take into account all variables and accurately represent production workloads. Testing also stresses the actual code with user transaction loads to capture performance bottlenecks inherent in the applications that you plan to run under Linux. For more information on planning to test your solution's performance in a lab setting, see the Planning for testing topic.

__ Plan to sustain performance through growth

Ongoing monitoring of your Linux systems provides for updated data points that you can use to validate and enhance your system's performance.

When you have completed the tasks identified in this topic, you should have a plan for your Linux performance that identifies the following elements:

After you finish

__ Identify and record any necessary changes to the server's operating environment, such as adding a large number of users or a significant software product.

__ Identify and record any considerations for upgrading to a new Linux release, such as requirements for disk storage, CPU, and memory.

__ Identify and record communications performance requirements.

__ Identify and record database accessibility requirements as they relate to disk and disk device requirements.

__ Identify and record the components of the workload.

__ Identify and record all performance requirements.

__ Identify and record the estimated resource requirements of the workload.

__ Record a complete strategy for meeting the performance requirements of projected workloads.

Parent topic: Planning for performance

Planning for availability

To minimize downtime and maximize availability, you need to prepare for hardware failures, power outages, server transitions, and disaster recovery.

Prepare a plan to use technologies and techniques to minimize downtime and maximize availability. The plan should include provisions for disaster recovery, power outages, server transitions, and hardware failures. This topic introduces the options for availability with each operating system.

- **Planning for availability with AIX**
- **Planning for availability with Linux**

Parent topic: Solution planning

Planning for availability with AIX

To minimize downtime and maximize availability on your AIX server, perform the planning tasks listed below. Before you begin your planning tasks, complete the items in the following checklist:

Before you begin

__ Read the AIX Release Notes.
__ Identify your disaster recovery plan.
__ Identify your backup and recovery strategy.
__ Identify the cost per hour of a system outage to both your business and your users.

	AIX availability planning tasks
__	Establish a backup policy Determine a strategy for backing up your organization's systems and files. For more information about backing up your systems, see the Backup files and storage media and Establishing a backup policy topics.
__	Establish a logical volume policy Determine a strategy for logical volume use that is oriented toward availability and performance.

		This policy can include items such as write-verify and mirroring, which can enhance availability but degrade performance. Establish a policy that is best suited to your needs. For more information about creating a logical volume policy, see the Developing a Logical Volume Strategy topics.
__	Establish a volume group policy Determine a strategy for volume groups that will help protect against disk failure, including mirroring (which can also aid performance). For more information about creating a volume group policy or using commands to mirror your volume group, such as the alt_disk_install command, see the Developing a Volume Group Strategy topic.	
__	Understand the different file system types Know the difference between CIFS, GPFS, JFS, JFS2, NFS, UDFS, and other file system types and how they can increase your AIX availability. For more information about clusters in	

AIX, see File Systems.

When you have completed the tasks identified in this topic, you should have a plan for AIX availability that identifies the following elements:

After you finish

__ Implement your established backup policy.
__ Record a complete availability strategy for a single server or multiple server environment.
__ Record a complete strategy for backing up your server.
__ Record a complete strategy for server recovery.
__ Record a complete strategy for data protection that includes solutions such as mirroring, concurrent maintenance, and Redundant Array of Independent Disks (RAID). Include detailed configuration and placement information for disk subsystem components.
__ Ensure the hardware requirements for your cluster configuration have been met, if applicable.

Parent topic: Planning for availability

Planning for availability with Linux

To keep your business running continuously with your Linux server, perform the planning tasks listed below. See this information to build a complete plan for availability. Before you begin your planning tasks, complete the items in the following checklist:

Before you begin

__ If you are migrating or upgrading, identify your current disaster recovery plan.
__ If you are migrating or upgrading, identify your current backup and recovery strategy.
__ Identify the cost-per-hour of a system outage to both your business and your customers.

Linux availability planning tasks	
__	Determine how clusters enhance availability Decide how best to use clusters in your environment to enhance availability. For more information about clusters in Linux, see Linux cluster software documentation and see the documentation

provided by your Linux distributor.

__ Identify options for service support

Several routes are available for providing Linux information directly to your service provider, where skilled technicians will review the problem details and inventory information. Your next level of support can then send an authorized service provider to your site to replace the failing hardware before a system outage occurs. For further information, see Setting up your server to connect to service and support.

__ Identify options for Linux reliability

Several tools are available to support Linux reliability, availability, and scalability (RAS), including:

- **snap**, which provides snapshots of system error data
- **update_flash**, which allows customers to download firmware updates

- **diagela**, which provides error analysis and writes interpreted errors back to the Linux syslog

__ Build a backup and recovery strategy

A backup and recovery plan for your server is a key part of system availability. Use the Backup and recovery topic to plan and build a backup and recovery strategy that is customized for your computing environment.

When you have completed the tasks identified in this topic, you should have a plan for availability that identifies the following elements:

After you finish

__ Record a complete strategy for backing up your server.

__ Record a complete strategy for server recovery.

__ Record a complete strategy for data protection that includes solutions such as mirroring, concurrent maintenance, and Redundant Array of Independent Disks (RAID). Include detailed configuration and placement information for disk subsystem components.

__ Record a complete and validated plan for cluster configuration, if applicable.

__ Ensure that the hardware requirements for your cluster configuration have been met, if applicable.

__ Record a complete availability strategy for a single server or multiple server environment.

Parent topic: Planning for availability

Planning for service processor failover

The ESCALA PL 850R/PL 1650R/R+ models support redundant service processor configurations that allow you to plan for dynamic failover. It is important to understand the considerations and requirements for a redundant service processor configuration to prepare for enabling the failover capability.

The redundant service processor capability enables you to configure a secondary service processor that is activated when the primary service processor fails. This information describes the considerations and requirements for enabling this capability, whether you are installing a new system with redundant service

processor capability or upgrading an existing system.

Preparing your network environment for failover

Preparation checklist

Use this checklist to prepare for redundant service processor enablement.

_ Review the configuration requirements discussed in the preceding section.

_ Decide which HMC configuration you will use (single HMC configuration or redundant HMC configuration).

_ Determine if additional cables are required for the redundant service processor.

_ If you are replacing your service processor to upgrade to a redundant service processor, ensure that you first back up your logical partition (LPAR) profiles and your service processor settings. Replacing your service processor causes a loss of LPAR configurations.

  Back up your partition profile data to a named file, using the instructions described in Backing up partition profile data. Make sure you specify a backup file name and do not use the HMC default file name. This enables you to preserve a perpetual copy of the backup settings on the HMC. Record the backup file name that you specify because you will use this file name to restore your partition data. See Restoring Profile Data.

  To back up your service processor settings, and find more information about installing the redundant service processor feature, see Install a model ESCALA PL 850R/PL 1650R/R+ redundant service processor assembly.

_ Ensure that your system meets the supported hardware and software version requirements for the service processor failover functionality.

Enabling service processor failover

After the redundant service processor environment setup has been completed, you can enable the service processor failover from the HMC. See Enabling service processor failover to enable the redundant service processor for failover mode.

Note: To initialize service processor failover, the first time you enable it your system must be in the powered-off state. For information about powering off and powering on your managed system from the HMC, see Powering on and off a managed system. After the initial enablement, powering off the system is not required to enable or disable the failover.

Parent topic: Solution planning

Planning for networking communications

How you configure your server to connect servers and other systems through local area networks, wide area networks, and to the Internet requires careful planning before successful implementation.

Servers exist to communicate with clients through networks. Therefore, network planning plays an essential role in overall solution planning. Many solutions contain several different types of networks, including local area networks (LANs), wide area networks (WANs), and various networks across the Internet, including virtual private networks (VPNs). When you consider all the elements in a successful networking strategy, you need to take great care in planning your networking and communications setup. The following topics comprise the necessary tasks for a complete network plan.

Network planning contains two primary components: planning the logical connections and planning the physical connections between network hosts, or nodes. For the purpose of convenience, this topic will use software to comprise the logical network planning and hardware to comprise the physical network planning.

Parent topic: Solution planning

Planning for network software

The first step in planning your network is to develop a software plan, which will detail the applications you need to run over the network and the minimum bandwidth and latency required by the applications. After you have determined the required bandwidth and latency for your applications, you can begin to develop a hardware plan.

Before you begin

__ Develop a list of business activities that require network resources.

__ Review resources relevant to your family of servers, including the Planning your TCP/IP Network topic in the *System Management Guide* in the Hypertext Documentation Library.

Network software planning tasks	
__	Develop a list of network applications Starting with the list of business activities, develop a list of applications that will require network resources. The types of applications range from universal applications, such as e-mail and Web serving, to specialized applications such as video conferencing and voice over IP. Depending on the list of applications and the number of users that require access to the applications, your network

resource needs can vary widely. Therefore, starting with the applications is an important first step in determining the scope of your network plan.

__ Obtain a network number

In order for your network to communicate with the internet, you will need to obtain a network number and register your domain with an accredited domain registration service. The Internet Corporation of Assigned Names and Numbers (ICANN) maintains a list of accredited registrars in your area. Your entire logical connection scheme, including the IP addresses and the host names associated with the addresses, starts with your company's assigned name and number.

For more information on obtaining an assigned name and number, see the ICANN Information Web site.

__ Devise an IP addressing scheme

Your hosts, or end user workstations, need IP addresses based

on your assigned name and number. The scheme you devise needs to scale to your business needs and enable easy management. For these reasons, an addressing scheme is a key part of your network software plan. The basic scheme involves assigning a unique IP address and host name to every host in your network. This allows applications to look up the address and host name to send the appropriate host the needed messages.

Depending on the size and scale of your network, your first consideration in developing this scheme is whether you want to use static or dynamic addressing. In order to manage a growing network, most networks use dynamic addressing for workstations and static addressing for servers. Dynamic addressing automates IP address assignment, which can significantly reduce management overhead. Dynamic addressing is usually done

through a Dynamic Host Configuration Protocol (DHCP) server. Depending on your operating environment, a number of tools can make setting up and managing a DHCP server relatively easy.

To learn how to plan your IP addressing scheme, see the chapter about address, name and network management in the IP Network Design Guide.

__ Build an IP address and host name database

You will need to keep track of all your IP addresses and host names in your network to efficiently manage organizational change and troubleshoot bandwidth and latency problems. Start by creating a list of all IP addresses and host names on your network. There are research tools that help you create a database that relates IP addresses or host names to individual machine names on your network topology. The machine names are typically identified by the medium access control (MAC) address on the host's network

card.

To learn how to build an IP address and host name space, see the chapter about address, name and network management in the IP Network Design Guide.

__ Plan for name management

Some form of directory services is required to manage host names and addresses, and their interrelations in network domains and zones. You have many options related to the type of name service you use. If you use static addressing, this is typically done through a Domain Name System (DNS). The DNS provides applications with a mapping of IP addresses to host names wherever they reside in various network domains and zones. It also provides other vital information to the application. If you use DHCP to dynamically assign addresses, your hosts have a different IP address every time they start up and initialize a connection to the DHCP server. To manage the names and addresses in a dynamic

addressing system, you need to plan for a dynamic Domain Name System.

To learn how to plan for name management, see the chapter about address, name and network management in the IP Network Design Guide.

__ Plan for subnets

In large networks with routers, a lot of overhead is created with a large number of hosts. To improve performance and manageability, the host number (typically the second half of an IP address) can be subdivided into a subnet number and a host number to provide a second logical network. The second network is called a subnetwork or subnet. Determining your subnet scheme is an important step in your network software plan. A good scheme can ensure that each router in your network is performing well and your hosts do not need to send messages through too many hops to get them to their destinations.

To learn how to plan for subnets, see the chapter about address, name and

network management in the IP Network Design Guide.

__ Plan for administrative subdivisions

You need to create administrative subdivisions to improve manageability, to isolate sensitive information, and to ensure adequate resources to mission-critical applications. Typically, businesses are divided into a front end and a back end. The front end includes a basic file and print network, which also provides e-mail and Web browsing to users. The back end contains all the transaction processing for the business, including automated accounting, shipping, receiving, Web and e-commerce workloads, and other types of electronic data interchange (EDI).

Your plan for administrative subdivisions will include the platforms on which to run the subdivisions. The front end may not need to meet the rigorous requirements of performance, availability, and security, which the back end requires.

To learn how to plan for administrative subdivisions, see the chapter about address, name and network management in the IP Network Design Guide.

When you have completed the tasks identified in this topic, you should have a network software plan that identifies the elements in the following list.

After you finish

__ Record your assigned network numbers and names.

__ Record a database of IP addresses or host names for your network.

__ Record a table of subnets on your network and compare it to your routing topology when you complete the topology.

__ Record a table of administrative subdivisions on your network, with the operating environment and server responsible for each subdivision.

Parent topic: Planning for networking communications

Planning for network hardware

After you have a software plan in place, you can begin designing a network hardware topology that will provide sufficient network resources for your applications. Many networks grow without proper planning. As the business grows, they become unmanageable and suffer from performance problems. Networks that are not properly planned can lack the scalability that would allow them to grow without adversely affecting future business needs. In short, adequate network design can enable sufficient performance, availability, and security. In the process, you can provide enough information and transaction processing for all your users.

The following checklists will help you make these planning decisions and begin designing a network that fits your needs.

Before you begin

__ Review the Network communications topic to coordinate information gathering pertaining to the communications infrastructure at your site.

__ Create a list of users that need network access.

__ Develop a list of servers that need network connections.

Network hardware planning tasks

__ Determine the number of host machines

The first step in hardware network

planning is to develop a list of host machines for your networks to support. Host machines are user workstations that connect to networks. Each host machine needs a unique IP address and name. In addition, each host machine will need access to an appropriate amount of bandwidth to support the applications that are planned for the host machine.

__ Plan for types of hosts

Your network might contain several types of hosts, including stand-alone, diskless, and dataless hosts. Your network design will be affected by your host types. For example, if you have a large number of stand-alone Windows-based PC hosts, you need to take into account server platforms, client protocols, and additional security measures. Or, if you have diskless hosts, some network media not be suitable.

_ Plan for network media

Network media are the types of connection that make up the network. They include the actual cables as well as the protocols that govern the

connections. You have several options in choosing network media, including Ethernet (fast or Gigabit), token ring, Fiber Distributed Digital Interface (FDDI), Asynchronous Transfer Mode (ATM), wireless technologies, and others. Each medium has advantages and disadvantages. Ethernet is most often used because it is inexpensive and easy to manage, but it carries a performance cost. Mission-critical hosts can connect by using token-ring or FDDI technologies instead of Ethernet to improve performance. ATM is most often used as a backbone technology between different networks because of its unique properties. Choosing your network media is often determined by the balance between performance and availability on one side and cost on the other.

To learn how to plan for network media, see the chapter on network infrastructure in IP Network Design Guide.

__ Plan for routers and switches

Different subnets or administrative subdivisions within a network can be

connected by bridges, hubs, routers, or switches. Bridges and hubs are used sparingly because of their inherent limitations. Routers are most commonly used to connect different domains or subnets within a network because they offer better administrative control over network traffic. However, they can cause performance problems if too many routers exist between hosts. For this reason, switches are often used to speed connections between subnets on a network. Whether you choose a router or a switch to connect network subnets requires careful planning. An adequate plan for routers and switches enables your network to grow with your business without adversely affecting network performance.

To learn how to plan for routers, see the chapter about routing and design in the IP Network Design Guide.

__ Create a network topology

After you have determined the components of your network, you need to develop a network topology. The two main types of typology are flat and hierarchical

networks. Unless your network is quite small, you will most likely create a hierarchical network, which resembles an inverted tree with the root or trunk at the top and the nodes of the network (or hosts) connected by branches at the bottom. Your topology should schematically itemize all the physical cables and connections of the hardware connected to the network. It should include the types of hosts, network media, hubs, bridges, routers, switches, and servers.

To learn how to design a network topology, see the IP Network Design Guide.

When you have completed the tasks identified in this topic, you should have a networking hardware plan that identifies the following elements:

__ Record a topology of your network.

__ Record a list of hardware, including network hosts, interface cards, and cables, that you need in order to implement the topology.

Parent topic: Planning for networking communications

Planning for remote access

In distributed businesses, employees need to access corporate resources remotely. A complex and evolving set of technologies enables remote access. For this reason, planning your network for remote access can be challenging. Careful research and design can ensure that users who need remote access will experience the network as though they are on site, without compromising the security, reliability, performance and manageability of the overall network.

Before you begin

__

Create a table of users that need remote access to the corporate infrastructure, along with the applications they will use in a related column.

Remote access planning tasks

__ Plan for remote offices

A remote office extends the network topology to off-site locations. At a minimum, it will contain one or more hosts and might contain servers, hubs, bridges, routers, or switches. You can either connect the remote office to the local office through a private leased line or through a virtual private network (VPN), which creates a secure connection over the Internet. A physical private network will be easier to manage, will perform better, and will be more secure than a VPN at a substantially higher cost. The decision to use a VPN rather than committing to a leased line is typically based on the size of the office. Home office employees and small satellite offices are best suited to VPNs. For medium-sized and large remote offices, leased lines are recommended. Also, if small offices have high-bandwidth or

low-latency needs, such as video conferencing or Voice over IP (VoIP) respectively, a leased line is recommended.

To learn how to plan for remote offices, see the chapter on remote access in the IP Network Design Guide.

__ Plan for Internet connections

Choosing Internet service providers (ISPs) and designing connections to them are crucial steps in developing your network plan. Various technologies enable your company to connect to the Internet, and for clients and remote offices to access your company resources and enable remote access to your company resources. Large companies typically use leased lines to connect to an ISP, which connects to the Internet backbone. Small companies and small offices can often save cost by using broadband connections, such as DSL. In addition to the connection type, you must take several other design considerations into account. For

example, you need to decide whether your ISP hosts your Web and e-mail servers, or whether you do. These decisions effect many later network planning decisions, such as the locations of firewall servers.

To learn how to plan for Internet connections, see the chapter on remote access in the IP Network Design Guide.

__ Plan for other remote access

Often employees will need to dial into your network while traveling or for server and network diagnostics. If traveling employees have Internet access, this is typically done through the same VPN that you set up for small satellite offices. But you also need to plan for remote personnel to dial directly into your network through a modem connected to a server. There are several reasons to plan for direct remote access:

- It is often the most economical solution for text-based data transfer.
- It is often necessary for service providers.

- It can provide emergency failover in case your ISP or your leased line connection are out of service.

To learn how to plan for remote dial-in access, see the chapter on remote access in the IP Network Design Guide.

When you have completed the tasks identified in this topic, you should have a remote access plan that identifies the following elements:

__ Record a topology of all off-site network resources, including the remote access connection points to your local area network (LAN).
__ Record a list of service providers and leased lines in use and determine the peak bandwidth of each line.
__ Estimate future remote access needs and record a strategy for improving the reliability, manageability, security, and accessibility of your remote networks, while lowering their cost.

Parent topic: Planning for networking communications

Planning for network security

Network security is perhaps the most vital and challenging aspect of network planning. Your network connection must allow legitimate traffic through the door while keeping illegitimate traffic out.

Before you begin

__ Develop a list of points of entry into your network.
__ Create a corporate security policy from which your network security policy will follow. Include policies on access to confidential and sensitive information, what actions are taken in the event of a breach, and by whom.

Network security planning tasks

__ Develop a network security policy

Starting with your corporate security policy, develop a network security

policy. The following elements are recommended:

- Create a firewall

  Any adequate security policy includes the use of a firewall to filter traffic in an out of the network. The firewall should restrict data according to the protocol it uses and terminate traffic if the protocol does not match the port through which it is attempting to travel. It should also strictly limit open ports to prevent intruders from entering the corporate network.
- Isolate confidential information

  Any system that has confidential or sensitive information should not be directly accessible from the outside. Also, access to

such systems should be restricted from the inside; only authenticated users should gain access.

- Create a demilitarized zone

  A demilitarized zone is an area outside of the firewall where transactions can take place without putting the network in jeopardy. All anonymous access to the network should remain in the demilitarized zone.
- Develop an authentication scheme

  Authentication is the process of requiring a user ID and password, or some form of certificate-based authentication, in order to access a network domain. All direct access to the corporate intranet should require

authentication. All direct access through the firewall should also require authentication. Plan to follow user ID and password best practices, which include long passwords (at least 8 characters), mixed passwords (a combination of letters, numbers, capitals, and lower case symbols), and regularly changed passwords (every two or three months).

- Develop an encryption system

  Encryption is the process of turning all data into a code which is only decipherable by a system of private and public keys. All sensitive data exiting the corporate network should be encrypted. All sensitive data from

remote offices into the network should also be encrypted.
- Develop a social engineering blocking system

  Social engineering is the process of impersonating trusted individuals over the phone to gather sensitive information, such as passwords and corporate organizational information. This is a common technique used by hackers to gain access to networks. Training employees to never give out this information over the phone is the only defense against this type of security breach.

To learn how to develop network security policy, see the chapter on IP security in the IP Network Design Guide.

__ Plan for IP Security Architecture IP Security Architecture (IPSec) is an open,

standards-based security architecture that provides the following features:

- Data integrity (prevents attacks based on ill-formed data)
- Replay protection (prevents attacks based on replaying messages)
- Secure creation and automatic refresh of encryption keys
- Strong cryptographic algorithms
- Certificate-based authentication

IPSec includes several protocols that each perform one of these functions. Many security products use IPSec as a foundational architecture.

To learn more about IPSec, see the chapter on IP security in the IP Network Design Guide.

— Plan for virtual private networks

Virtual private networks (VPNs) use IPSec to create a secure, private connection, or tunnel, through a public network such as the Internet. Several tools are available for each platform to turn ordinary Internet connections into

VPNs. Considering the need for communication between remote users, branch offices, and corporate partners, VPNs are an important way to encrypt and authenticate information between remote nodes of the corporate network.

To learn how to implement a VPN, see the chapter on IP security in the IP Network Design Guide.

__ Plan for virus and spyware protection

Viruses and other harmful software, called malware, disguises itself as legitimate business content, only to run malicious activity after it is inside the company network. Malware is the most pervasive form of network security breach. Each host on your network should be equipped with antivirus and antispyware applications that are updated weekly and run at least weekly. These programs are designed to block malware before it can replicate themselves over your network.

To learn how to prevent virus and spyware infections, see the chapter on IP security in the IP Network Design Guide.

When you have completed the tasks identified in this topic, you should have a network security plan that identifies the following elements:

__ Record a network security policy, that includes firewalls, demilitarized zones, access rules for sensitive information, authentication, encryption, and counter-social engineering training.

__ Record a topology of your security architecture, including which areas require authenticated access, which areas are protected by firewalls, where your demilitarized zones are connected, and which remote users or offices use VPNs.

__ Record a list of antivirus and antispyware applications that you plan to load on host machines. Develop a policy for weekly updates; and configure the hosts to automatically run the applications at least weekly.

Parent topic: Planning for networking communications

Planning for network performance

You can have fast servers and workstations, but if the data traffic between them is slow, the whole enterprise is slow. Therefore, it is important to plan your network bandwidth to match the speed of your business. You can improve performance in three main ways:

- Increase the speed of all data traffic throughout the network
- Change some of the data flow from point-to-point to multicast
- Allow higher priority data to flow faster than lower priority data. This last item is called Quality of Service (QoS)

Before you begin

__ Highlight areas of your network topology where potential bottlenecks occur.

__ Identify network traffic that should be given highest priority.

Network performance planning tasks	
__	Plan to remove bottlenecks The first step in network performance planning is to identify areas where network traffic is greater than the bandwidth it is flowing through. Start by examining the topology and identifying potential slow areas, and then monitoring those areas. After you identify slow areas, or bottlenecks, plan to upgrade hardware and improve performance. Possible problem areas include:

- Older Ethernet network cards

  If your Ethernet network interface cards (NICs) are 10BASE-T, they can be easily upgraded to Fast Ethernet. In mission-critical networks, you can upgrade Ethernet to Fiber Distributed Digital Interface (FDDI).
- Hubs instead of switches

  Hubs send data to all participants connected to them. Switches send data only to its desired destination. If a hub is connected to three hosts, a switch will typically be three times faster than that hub. If tens of hosts are connected to a hub, the switch will speed performance by at least an order of magnitude.
- Overloaded routers

  Routers can significantly slow traffic if

more hosts are connected to them than they can reasonably handle. Your options include upgrading the router or converting it to a smart switch.

- Too many routers

  The temptation with overloaded routers is to add more subnets and connect them with more small routers. This can make the situation worse by increasing the number of hops data must travel through in order to get to its destination. It is often better to upgrade the router than add hops to the network.
- Outdated servers

  Some network administrators put older servers on the front end because the data flow is not mission critical, as it is in the back end. But with the advent of graphics-intensive user applications such as

Flash programs running over the Web, older servers may not be able to keep up and users end up waiting for applications to load.

To learn how to improve network performance, see the chapter on multicasting and quality of service in the IP Network Design Guide.

__ Plan for multicasting

Multicasting sends data from the server to multiple clients at one time. In one-to-one networking, the total bandwidth required equals the bandwidth needed by the application times the number of clients. With multicasting, the total bandwidth required equals only the amount of bandwidth needed by the application. Multicasting only works with so-called "push" applications, such as online newsletters. If you can convert some of your one-to-one applications to multicasting, you can conserve network bandwidth and improve performance in the process. However, setting up the network to handle multicast traffic involves designing the entire network topology with multicasting in mind.

__ Plan for Quality of Service (QoS)

Quality of Service (QoS) works like high-occupancy commuting lanes on highways. Special lanes are set up for traffic with two or more passengers per car, which arrive at their destinations faster because they do not get stuck in traffic. Similarly, in QoS, the network gives priority to certain data packets and ensures that they arrive at their destinations within a certain time frame. Like multicasting, planning for QoS must include the entire network topology. For this reason, if you plan to implement QoS, review the network software and hardware planning steps and incorporate prioritized traffic protocols throughout your topology.

When you have completed the tasks identified in this topic, you should have a network performance plan that identifies the following elements:

After you finish

__ Identify the nodes of your network topology that need performance-related equipment upgrades.
__ If you plan to multicast, record a list of hardware and software that enables multicasting.
__ If you plan to use QoS, record a list of hardware and software that enables QoS.

Parent topic: Planning for networking communications

Planning for network availability

High-availability networks provide redundant infrastructure that can be switched on in case the primary network resources experience performance problems or failures of any kind. The first step is to determine your needed degree of uptime. Systems with better than 99 percent uptime are considered fault tolerant. As the availability percentage approaches 100, you get into the high availability networks. The closer you get to 100 percent uptime, the more expensive this availability gets. Therefore, you need to develop a good business case for high availability networks. For example, application service providers need high availability (99.9999 percent uptime). Your corporate Web site might only need 99.9 percent uptime. The difference in cost can be substantial, depending on the size and scale of your network.

Before you begin

__ Create a table of applications that require fault tolerant or high-availability networks.

__ Identify the parts of the network topology used by those applications.

Network availability planning tasks

__ Identify single points of failure

The easiest and most economical way to improve network availability is to remove single points of failure. A single point of failure occurs when there is just one physical connection between parts of a network. Many different network topologies can help you remove single points of failure. The basic principle is to connect more nodes to individual servers and other network resources. If one of the nodes fails, traffic can be rerouted around the failed system.

__ Plan for fault tolerance.

Fault-tolerant networks have very few single points of failure, if any. In addition, fault-tolerant networks have disaster-recovery hardware at each node. Typical hardware measures per node include:

- Replicated hardware subsystems

  If a network is important enough, a second server, router, or other

device is available at each node in case of system failure of the primary device.

- Standby hardware

  An example of standby hardware is a redundant array of independent disks (RAID), which enables hot-swappable storage media.
- Fast boot methods

  You need to be able to dump and reboot in the shortest possible time to maximize uptime.
- Backup power

  Plan to connect as many nodes as you can to uninterruptible power supplies. Large data centers should have backup generators as well.
- Total remote management

  You should be able to remotely diagnose and reboot

servers regardless of their state.
- Concurrent backup and restore

  Make sure you can use the backup system as soon as a failure is detected, and begin backing up again in real time.

To learn how to plan for high availability and clusters, see the Planning for availability topic.

__ Plan for clustering

Clustering is the process of connecting a large number of servers to achieve continuous, or 100 percent uptime. Many families of servers enable clustering, and several software packages, such as WebSphere application and Web server software, enable clustering. Clustering can be relatively straightforward for continuous or steady-state usage. The challenge is to maintain uptime during routine maintenance or while upgrading systems within a cluster.

The basic principle behind clustering is virtualization. That is, though a group of servers are physically distinct, they are logically

indistinct. Part of the virtualization process includes virtual IP addressing, which assigns IP addresses to a pool of servers rather than each physical server. In this way, no routing is involved when one server goes down and one of the backup servers that are connected to the same cluster as the primary server takes its workload.

In , virtual IP addresses can be used to provide redundancy of physical adapters by not having a given virtual IP address assigned to a single physical adapter.

When you have completed the tasks identified in this topic, you should have a network availability plan that identifies the following elements:

After you finish

__ Record a list of all single points of failure and plan to create redundancy.

__ Record a list of hardware that requires backup and disaster recovery measures.

__ Record a list of servers that will be part of a cluster, and develop a plan for clustering software that will enable you to implement your clustering plan.

Parent topic: Planning for networking communications

Planning for network management

So far, you have designed your network to provide adequate bandwidth to your business processes, applications, and users. Now you need to design additional systems to make sure that your network continues to function as designed amidst growth and other business change. This involves routine maintenance, monitoring and troubleshooting problems, and developing upgrade paths in an iterative process. Sufficient planning for network management involves ensuring that you have adequate processes, tools, and infrastructure to maintain and grow your network resources as your business demands.

Before you begin

__ Have a completed network plan that includes software, hardware, remote access, security, performance, and availability.

__

Identify administrators who will be responsible for managing administrative subdivisions within the network.

Network management planning tasks

__ Plan for a network management protocol

Because Simple Network Management Protocol (SNMP) is the most widely used management protocol, every family of servers includes an SNMP agent. The SNMP agent provides a framework that enables information stored in hosts and in the Management Information Base (MIB) to affect changes in the network. Several network management software packages include SNMP as a foundational architecture. These tools vary by software operating system.

__ Develop a network management strategy

Network management is crucial, but it exacts a cost on the network. Ironically, network monitoring,

which is designed to enhance network performance and availability, itself, requires network resources that can slow down a network. Therefore, an adequate network management strategy will enable strong management without causing performance or availability problems. The following elements comprise a network management strategy:

- Create a network management objective that details what a successful strategy will entail.
- Determine your system's SNMP capability.
- Determine your network management software capability.
- Customize your network management software to meet your objectives, if necessary.
- Configure the agents and

managers for correct community names.

To learn more about managing your network, see the chapters on network management in the IP Network Design Guide.

When you have completed the tasks identified in this topic, you should have a network management plan that identifies the following elements:

After you finish

__ Record a network management strategy.

__ Record a test procedure to ensure that you have adequate software to manage your network resources on implementation.

Parent topic: Planning for networking communications

Planning for InfiniBand Networks

Learn about clustering systems using InfiniBand (IB) hardware.

server hardware now supports clustering using InfiniBand (IB) hardware. The information in this topic collection discusses the planning resources and considerations for clustering your systems using InfiniBand (IB) hardware.

- **Overview of InfiniBand products and networks**
  Learn about setting up an InfiniBand (IB) network.
- **Planning switch networks**
  View resources to help you plan for an InfiniBand (IB) switch network.

Parent topic: Solution planning

Overview of InfiniBand products and networks

Learn about setting up an InfiniBand (IB) network.

If you plan to set up a clustered server configuration using InfiniBand (IB) switches to network your servers, this section provides an overview of the components required for the network. The requirements are based on the type of host channel adapter (HCA) used to connect to the InfiniBand fabric. The following table shows the required components and supported adapters for setting up your IB network.

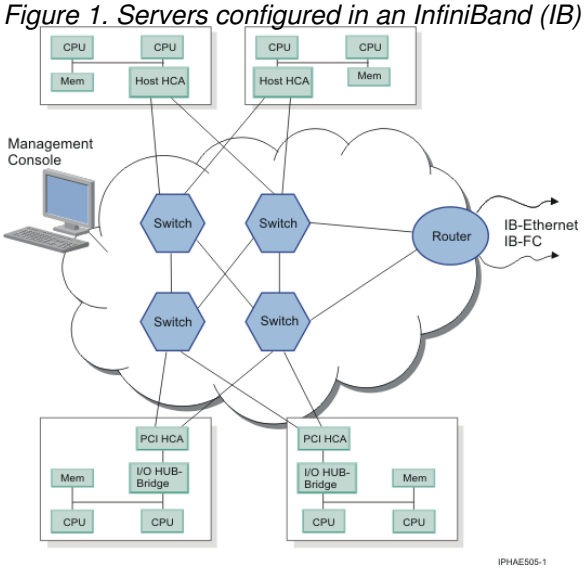
Table 1. Supported InfiniBand (IB) components

IB component	PCI adapter	GX adapter

Adapter	PCI-X 4x IB Host Channel Adapter (HCA)	GX 4x/12x IB Host Channel Adapter (HCA)
Systems	server, low-end	server, mid-range and high-end
Switches	Topspin 120 Server Switch (481/20), Topspin 270 Server Switch (482/70)	
Cables	certified cables	
Fabric Management	Topspin Web user interface and Element Manager	Network Manager
AIX version	AIX 5L version 5.3 with the 5300-03 Recommended Maintenance package	
Linux version	SUSE Linux Enterprise Server 9 SP2 with Topspin Enterprise Commercial Stack	SUSE Linux Enterprise Server 9 SP2 with IB GX HCA driver and OpenIB Gen2 Stack

The following illustration shows servers that are working in a cluster with InfiniBand (IB) switch networks.

Figure 1. Servers configured in an InfiniBand (IB) network



Parent topic: Planning for InfiniBand Networks

Planning switch networks

View resources to help you plan for an InfiniBand (IB) switch network.

Use the following guide to resources to plan your InfiniBand network:

- For information about the requirements and installation procedures for Topspin switches and InfiniBand environments, see the InfiniBand Hardware Installation and Cabling Guide Web Release, Topspin number: 10-00122-WEB.
- To help you get started with planning your IB switch network using the481/20 - Topspin 120 and 482/70 - Topspin 270 switches, see the steps for installing the cluster in The *Guide to Clustering systems using InfiniBand (IB) hardware*. The guide provides planning and installing information to help guide you through the process of installing a cluster fabric using these switches.
- If you are setting up or servicing a cluster network, use the *Guide to Clustering systems using InfiniBand (IB) hardware*

The following guides are also available to help you set up and service your network:

- *InfiniBand Hardware Installation and Cabling Guide Web Release, Topspin number: 10-00122-WEB*
- *Topspin 120/Cisco SFS 7000 Hardware Guide, Topspin number: 10-00032-04-A0*
- *Topspin 120/Cisco SFS 7000 Quick Start Guide, Topspin number: 10-00033-04-A0*

- *Topspin 270/Cisco SFS 7008 Hardware Guide, Topspin number: 10-00044-04-A0*
- *Topspin 270/Cisco SFS 7008 Quick Start Guide , Topspin number: 10-00045-04-A0*
- *Element Manager User Guide, Topspin number: 10-00116-02-A0*
- *Chassis Manager User Guide, Topspin number: 10-00029-05-A0*
- *Command Line Interface Reference Guide, Topspin number: 10-00012-07-A0*
- *Host-side Drivers User Guide for Linux, Topspin number: 10-00125-02-A0*

These guides are available for download in the ESCALA Power5 Hardware Information.

Parent topic: Planning for InfiniBand Networks

Planning for hardware

Before installation, you will need to ensure that you have all the required upgrade hardware. You will also need to plan for power, environmental needs, and server placement. Finally, you need to prepare for unique configurations based on how you plan to use the server, including data storage and cabling.

Whether you are upgrading an existing solution or developing a new solution, good hardware planning is essential for the successful setup and use of your server. It ensures that you have everything you need and that you have met all of your server requirements.

Your hardware plan contains the following sections.

- **Planning for your physical site**
- **Planning for I/O**
- **Planning for disk space**
- **Planning for removable media**
- **Planning for printers**

Parent topic: Solution planning

Planning for your physical site

Prepare a cool, dry space with a raised floor, plenty of clean, steady power and all the necessary bandwidth for your server. Before you begin with the main planning tasks, you will need to gather the following information.

Before you begin

__ Have a list of current hardware.
__ Have a list of current configurations.
__ Have a list of new hardware.

	Physical site planning tasks
__	Plan for physical hardware This quick reference organizes your Planning reference into

logical categories. Within each category, you can choose step-by-step processes that give you the guidance you need to prepare your site for your server. It includes physical site planning, server specifications, hardware specification sheets, power, and cables.

Note: Pay particular attention to the power cable specifications. If at any time in the future, you plan to use a 64-way server, you will need 100 amp-rated breakers and power cords.

__ Plan for server cables

Depending on the number of adapters and devices you will connect to your system, cabling can become complicated.

After you finish

__ Record a physical floor plan for placement of your system components.
__ Record a configuration plan showing placement for the internal components of your system.
__ Identify hardware placement to support logical partitions and disk unit configuration.

Parent topic: Planning for hardware

Planning for I/O

Input/Output (I/O) is perhaps the most unique aspect of your solution. Because of the variety of I/O types and processes you could have in your server solution, I/O processes can be the most labor-intensive aspect of solution planning. Much of your I/O planning is covered in the Planning for networking and communications topic. This topic focuses on I/O that is not related to networking and communications. Even though I/O processes are complicated, your manufacturer has resources that can help you plan. Before you begin with the main planning tasks, you will need to gather the following information.

Before you begin

__ Have a list of devices that need to communicate with your server.
__ For each device, indicate the type of connection it makes to the server.
__ Ensure that those types of I/O connections are still supported.

I/O planning tasks

__ Plan for I/O expansion units

If your solution requires I/O expansion units, make sure you add this to your plan, complete with the RIO loop connection to the expansion unit. For each unit, you should include a list of attached I/O devices; and for each device, you should check to make sure you have the appropriate driver. If you plan to hot swap cards or drives in your expansion units, make sure you add this to you plan.

__ Plan for I/O devices

I/O devices typically connect to expansion

units. The devices perform functions that your solution demands, such as storage. Your plan needs to include a list of all devices, including their connection to the server through expansion units.

__ Plan for I/O adapters

Often solutions demand special adapters to connect I/O devices. If your solution requires adapters, add these to your plan.

After you finish

__ Record a list of I/O expansion units to be installed with a diagram of their RIO loops.

__ Record a list of devices initially plugged into the I/O expansion units with the necessary drivers and adapters next to the name of each I/O device.

Parent topic: Planning for hardware

Planning for disk space

A plan for flexible data storage is a critical element of a server solution. A complete plan will include both independent disk pools (also known as independent auxiliary storage pools) and switchable disk units. Before you begin with the main planning tasks, you will need to gather the following information.

Before you begin

__ Have a schematic of all current disk storage detailing how the storage is attached.

__ Quantify available disk storage.

__ Have a list of disk requirements for both applications and data.

Disk planning tasks

__ Plan for physical disks

Calculate the amount of storage you need initially and develop an upgrade path that allows for additional disk drives to be added later. Determine how each drive will be attached, what type of drive it is (for example, SCSI), and what its function is in the overall solution.

__ Plan for disk partitions On AIX and Linux systems you can divide your hard disks into partitions. Each disk can have a number of partitions on it, allowing you to separate system recovery software from other applications, for example. For each disk, determine the size and quantity of partitions. Allow for future reconfiguration of your disk partitions where necessary.

After you finish

__ Record a list of disks that must be added and how those disks will be attached.
__ Record a disk partition plan showing on what partitions data and applications reside, if applicable.
__ Identify an upgrade path for future disk storage needs.

Parent topic: Planning for hardware

Planning for removable media

Your media plan should include the types of backup media, how the drives are connected to the server, what drivers you need for your drives, where you plan to store your media, and your backup schedule. To ensure that your plan has all the necessary elements, complete the following checklist. Before you begin with the main planning tasks, you need to gather the following information.

Before you begin	
__	If you have not already done so, record a backup and recovery plan detailing your backup media needs.
__	Have a list of current data to backup.
__	Have a list of applications to back up.

Backup media planning tasks	
__	Plan for tape drives If you plan a new installation with tape backup media, ensure that you choose the appropriate tape size and format for your solution.
__	Plan for tape compatibility If you plan a data migration, ensure that your current and target servers and tape devices are compatible.
__	Plan for optical media Optical media allows you to access your backup data much more quickly than tape. If you are planning to use optical media, such as DVD drives, include this in your plan.

Make sure you include a plan for your HMC optical drive.

After you finish

__ Record a list of tape drives including to what devices they are attached.
__ Record a list of optical drives including how they will be attached.
__ Calculate how much tape and optical media you will need for your backup plan.

Related Information

For more information on managing media devices, see Managing Devices.

For more information on tape storage solutions, see Tape.

Parent topic: Planning for hardware

Planning for printers

Printing can reduce productivity if it is not properly planned and implemented. To ensure that your printers handle the work your users demand, complete the planning tasks below. Before you begin with the main planning tasks, you need to gather the following information.

Before you begin

__ Have a list of current hardware.
__ Have a list of current configurations.
__ Have a list of new hardware.

Printer planning tasks

__ Plan for new printers

To develop an adequate printing plan, start by calculating printer workloads based on the number of users on the network and how much each user prints. Next, take an inventory of all network-attached printers and detail the number and type of new printers that you will need to cover the workloads. Then

	add the printers that need to be directly connected to client machines. Keep in mind that it might be more economical to purchase one high-end printer instead of two midrange printers.

After you finish

__ Record a list of users with anticipated printer use for each user.
__ Record a list of printers that collectively will handle those workloads.
__ Identify future printing needs and how you plan to meet those needs.

Parent topic: Planning for hardware

Planning for service and support

Understanding the different functions and features of your service environment can help you prevent server problems. Understanding the applications that you can use to provide those functions can help you plan for regular preventive maintenance.

Your service and support plan ensures that ongoing maintenance schedules are maintained, and helps keep your systems in good health. Before you begin your planning tasks, be sure you have completed the items in the following checklist:

Before you begin

__ Identify your partitioning environment.
__ Identify the operating system you will be installing on your partitions.
__ Identify your console environment.

Plan for service and support	
__	Understand the service environment Understand all of the elements of your service environment before developing a service and support plan.

- Elements of your service environment

  These elements include connectivity, inventory, electronic problem reporting, fixes, and remote support.
- Introduction to the service applications

  You can run various service applications on the HMC and the partitions, such as Inventory Scout, Remote Support Facility, and Service Focal Point.
- Map of service applications and functions

  Create a map of the different elements of the service environment to your applications, which will become a critical piece of your service and support

plan.

__ Plan your console configuration and placement

Consoles need to be carefully configured and placed in order to give service providers access to important service functions. For more information on the configuration and placement of consoles for service and support purposes, see the Planning for consoles for your service environment topic.

__ Plan your network

Understand the networking requirements for setting up your service environment.

- Networking for your service environment

  Understand physical and logical requirements before developing a network plan for your service reporting.
- Managing your server using the Hardware Management Console

Understand the requirements and capabilities of the HMC before planning to use the HMC on your network for service reporting.

__ Choose a service configuration

Understand how to set up your service environment using different scenarios before developing a service configuration plan.

- Scenarios: AIX

  This scenario demonstrates the recommended connectivity methods for AIX.
- Scenarios: Linux

  This scenario demonstrates the recommended connectivity methods for Linux.

__ Plan a fix strategy

Understand how to develop a fix management strategy before adding it to your service and support plan.

After you finish

__ Record the networking requirements for your environment.
__ Record additional hardware requirements.
__ Identify your electronic reporting strategy.

Parent topic: Solution planning

Planning for testing

Testing can help validate that your new system is functioning as planned. Based on your system requirements and needs, your test can range from covering the basics to an in-depth analysis.

Testing is an ongoing process in which parts of your solution will be running in real time while others are still in the testing phase on secondary partitions. Because of the complexity of testing process, testing your solution requires careful planning. Follow these steps to complete a successful test plan. Before you begin with the main planning tasks, you will need to do the following.

Before you begin

__ Have the rest of your hardware planning done.
__ Verify that you have taken into consideration physical planning and installation requirements.
__ Have an understanding of how your solution is supposed to work.

Test planning tasks

__ Determine acceptance criteria

Determining acceptance criteria is the first step in your test plan. These criteria should establish requirements for what it will take to bring your system to the appropriate level of function, performance, availability, and risk. These criteria will help promote a quick and easy transition from the time the authorized service provider presents the system to you until you formally accept your new system.

__ Assess your business needs

An adequate business assessment should place testing priority on mission-critical functions. Mission-critical functions may require multiple regression tests, in addition to the overall system testing you plan to perform.

__ Identify resources that could support this testing

Testing can be resource-intensive. In your test plan, make sure you have sufficient resources in the following areas:

- Hardware
- Software
- Labor
- Tools
- Licenses
- Location

__ Assign personnel

Make sure your plan includes human resources assigned to perform and monitor the testing.

__ Develop a test schedule

Your plan must include the length of time for testing, a target date for activating your solution, and how long you will continue to test certain inactive features.

After you finish

__ Review your test plan thoroughly before implementing it. This review should focus on your time-line, requirements, and steps necessary to complete your plan.

__ Record a list of resources that you need, including human resources and the costs of those resources.

Parent topic: Solution planning

Technical publication remarks form

Title :	ESCALA POWER5 Hardware Information Solution planning

Reference N° :	86 A1 06EW 00	**Date:**	July 2006

ERRORS IN PUBLICATION

SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please include your complete mailing address below.

NAME : _____ Date : _____

COMPANY : _____

ADDRESS : _____

_____

Please give this technical publication remarks form to your BULL representative or mail to:

Bull - Documentation Dept.
1 Rue de Provence
BP 208
38432 ECHIROLLES CEDEX
FRANCE
info@frec.bull.fr

Technical publications ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

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

Phone: +33 (0) 2 41 73 72 66
FAX: +33 (0) 2 41 73 70 66
E-Mail: srv.Duplicopy@bull.net

CEDOC Reference #	Designation	Qty
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
[_ _] : The latest revision will be provided if no revision number is given.		

NAME: ______________________________ Date: ____________

COMPANY: ______________________________

ADDRESS: ______________________________

____

PHONE: ____________________ FAX: ____________________

E-MAIL: ______________________________

For Bull Subsidiaries:

Identification: ______________________________

For Bull Affiliated Customers:

Customer Code: ______________________________

For Bull Internal Customers:

Budgetary Section: ______________________________

For Others: Please ask your Bull representative.

BLANK

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

REFERENCE
86 A1 06EW 00