IBM

System i

System i integration with BladeCenter and System x: iSCSI-attached System x and blade systems

Version 6 Release 1

IBM

System i

System i integration with BladeCenter and System x: iSCSI-attached System x and blade systems

Version 6 Release 1

> **Note**
>
> Before using this information and the product it supports, read the information in "Notices," on page 251.

Contents

What's new for V6R1

Read about new or significantly changed information for the System i® integration with BladeCenter® and System x™ topic collection.

Changes to iSCSI-attached integrated servers

- The hardware resource name is now configured by specifying the Network Server Host Port resource name which is in the form CMN*xx* by default.

  Note: For i5/OS® V5R4, the resource names were configured in the form LIN*xx*. If you are upgrading from i5/OS V5R4 to V6R1, Network Server Host Adapter (NWSH) device descriptions are not automatically reconfigured. Configure the NWSH to point to the new resource name before you use it. See "Creating an NWSH object for each new System i iSCSI HBA port" on page 110 for information about finding the resource name.

- Shared data memory pools are supported on iSCSI-attached integrated servers. Use this function to isolate iSCSI I/O operations from other i5/OS I/O operations.

  Note: If you are upgrading from i5/OS V5R4, shared data pools replace the private memory pool. Configure shared data memory pools for the integrated servers.

  See "iSCSI virtual I/O shared data memory pool" on page 61.

- iSCSI-attached integrated servers support both target and initiator CHAP. See "Configuring CHAP for integrated servers" on page 215.

- iSCSI direct connect allows the target and initiator iSCSI HBAs to connect without a network switch.

Changes to integrated Windows® servers

- Windows Server 2008 x64 editions are supported on qualified iSCSI-attached integrated servers. See

  BladeCenter and System x models supported with iSCSI .

- Support for backing up active iSCSI-attached integrated Windows servers is added. See "Using i5/OS to back up disks for active integrated Windows servers" on page 154.

- Use the Disable User Profile (DSBUSRPRF) value on the Install Windows Server command or the Network Server Description to specify that user profiles will not be disabled on the Windows operating system when they are disabled on the i5/OS operating system. See "User and group concepts for iSCSI-attached integrated servers" on page 45.

- A new value for time synchronization is supported. Specify None to ensure that the integrated server time is never synchronized with the i5/OS time. See "Configuring time synchronization for integrated servers" on page 109.

VMware ESX Server is supported on iSCSI-attached integrated servers

VMware ESX Server is supported on iSCSI-attached integrated server hardware. See "Installing, configuring, and managing VMware ESX Server in iSCSI-attached integrated server environments" on page 165.

Changes to integrated Linux® servers

- SUSE Enterprise Linux Server 10 for AMD64 and Intel® EM64T (SLES 10) and Red Hat Enterprise Linux 5 for x86-64 (RHEL 5) are supported on iSCSI-attached integrated Linux servers.

- iSCSI-attached Linux servers now support file-level backup from the i5/OS operating system. See "Backing up and recovering individual integrated Linux server files and directories" on page 187.

1

- Support is added for backing up active Linux servers. See "Backing up storage spaces for an active integrated Linux server" on page 185.
- A new value for time synchronization is supported. Specify None to ensure that the integrated server time is never synchronized with the i5/OS time. See "Configuring time synchronization for integrated servers" on page 109.

Changes to IXS and IXA-attached integrated Windows servers

- Use the Disable User Profile (DSBUSRPRF) value on the Install Windows Server command or the Network Server Description to specify that user profiles will not be disabled on the Windows operating system when they are disabled on the i5/OS operating system. See User and group concepts for integrated Windows servers.
- A new value for time synchronization is supported. Specify None to ensure that the integrated server time is never synchronized with the i5/OS time. See Configuring time synchronization for integrated Windows servers.
- The Windows Server Installation Advisor no longer supports IXS and IXA-attached integrated servers. Use the Installation worksheet for i5/OS parameters to select parameters for the Install Window Server (INSWNTSVR) command.

Support withdrawn for Linux running on IXS and IXA-attached hardware

At V6R1, integrated Linux servers are supported only on iSCSI-attached hardware. Linux installations are not supported on IXS or IXA hardware.

The i5/OS operating system will allow migration from V5R4 to V6R1 for Linux servers running on IXS or IXS-attached hardware. However, the IXS/IXA integrated server function for Linux will be limited and will not be serviced in V6R1. For more information, see the Linux on integrated servers Web site (www.ibm.com/systems/i/bladecenter/linux/).

For information about integrated Linux servers for IXS and IXA-attached hardware, see the Linux on an integrated xSeries® solution topic collection in the V5R4 i5/OS Information Center.

Changes to System i integration with BladeCenter and System x information

In V6R1, all information for installing and configuring an iSCSI-attached integrated server is contained in one topic collection. The following information has been merged into this topic:
- Installation steps from iSCSI install read me first Web page
- *iSCSI Host Bus Adapter for IBM® BladeCenter, System x, or xSeries* topic collection from the IBM Systems Hardware Information Center
- *iSCSI Network Planning Guide* from the iSCSI install read me first Web page
- *Linux on an integrated xSeries solution* topic collection from the V5R4 i5/OS Information Center
- *Windows environment on iSeries®* topic collection from the V5R4 i5/OS Information Center

At V6R1, the information is categorized by hardware type. See "iSCSI-attached System x and blade systems" on page 5 and IXS or IXA-attached integrated Windows servers.

What's new as of 14 November 2008

The following information is updated:
- Changes to iSCSI initiator configuration topics.
- Changes to the Service Processor Manager function of i5/OS Integrated Server Support to perform discovery and control power for iSCSI-attached servers. See "Configuring i5/OS to use Service Processor Manager" on page 107 for details.

What's new as of 26 August 2008

The following information is updated:
* Changes to Windows Server 2008.
* Additions and corrections to the iSCSI-attached server installation information.

How to see what's new or changed

To help you see where technical changes have been made, the information center uses:
* The ≫ image to mark where new or changed information begins.
* The ≪ image to mark where new or changed information ends.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what's new or changed this release, see the Memo to users.

iSCSI-attached System x and blade systems

You can integrate System x or blade systems using the integrated server support option and supported iSCSI hardware.

Concepts for iSCSI-attached integrated servers

Understand concepts for iSCSI-attached servers for the System i integration with BladeCenter and System x solution.

Integrated server overview

An integrated server is a combination of integrated server hardware, network components, virtual disks, shared devices, and i5/OS integrated server configuration objects.
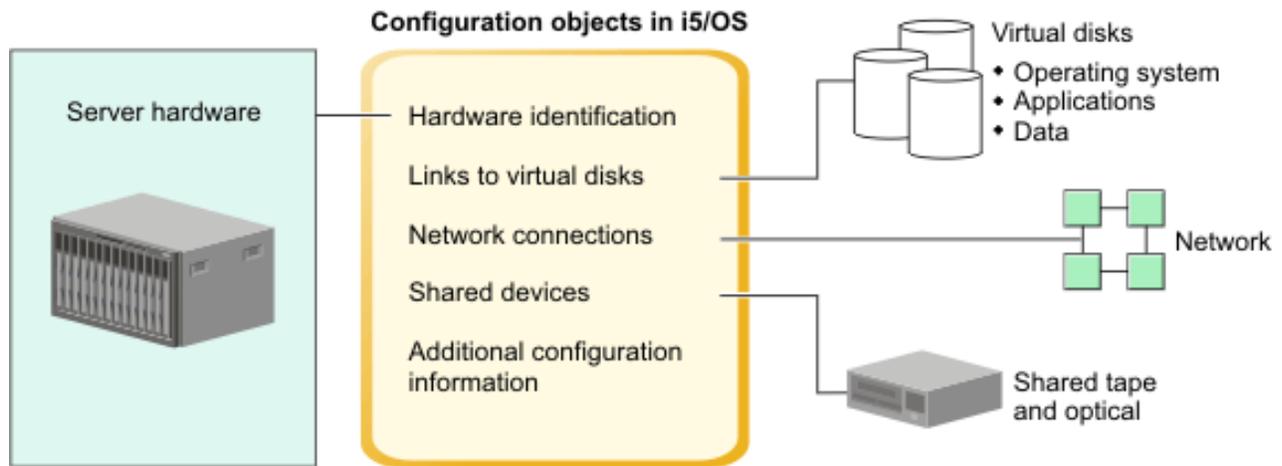
Figure 1. Integrated server overview

Server hardware

The server hardware is the physical hardware (such as the processor and memory) that the integrated server runs on. There are several types of server hardware that can be used for integrated servers, depending on your needs. The integrated server hardware is an external System x or BladeCenter product that is attached to a System i product with an iSCSI host bus adapter. The integrated server can also use tape and optical devices that are connected to the hosting i5/OS partition. See "iSCSI-attached integrated server overview" on page 7 for more information about the types of hardware that can be used for integrated servers.

Network

Each integrated server has one or more connections to a network. Both physical network connections with a network adapter and System i virtual Ethernet network connections are supported. See "Networking concepts for integrated servers" on page 23 for more information about the types of network connections that can be used with integrated servers.

5

Virtual disks

Each integrated server uses virtual disks that contain the integrated server operating system, applications, and data. These virtual disks are allocated from i5/OS disk storage. The integrated server treats these drives as physical disk drives that are contained within the server. However, the integrated server does not actually have any physical disk drives of its own. See "Storage management for integrated servers" on page 15 for more information about virtual disks.

Shared devices

Shared devices include all supported tape drives and optical devices that the integrated server can access as if they were local to the integrated server. By default, all System i tape and optical devices are automatically accessible by the integrated server. You can choose to restrict which of these System i devices the integrated server can access.

i5/OS integrated server configuration objects

Configuration objects in i5/OS describe each integrated server. The i5/OS configuration objects identify the hardware that the integrated server runs on, the virtual disk drives that the integrated server uses, the virtual Ethernet connections that the integrated server uses, and many other attributes of the server. See "Software concepts and configuration objects for iSCSI-attached integrated servers" on page 40 for more information about the i5/OS configuration objects that describe an integrated server.

Integrated server capabilities

Integrated servers allow you to run supported versions of the Windows, Linux, or VMware operating systems while taking advantage of System i capabilities such as storage management, high availability, and user propagation solutions.

There are fewer pieces of hardware to manage requiring less physical space. iSCSI-attached integrated servers can take advantage of BladeCenter hardware.

Greater accessibility and protection for your data

- Integrated servers use System i disk storage, which is generally more reliable than PC server hard disks.
- iSCSI-attached servers allow you to run x86 Windows Server 2003 or AMD64 and Intel EM64T versions of Linux, Windows Server 2008, and VMWare ESX server.
- You have access to faster System i tape devices for integrated server backups.
- You can back up the entire integrated server as part of your System i server backup. This allows you to recover a failed server much faster and easier than with typical file level recovery on the integrated server operating system.
- Integrated servers implicitly take advantage of superior data protection schemes which exist in i5/OS such as RAID or drive mirroring.
- Typical integrated server configurations have storage space data spread across more System i disk drives than would be configured in standalone (non-integrated) server installations. This can frequently provide better peak disk I/O capacity, since each server is not constrained to few dedicated drives.
- You can add additional disk storage to integrated servers without shutting down the server.
- It is possible to gain access to DB2® for i5/OS data through an enhanced Open Database Connectivity (ODBC) device driver using System i Access. This device driver enables server-to-server applications between integrated servers and i5/OS.
- You have the ability to use an integrated server as a second tier in a three-tier client/server application.
- Virtual networking for integrated Windows servers does not require additional LAN hardware and provides communications between System i logical partitions, Integrated xSeries Server (IXS)s, Integrated xSeries Adapter (IXA)s, and iSCSI HBAs.

Simplified administration

- Your computer system is less complicated because of the integration of user administration function, security, server management, and backup and recovery plans between the i5/OS and integrated server operating systems.. You can save your integrated server data on the same media as other i5/OS data and restore individual files as well as i5/OS objects.
- For integrated Windows servers, user parameters, such as passwords, are easier to administer from i5/OS. You can create users and groups and enroll them from i5/OS to integrated servers. This makes updating passwords and other user information from i5/OS easy.

Remote management and problem analysis

- You can sign on to i5/OS from a remote location and shut down or restart your integrated server.
- Since you can mirror integrated server event log information to i5/OS you can remotely analyze Microsoft® Windows errors.

Multiple servers

- Integrated Windows servers and logical partitions running on the same System i have high-performance, secure virtual networking communications that do not require using LAN hardware.
- You can run multiple integrated servers on a single System i product. Not only convenient and efficient, this also gives you the ability to easily switch to another up-and-running server if the hardware fails.
- If you have multiple integrated servers installed on your System i product, you can define their Windows domain roles in a way that will simplify user enrollment and access. For example, you might want to set up one of these servers as a domain controller. Then, you only have to enroll users to the domain controller, and users can log on from any Microsoft Windows machine on that domain.
- A System i product's optical and tape drives can be shared with integrated servers.

Hot spare support

- Server integration and storage virtualization provide innovative options that can enhance the reliability and recoverability of the integrated server environment.
- If the integrated server hardware fails, you can quickly and easily switch the server's configuration to hot spare System x or BladeCenter hardware without restarting your System i product. This may reduce the overall number of PC servers needed to provide increased availability.
- Hot spare support also adds flexibility by enabling one spare server to be used to protect multiple production servers.

iSCSI-attached integrated server overview

A basic iSCSI network consists of an iSCSI target (an iSCSI HBA that is installed on a System i product) and an iSCSI initiator (an iSCSI HBA or Ethernet Network Interface Card (NIC) that is installed on a System x or IBM BladeCenter system).

The target and initiator devices are connected over an Ethernet local area network (LAN). The iSCSI target for System i provides the storage and removable media devices for the iSCSI initiator. Figure 2 on page 8 illustrates a basic iSCSI network.

RZAHQ509-3
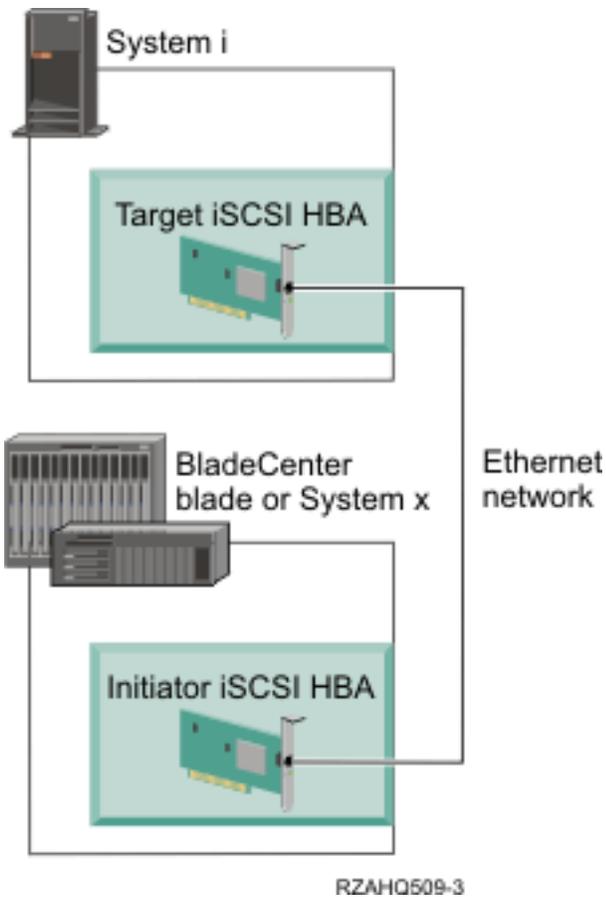
Figure 2. Basic iSCSI network

You need to configure both the iSCSI target and initiator adapters with i5/OS commands. The iSCSI
network is used for iSCSI traffic only.

Typical iSCSI-attached System x or BladeCenter system installation

iSCSI-attached servers are standard System x or IBM BladeCenter models that have processors, memory,
and expansion cards, but no physical disks. Integrated servers use virtual disks on the System i product
that are managed by the i5/OS operating system.

The installation procedure for an iSCSI-attached integrated server requires hardware to be installed and
configured in both the System i and System x or BladeCenter products. You can use the System x
expansion slots for additional options.

The following graphic illustrates a typical iSCSI HBA installation:
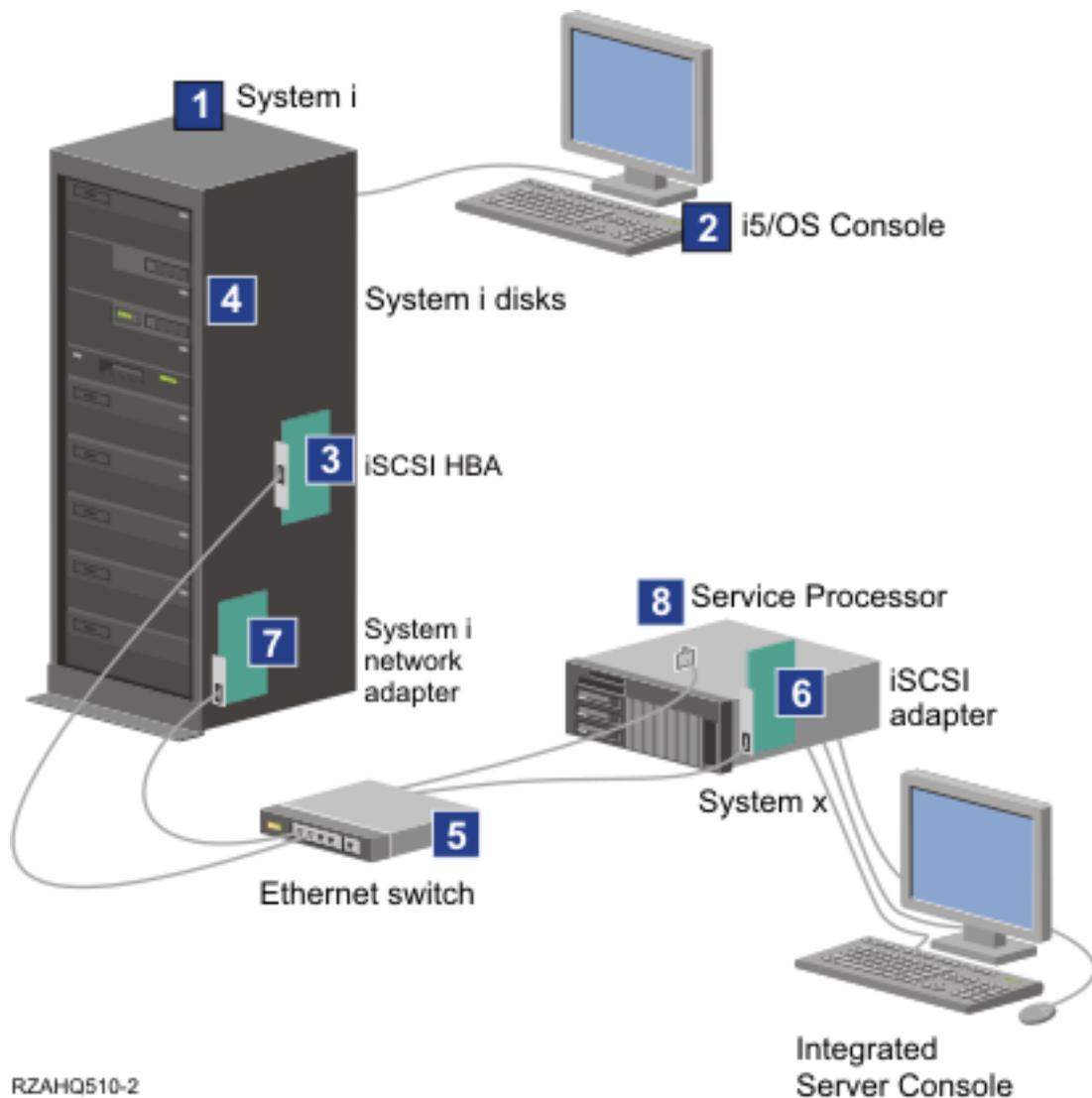
Figure 3. A typical iSCSI-attached server or BladeCenter installation

1. You need a compatible System i model. See "Planning for iSCSI-attached integrated servers" on page 54 for compatibility information.
2. The i5/OS console, from which you connect to the System i product using System i Navigator or the character-based interface, is shown to make clear the distinction between it and the integrated server console.
3. Depending on the type of the physical network, copper or fiber iSCSI HBAs are available. This iSCSI HBA installed in the System i model is the target device and connects to an Ethernet network using standard Ethernet cables.
4. An integrated server does not have its own physical disk drive. The i5/OS operating system emulates hard disk space for it to use from System i disks. These disks and other System i storage devices are accessed through the iSCSI HBA.
5. The iSCSI HBA network cables are connected to a standard Gigabit Ethernet switch.
6. An additional iSCSI HBA is required in the System x blade hardware. This adapter provides the connection to target iSCSI HBA in the System i model. This adapter can be viewed from the System x or blade model as the storage adapter, where the disks are found across the network.

7. A typical System i product has a network card. A System i LAN connection is required to discover and manage the System x or BladeCenter hardware.

8. A service processor allows the System i product to discover and manage the system. The service processor may be a Remote Supervisor Adapter (RSA II), a Baseboard Management Controller (BMC), or a Management Module of a BladeCenter system. The RSA II, BMC, or Management Module is connected to the System i product over an Ethernet network.

For more information about hardware, see the System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/) Web site.

Single-server environment

A basic iSCSI-attached integrated server configuration requires iSCSI host bus adapters (HBAs) and i5/OS configuration objects.

The simplest form of the physical connection between an initiator system and a System i product is illustrated in Figure 4 on page 11.
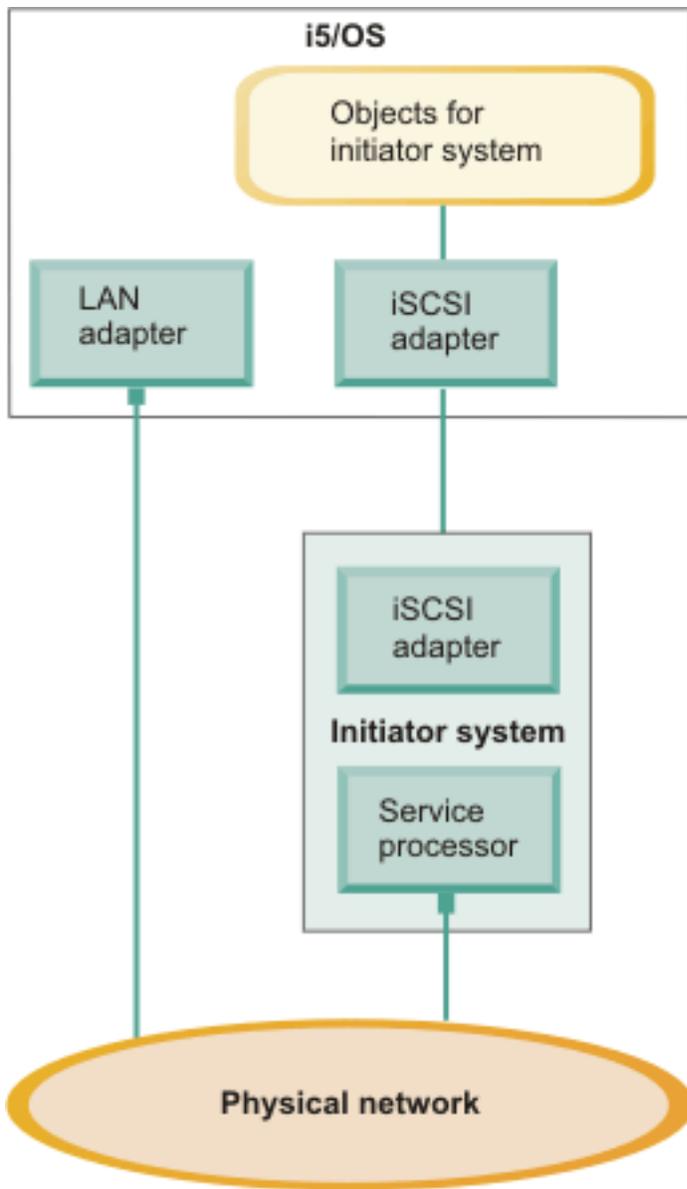
Figure 4. Single iSCSI-attached server

An iSCSI host bus adapter (HBA) is installed in each system. The Ethernet network between the HBAs is known as the iSCSI network. The initiator system (System x or BladeCenter system) uses this network to access storage through the target iSCSI HBA that is installed in the System i product.

The initiator system has no physical disks and connects to virtual disks and virtual removable media devices on the System i product. The SCSI commands to access these devices are packaged in TCP/IP frames and travel over an Ethernet network from the initiator system to the target iSCSI HBA that is installed in the System i. This mode of communication is known as Internet SCSI or iSCSI.

The iSCSI-attached servers are configured in i5/OS objects. For more information about these objects, see "Software concepts and configuration objects for iSCSI-attached integrated servers" on page 40.

The i5/OS operating system can locate and manage remote systems by sending commands to the service processor of the remote (initiator) system over an Ethernet network. For more information, see "Service processor functions and support" on page 24.

Two distinct networks are illustrated in "Single-server environment" on page 10. The iSCSI network uses an isolated switch or a direct connection. The service processor connection uses an external network (shared network).

Two distinct networks are not required. For example, the service processor connection can use the same isolated switch as the iSCSI network. This is one way to secure the service processor connection. However, the System i LAN adapter would not be available for other applications on the external network.

Both types of networks should be secured. For more information about security for iSCSI-attached servers, see "Network security for integrated servers" on page 35.

Multiple-server environment

You can use one target iSCSI HBA in the System i product to host multiple initiator (System x or blade) systems.

This concept is illustrated in Figure 5 on page 13.
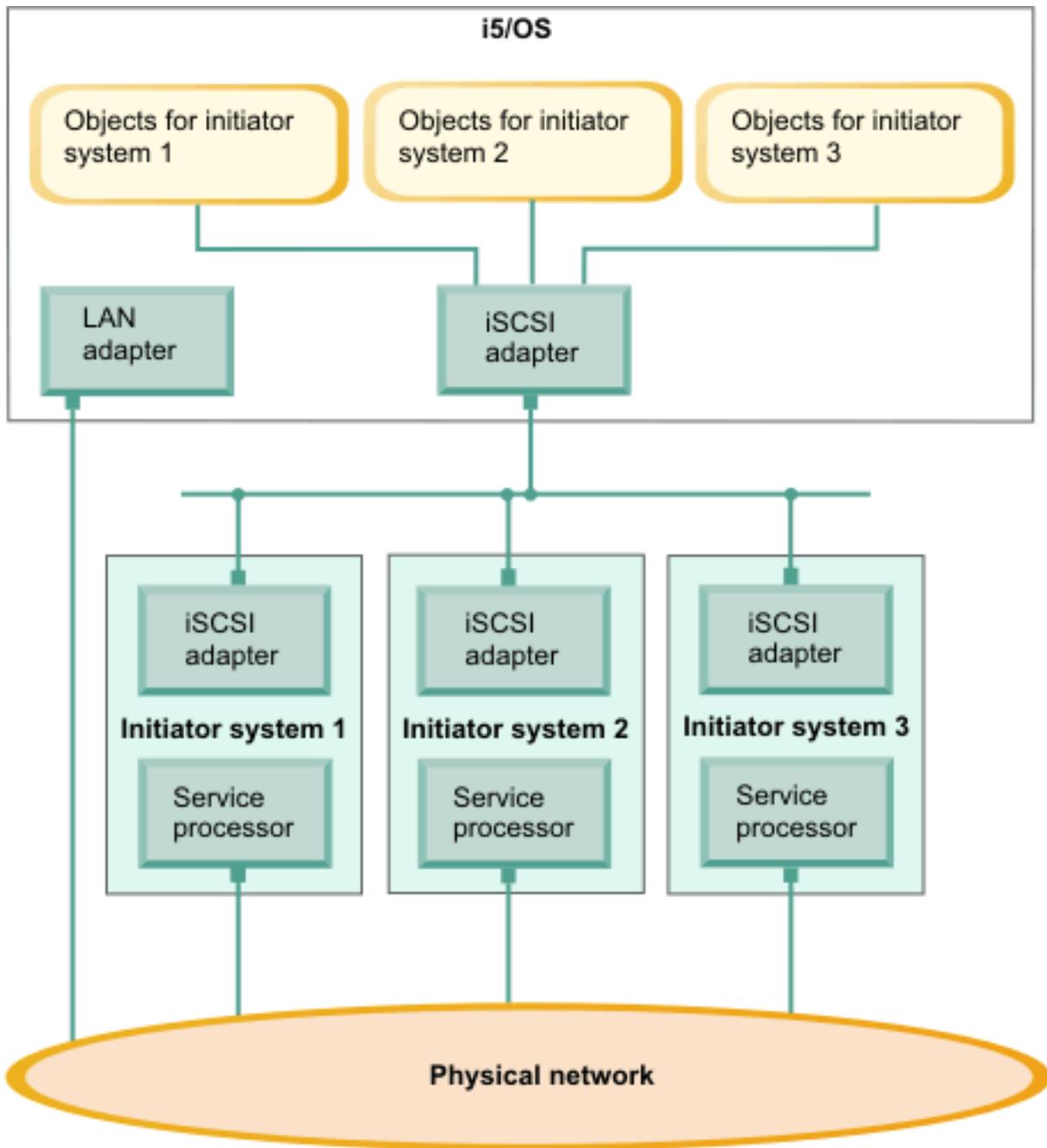
Figure 5. Multiple iSCSI-attached servers

The horizontal line in the diagram between the iSCSI adapters represents a switch. A switch is required when more than one initiator iSCSI HBA share a single target iSCSI HBA.

You must install an initiator iSCSI HBA in each hosted System x or blade product. The iSCSI HBAs are connected by an Ethernet network. This network can be a physically secure or isolated network when a physically secure model is implemented. Each initiator system is represented by a set of i5/OS objects. For more information, see "Software concepts and configuration objects for iSCSI-attached integrated servers" on page 40.

Each initiator system must have a service processor installed for remote discovery and power management. Multiple service processors can be connected to a single i5/OS LAN adapter over an external network.

Two distinct networks are not required. For example, the service processor connection can use the same isolated switch as the iSCSI network. This is one way to secure the service processor connection. However, the System i LAN adapter would not be available for other applications on the external network.

Initiator system and service processor discovery

The i5/OS operating system uses either the Service Processor Manager of i5/OS Integrated Server Support or IBM Director Server to locate System x or BladeCenter hardware on the network, to turn the initiator system hardware on and off, and to retrieve power status.

Initiator systems are identified by information stored in the remote system configuration and the service processor configuration objects in the i5/OS operating system.

This is a different connection than the iSCSI network connection between the System i iSCSI target adapter and the iSCSI initiator adapter in the initiator system. The LAN adapter for the service processor of the remote server must be attached to a network that is reachable by a LAN adapter that is installed in the System i hardware.

Both the i5/OS objects and the service processor must be configured. You can configure the discovery method used in the i5/OS network server configuration objects.

Related tasks

"Configuring initiator system discovery and management" on page 228
Use the information from the i5/OS remote system configuration and service processor configuration objects to locate and manage the hardware of iSCSI-attached System x and blade integrated servers.

Boot modes and parameters

iSCSI-attached integrated server hardware is diskless. The boot device is a port configured on the initiator iSCSI HBA installed in the System x or blade hardware.

Both the i5/OS remote system configuration and the initiator iSCSI HBA must be configured before you install or use a new integrated Windows server. See "Remote system configuration" on page 42.

Boot modes and parameters

Boot parameters for an iSCSI initiator are configured with an iSCSI initiator configuration function. Boot parameter values must match the values in the i5/OS remote system configuration object. The parameters vary depending on the selected boot mode.

See "Planning for iSCSI-attached integrated servers" on page 54 for information about configuring the iSCSI initiator port as the iSCSI boot device. See "Changing remote system configuration properties" on page 210 for information about changing parameters for the remote system configuration object.

Enabling the hosted server boot device

The initiator iSCSI HBA installed in the System x or blade hardware acts as a boot device during the boot process, based on the configured parameters.

You must configure at least one port on the iSCSI initiator HBA as a boot device.

Integrated server console

The integrated server console is a direct interface to the integrated server operating system.

Depending on your configuration of hardware and software, you can use a monitor, keyboard, and mouse that are attached by one of the following methods:

Directly attached monitor, keyboard, and mouse
> You can use a monitor, keyboard, and mouse that are directly connected to the System x or BladeCenter product. You interact with the integrated server through these devices exactly as you would with a regular personal computer (PC).
>
> A directly attached monitor, keyboard, and mouse are required for some iSCSI HBA configuration tasks.

Remote GUI desktop application
> You can use an application such as Microsoft Terminal Services, Remote Desktop, or another third party application to display the integrated server graphical user interface (GUI) desktop on a remote workstation. Most administration tasks that are normally performed on the server's directly attached console can be performed on the remote desktop. See the Microsoft Terminal Services or other third party application documentation for information about how to configure and use a remote desktop for the server console.

Remote Supervisor Adapter II graphical console redirection
> For System x products equipped with an RSA II service processor, the RSA II also provides full hardware-based graphical console redirection, which means you can use a local desktop to access and control a remote server.

Blade center Management Module (MM) or Advanced Management Module (AMM) graphical console redirection
> A BladeCenter enclosure (chassis) uses either a Management Module (MM) or an Advanced Management Module (AMM) which provides hardware-based graphical console redirection and allows a remote to access and control a remote server using a Web browser interface enabled for Java.

Storage management for integrated servers

Integrated servers use virtual disks that are managed by the i5/OS operating system.

Virtual disks for integrated servers

Integrated servers use virtual storage provided by i5/OS instead of physical hardware attached to the integrated server hardware.

Operating systems, such as Windows, Unix and Linux, work with what they see as physical disk drives; there is little or no virtualization of storage at an operating system level. Because i5/OS virtualizes all disk storage, you can use chunks of disk space from the storage pool to form virtual disk drives, which can then be allocated to the integrated server operating system. These virtual disks are also known as storage spaces. Integrated Linux, VMware and Windows servers, as well as AIX® 5L and Linux running in System i partitions, see these storage spaces as physical disk drives.

Important: Because virtual disks, as seen by integrated servers, are physically scattered over all disk drives in the ASP, you can create disks as large as 1 TB if there is available storage in the specified ASP.

The i5/OS object that is used to create a virtual disk for an integrated server is called a Network Server Storage Space (NWSSTG), or storage space for short. These storage spaces are stored in the root of the i5/OS integrated file system (IFS) in a directory called /QFPNWSSTG. You can use the Work with Links (WRKLNK) command from an i5/OS command line to view the contents of the /QFPNWSSTG directory. This storage space architecture is used by integrated Windows, VMware and by Linux servers and Linux and AIX 5L™ running in System i logical partitions. Storage spaces can be interchanged between each of these different operating systems.

The amount of disk storage that you create for your servers is taken directly from the System i available storage, and each virtual disk is physically scattered across the physical disks in the System i disk pool.

Storage spaces are different from other i5/OS file objects because the size that you specify for a storage space is completely allocated at the time it is created. This is because integrated servers need to be able to connect to and format a drive of a fixed size.

It is a good idea to make a backup of the system drive before and after you make changes to the operating system. If something should happen, you can recover by restoring a backup of the system drive, rather than rebuilding the server from scratch. In order to recover quickly from a system failure, you should not store user files on the system or installation drives. Files and data that change frequently should be stored on a different drive.

Before you start creating new drives for your server, take some time to calculate what the server needs now and in the future. After the server has been installed you can create additional drives for your integrated server at any time. These drives can be linked to the server while it is shut down (static linking) or started (dynamic linking). This means that you do not need to allocate large portions of your System i storage when the server is created; you can create additional drives of any size you wish (up to the limit) when they are needed.

Here is a summary of the operations that you can perform on integrated server virtual disks:
- Create a new disk
- Delete a disk
- Link a disk
- Unlink a disk
- Clone a disk
- Expand a disk

Disk operations can be performed in these ways:
- Using System i Navigator or IBM Systems Director Navigator for i5/OS
- Using CL commands.

i5/OS storage management for integrated servers
Integrated servers use virtual disks that are managed by the i5/OS operating system.

This brief overview of i5/OS storage management concepts is intended for administrators who are more familiar with how x86-based servers manage storage. Some techniques, such as defragmenting, are not necessary in an integrated server environment.

i5/OS and disk drives

The i5/OS operating system does not directly manage disk drives. Beneath the operating system a level of software (called Licensed Internal Code) "hides" the disk drives and manages the storage of objects on those disk drives. A virtual address space is mapped over the existing disk space and used for addressing objects rather than disk drive IDs, cylinders, and sectors. Needed objects are copied ("paged in") from this address space on disk into the address space of main memory.

Because of the way i5/OS manages disk data, you do not generally need to worry about partitioning high-growth databases, defragmenting disks, or disk striping on your integrated server. The integrated server uses device drivers to share the i5/OS disk drives. These device drivers send and receive disk data to the i5/OS storage management subsystem. i5/OS storage management handles the hard disks, including spreading the integrated server disk drive images across multiple hard disk drives and applying RAID and file mirroring (if configured). Disk defragmentation software manages logical file fragmentation of the hard disk images. Because i5/OS storage management handles these tasks, running

a defragmentation program on the integrated server helps primarily in cases where "critical file system structures" can be defragmented.

Disk pools (ASPs)

In i5/OS physical hard disk drives are pooled together into one storage space called a disk pool, also called an auxiliary storage pool (ASP). If your file system runs out of space, you can add a new hard disk drive to the disk pool, and the new storage space will be available immediately. Every system has at least one disk pool, the system disk pool. The system disk pool is always ASP 1. You can configure additional *user* disk pools, numbered 2 - 255. You can use disk pools to distribute your i5/OS data over different groups of disks. You can also use this concept to move less important applications or data to your older, slower disk drives. Support for independent ASPs (33-255) is provided through System i Navigator. Both the Information Center and System i Navigator refer to ASPs as Disk Pools.

Disk protection

i5/OS disks can be protected in these ways:

- **Cross-site mirroring:** Cross-site mirroring, using the operating system geographic mirroring function for independent ASPs, mirrors data on disks at sites that can be separated by a significant distance.
- **RAID-5:** The RAID-5 technique groups several disks together to form an array. Each disk holds checksum information of the other disks in the same array. If a disk fails, the RAID-5 disk controller can re-create the data of the failing disk with the help of the checksum information about the other disks. When you replace a failing disk with a new one, i5/OS can rebuild the information from the failed disk on the new (and therefore empty) disk.
- **Mirroring:** Mirroring keeps two copies of data on two different disks. The i5/OS operating system performs write operations on both disks at the same time, and can simultaneously perform two different read operations on the two disks of a mirrored pair. If one disk fails, i5/OS uses information from the second disk. When you replace the failing disk, i5/OS copies the data from the intact disk to the new disk.

To further increase the level of protection, you can attach the mirrored disks to two different disk controllers. Then if one controller fails, and with it one set of disks, the other controller can keep the system up. On larger System i models, you can attach controllers to more than one bus. Attaching the two disk controllers that form a mirrored pair to two different buses increases availability even more.

You can define disk pools on i5/OS to have different levels of protection or no protection at all. Then you can put applications and data into a disk pool with the right amount of protection, depending on how important their availability is. For more information about i5/OS disk protection and availability options, see the Recovering your system topic collection.

When the integrated server operating system is running, it uses a portion of the System i disk capacity. For this reason, the administration of integrated server storage has both an i5/OS component and an integrated server operating system component. The i5/OS component is used to create and link a chunk of storage to the integrated server. Many of the common disk administration tasks encountered in stand-alone PC servers (disk drivers, addressing, configuration and protection) are eliminated when you use an integrated server.

Disk storage administration tasks such as formatting and partitioning can be performed on integrated servers in exactly the same way as they are on stand-alone servers.

The key to understanding how disk storage is allocated to integrated servers is an understanding of how i5/OS storage management works on the System i platform. The heart of storage management on the System i platform is a technology called single-level storage. Single-level storage is a revolutionary storage management architecture that not only gives the System i platform outstanding disk I/O performance, but greatly reduces the amount of administration required.

The major features of single-level storage are:

- Single storage pool

  The management of physical disk drives is implemented in the Licensed Internal Code, which is similar in concept to the BIOS on a PC.

  By default, the operating system and applications see only a single large pool of virtual storage (called the System Auxiliary Storage Pool or system ASP) rather than physical drives. Therefore, the management of physical storage is hidden from the user.

  To increase the size of the pool, simply add disk drives to the System i product and they automatically become part of the system ASP. Note that under some circumstances you might create additional storage pools that are called user ASPs and independent ASPs.

- Scattering of data

  Instead of an object being stored on a single physical disk drive, single-level storage scatters objects across all physical drives, transparently to the user.

  System i disk management supports fully parallel disk I/O, which provides outstanding disk I/O performance because each object on the system is accessible by multiple disk arms concurrently.

  There is no need to be concerned about particular disk drives filling up, or moving data from one disk to another to improve performance because all data management is taken care of by the licensed internal code. Therefore, the System i product does not require a Database Administrator. Licensed internal code also ensures that there is no disk fragmentation.

- Single address space

  Memory and disk on the System i product form a single 64-bit address space.

  A single address space enables objects to be accessed by name rather than hardware address, which provides additional integrity and reliability.

Predefined disks and naming conventions for integrated servers

Predefined disks are automatically created when you install the integrated server operating system. The system uses these disks for the integrated server support code and the operating system.

By default, i5/OS creates these disks in the system disk pool (ASP), but you can choose a different location during the installation. i5/OS also uses these disks to load and start the integrated server.

Predefined disks and naming conventions for integrated Windows servers

Integrated Windows servers have these predefined disks:

Boot and system drive (C)
> This drive serves as the system drive. i5/OS names this drive *server*1, where *server* is the name of the network server description (NWSD). This disk drive resides in the integrated file system and is automatically linked as the first drive.
>
> The C drive ranges from 1,024 to 1,024,000 MB.
>
> **Note:** If you plan to create NWSD configuration files, be aware that support for these files exists only for disk drives that are formatted as FAT or FAT32. See "Network server description configuration files" on page 238. A system drive that has been converted to NTFS is not accessible for NWSD configuration files. For more information about the different file systems, see Comparison of FAT, FAT32, and NTFS file systems.

Installation source drive (D)
> The D drive can be 200 - 2,047 MB and holds a copy of the Windows server installation code and the IBM i5/OS Integrated Server Support code. i5/OS names this drive *server*2, where *server* is the name of the NWSD. This disk drive resides in the integrated file system and is automatically linked as the second drive. i5/OS formats the D drive as a file allocation table (FAT) disk.
>
> **Attention:**

1. This drive must remain as a FAT drive. Do not make any changes to this drive. i5/OS uses this drive to perform code updates, and changing the drive can make performing updates impossible.
2. Some third-party applications such as Citrix require that the drive letter for this drive be changed. This is supported as long as the drive remains linked to the server and has a FAT or FAT32 file system to allow configuration files to be written when the server is started.

Note: For more information about servers upgraded from pre-V4R5 i5/OS systems, see Predefined disk drives for integrated Windows servers in the V5R3 iSeries Information Center.

Predefined disks and naming conventions for integrated servers running VMware ESX server

The Install Linux Server (INSLNXSVR) command creates two disks for integrated servers running VMware ESX server. They correspond to the first two drives that the integrated server recognizes.

System disk (/dev/sda)
> The VMware ESX operating system is installed on this disk.
>
> You should allow at least 12288 MB for this disk, including 8192 MB for the operating system and 4096 MB for integrated server utilities and other applications.

Installation drive (dev/sdb)
> This disk contains integrated server utilities that will be used during the server installation process and for integrated server function. Do not use it for other functions.
>
> You should allow at least 1024 MB for this disk.

Do not configure virtual machines on the system or installation disk. Create additional storage spaces and link them to the server for your virtual machines. For most environments, you can configure one virtual machine per storage space to simplify backup and other administration tasks.

Predefined disks and naming conventions for integrated Linux servers

The Install Linux Server (INSLNXSVR) command creates two disks. These disks are used to store the Linux operating system (called the system disk) and some IBM-supplied drivers (called the installation disk).

It is not possible to rename these disks directly. You must copy them and then supply a new name to the copy. However, it is rarely necessary to rename these two disks since the names are clearly associated with the NWSD for the server.

System disk (/dev/sda)
> This is the first disk that is linked to the integrated server. The Linux operating system is installed on this disk.
>
> The default value is calculated based on the space required to hold the Linux installation. Typically, a storage space of 12000 megabytes is created for the system disk. The size of the system storage space can be anywhere between 1024 MB and 1024000 MB. Depending on how much data you want to store on this disk, you might need to make it considerably larger. The system calculates a default value based on the space needed for the Linux system partition and the swap partition.
>
> **Linux system partition**
>> The estimate for the root and boot (if created) partitions with room for updates is 8 GB.
>
> **Swap partition**
>> This needs to be at least as large as the amount of installed memory. The system assumes that this is 4 GB.

Installation disk (dev/sdb)

> This disk resides in the integrated file system and is automatically linked as the second disk.

> The default size for this disk is calculated based on the space required to hold the integrated server files. Typically, a storage space of 1024 megabytes is created for the installation source disk. This virtual disk can be between 200 MB and 2047 MB. It does not need to be larger than the calculated value and it must be kept as *FAT format. The Linux integration code installs some utilities and configuration files here for its own use. The installation disk is not intended for general use.

Be careful about specifying a system disk size less than the calculated value. While this might work initially, over time as you install more distribution updates you might run out of space.

Storage space linking for integrated servers

Integrated servers do not use physical disks. i5/OS creates virtual disks (network server storage spaces) within its own file system and integrated servers use them as if they were normal physical disk drives.

To add a virtual disk to an integrated server, you create the disk, link it to the server, and then format it for the integrated server operating system.

iSCSI-attached integrated servers recognize only dynamic disk links. The disk link sequence position is assigned dynamically at the time that the disk drive is linked to an active server. The disk link sequence position can be specified, but it is not used until the server is restarted. The integrated server can either be shut down or active when adding a dynamic disk drive link.

When dynamically linking a virtual disk to an active server, the new disk drive appears following all other linked disks.

The following table shows the i5/OS virtual disk features supported for various types of server network server descriptions (NWSDs.)

Table 1. Disk features supported

Feature	NWSD type[1] *ISCSI with OS type *WIN32	NWSD type *ISCSI with OS type *WIN64	NWSD type *ISCSI with OS type *LINUX64[2]
Number of dynamic links	63	63	64
Number of shared access type links	0	0	0[2]
Maximum number of virtual disks that can be linked to the server	63	63	64
Maximum capacity per virtual disk	1000 GB	1000 GB	1000 GB
Maximum total virtual disk capacity, assuming 1000 GB per disk	61.5 TB	61.5 TB	61.5 TB
Can link virtual disks while the server is active?	Yes, Exceptions: dynamic links 1-2	Yes, Exceptions: dynamic links 1-2	Yes[3], Exceptions: dynamic links 1-2
Can unlink virtual disks while the server is active?	Yes, Exceptions: dynamic links 1-2, disk cannot be part of a volume set, and disk cannot be a volume mounted in a directory	Yes, Exceptions: dynamic links 1-2, disk cannot be part of a volume set, and disk cannot be a volume mounted in a directory	Yes[4], Exceptions: dynamic links 1-2
Virtual disk format types allowed when linking	*NTFS, *FAT, *FAT32, *OPEN	*NTFS, *FAT, *FAT32, *OPEN	*NTFS, *FAT, *FAT32, *OPEN

Feature	NWSD type[1] *ISCSI with OS type *WIN32	NWSD type *ISCSI with OS type *WIN64	NWSD type *ISCSI with OS type *LINUX64[2]
Virtual disk access types allowed when linking	Exclusive update, shared update	Exclusive update	Exclusive update, shared update[2]
Disk links requiring exclusive update access type	All dynamic links	All dynamic links	Dynamic links 1-2

Note:

1. See the Create Network Server Description (CRTNWSD) command help text for a description of the NWSD types and the associated operating system (OS) types.

2. Up to 62 storage spaces for NWSDs with server type *ISCSI and OS type *LINUX64 can only be shared with other NWSDs with types *ISCSI and *LINUX64 with OS version *ESX3. The value for OS version is specified by the INSLNXSVR command.

3. Dynamic linking of storage for NWSDs with types *ISCSI and *LINUX64 with OS version *ESX3 requires that you manually rescan the storage adapter (initiator iSCSI HBA) from the VMware Virtual Infrastructure Client to allow the operating system to detect the storage.

4. Dynamic unlinking of storage is not supported for NWSDs with types *ISCSI and *LINUX64 with OS version *ESX3. The value for OS version is specified by the INSLNXSVR command.

Network server storage spaces can reside in either the i5/OS system disk pool (ASP 1) or a user disk pool. You can copy one disk to another to move it to a different disk pool.

Network server storage spaces are one of the two types of network storage that integrated servers use. Integrated servers can also access resources on i5/OS that an administrator has shared with the network by using i5/OS NetServer™.

After you create a storage space and link it to an integrated server, you must partition and format the disk using the standard utilities provided by the integrated server operating system.

Related tasks

"Adding disks to integrated servers" on page 230
Use these tasks to add a disk to an integrated server.

Virtual and optical devices that are shared between i5/OS and integrated servers

Integrated Windows and Linux servers can use tested System i tape and optical devices.

Only the i5/OS operating system or one integrated server can use the device at any time.

Related tasks

"Sharing devices between i5/OS and integrated Windows servers" on page 155
Use these tasks to configure an integrated Windows server to use i5/OS tape and optical devices.

"Configuring a System i tape drive for use by Linux" on page 180
This topic describes the tasks you need to perform to set up a System i tape drive for use by an integrated Linux server.

Multipath I/O for iSCSI-attached integrated servers running Windows or VMware ESX Server

Multipath I/O enables multiple storage connections and provides automatic failover between connections to ensure that storage is accessible in case of a hardware failure.

A single target iSCSI HBA installed in the System i product is capable of supporting several servers or hosted systems. Each initiator HBA in the System x or blade system is also capable of connecting to multiple target iSCSI HBAs.

You can configure the iSCSI environment to support multiple target iSCSI HBAs, multiple iSCSI initiator HBAs, and multiple storage connections.
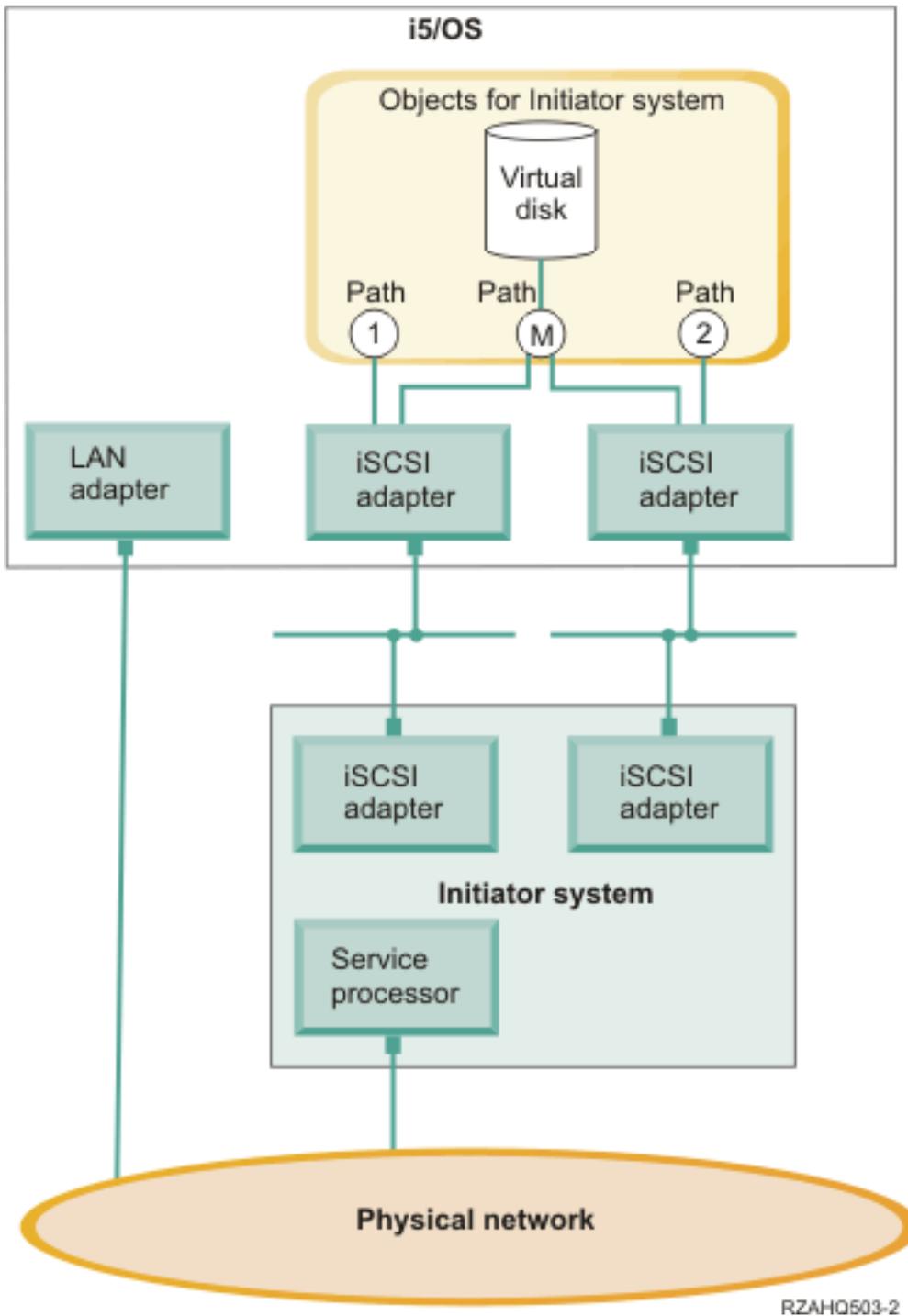
Figure 6. An environment with multiple iSCSI HBAs installed in the target and initiator systems

Paths

Paths are connection points between virtual devices and iSCSI HBAs in the System i product. A virtual device being hosted by i5/OS is said to be linked to a path. Initiator iSCSI HBA ports access the virtual device through the path.

System i virtual storage or devices are linked to a network server host adapter (NWSH) object. For example, a configured virtual disk (such as Drive C:) hosted in i5/OS is linked to the NWSH that represents the target iSCSI HBA adapter.

There are several storage paths defined in Figure 6 on page 22. The paths are labelled 1, 2 and M.

You can configure iSCSI-attached servers to use either a single path or a multipath group.

Multipath I/O and storage connection redundancy

A hosted system can use multiple iSCSI data paths to access virtual disks hosted by i5/OS.

You can configure a multipath group of two or more target iSCSI HBAs and then specify that a virtual disk be accessed using the multi-path group instead of a single iSCSI HBA. With this configuration, the data on the virtual disk can be accessed using any of the iSCSI HBAs in the multipath group.

In Figure 6 on page 22, the multipath group is defined as path M. The virtual disks that are linked to the multipath group can be accessed by any of the target iSCSI HBAs that are also linked to the multipath group. Only one multipath group can be defined per hosted system. This group can include up to four target iSCSI HBAs.

For the most reliable network you should do the following things:
- Configure multiple iSCSI targets in the System i product
- Configure multiple iSCSI initiators in the System x or blade product.
- Configure multiple switches
  - If you are using a BladeCenter system, you should configure multiple switch modules.
  - If you are using System x hardware, you should configure multiple switches in the iSCSI network.
- Link all storage to the multipath group

Note: Removable media devices cannot be defined in a multipath group.

The advantage of the multipath configuration is that, if there is a hardware failure, the hosted system can continue to access the disks that are configured to use the multipath group, using any of the iSCSI HBAs that are configured in the multipath group. This configuration can provide uninterrupted storage connections in case of a problem with a target iSCSI HBA, an initiator iSCSI HBA, or a switch.

See "Configuring multipath I/O for integrated servers" on page 192 for more information about installing the required software components and linking storage to the multipath group.

Networking concepts for integrated servers

iSCSI-attached integrated servers use several types of network connections.

Service processor connection for integrated servers

This physical connection is required so that the hosting i5/OS partition can communicate with the service processor of the initiator (System x or BladeCenter) system.

The connection can consist of a simple and switched network or a more complex and routed network.
i5/OS Integrated Server Support uses this connection to manage the state of the hosted system.

At one end of the connection is a LAN adapter or adapters that are controlled by the i5/OS operating system. This LAN adapter can be available for other uses. The IP address and other attributes of this adapter are controlled using standard i5/OS configuration methods. The i5/OS operating system does not configure this adapter. i5/OS can automatically discover the service processor using one or more i5/OS TCP interfaces that are already configured.

At the other end of the connection is the service processor. The service processor has its own Ethernet port and TCP/IP stack. This TCP/IP stack is active whenever the system power cord is plugged into an energized alternating current (ac) outlet, even if the system is not in a powered on state.

DHCP server for the service processor

If a unicast address is not configured for the service processor, an external DHCP server on the network providing the service processor connection can set the service processor IP address. The DHCP server should be active before plugging the hosted system's power cord into an energized alternating current (ac) outlet. (This DHCP server is distinct from the DHCP server that is built into the i5/OS side of the iSCSI network to assist with iSCSI boot of the integrated server operating system.) For more information, see "Dynamic addressing for service processors" on page 25.

IP multicast

There are several options that i5/OS offers for discovering the service processor. Note that the choices that provide the most automation require that the network support IP multicast. Some switches and networks do not support IP multicast by default. For more information, see "Service processor discovery for integrated servers" on page 26.

Performance and maximum transmission unit (MTU)

There is not a requirement or advantage to having a high speed network or using a large MTU for the service processor connection.

Security

The security capabilities of your service processor hardware may affect your decision to use an isolated network or a shared network to provide the service processor connection. For more information, see "Configuring security between i5/OS and integrated servers" on page 215.

> **Related tasks**
>
> "Configuring initiator system discovery and management" on page 228
> Use the information from the i5/OS remote system configuration and service processor configuration objects to locate and manage the hardware of iSCSI-attached System x and blade integrated servers.

Service processor functions and support

Use the information from the i5/OS remote system configuration and service processor configuration objects to locate and manage iSCSI-attached integrated servers.

Initiator systems are identified by information stored in the remote system configuration and the service processor configuration objects in the i5/OS operating system.

This is a different connection than the connection between the System i iSCSI target adapter and the iSCSI initiator adapter in the remote server. The LAN adapter for the service processor of the remote server must be attached to a network that is reachable by a LAN adapter that is installed in your System i hardware.

Both the i5/OS objects and the service processor must be configured. You can configure the discovery method used in the i5/OS network server configuration objects.

Dynamic addressing for service processors

A service processor using DHCP will initialize immediately when the server receives power and will start the DHCP process.

If an address cannot be obtained with DHCP, the service processor will use the default static IP address of 192.168.70.125.

Note: If the service processor fails to obtain an IP address with DHCP, the process can only be restarted by removing power and reapplying power.

Static addressing for service processors

The service processor is configured with a specific IP or host name.

Supported functions by service processor type

The configuration options depend on the type of service processor. For information about identifying the type of service processor in your System x product, see BladeCenter and System x models supported with iSCSI (www.ibm.com/systems/i/bladecenter/iscsi/servermodels/index.html)

Baseboard Management Controller (BMC)

The BMC service processor is available in some System x models.
- To configure the BMC, use the system BIOS setup menu
- The BMC supports static IP addressing.
- The BMC supports discovery by IP address. See "Configuring service processor discovery by IP address for integrated servers" on page 229.
- The BMC supports security using a password. See "Changing a service processor password for an integrated server" on page 216.

Remote Supervisor Adapter II (RSA II)

The RSA II service processor is available in some System x models.
- To configure the RSA II, do one of the following.
  - Use the system BIOS setup menu. This method cannot be used to configure a host name.
  - See "Configuring the integrated server Management Module or RSAII using the Web interface" on page 221.
- The RSA II can obtain IP address information using either of the following methods. Use the one that is the most appropriate for your network.
  - Dynamic addressing. This is the factory default.
  - Static IP addressing.
- The RSA II supports the following discovery methods. Use the one that is the most appropriate for your network.
  - "Configuring service processor discovery by SLP for integrated servers" on page 230.
  - "Configuring service processor discovery by IP address for integrated servers" on page 229.
  - "Configuring service processor discovery by host name for integrated servers" on page 229.
- The RSA II supports security using a password. See "Changing a service processor password for an integrated server" on page 216
- For more information about the RSA II, see the following information.

– IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II Installation Guide -

Servers (www.ibm.com/systems/support). Under **Browse**, select **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue**. Select **Publications**.

– IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide -

Servers (www.ibm.com/systems/support). Under **Browse**, select **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue**. Select **Publications**.

Management Module (MM) or Advanced Management Module (AMM)

These types of service processors are available in IBM BladeCenter servers.

* To configure the Management Module or Advanced Management Module, see "Configuring the integrated server Management Module or RSAII using the Web interface" on page 221.
* The Management Module can obtain IP address information using either of the following methods. Use the one that is the most appropriate for your network.
  – Dynamic addressing. This is the factory default.
  – Static IP address information.
* The Management Module or Advanced Management Module supports the following discovery methods. Use the one that is the most appropriate for your network.
  – "Configuring service processor discovery by SLP for integrated servers" on page 230.
  – "Configuring service processor discovery by IP address for integrated servers" on page 229.
  – "Configuring service processor discovery by host name for integrated servers" on page 229.
* IBM BladeCenter systems have additional considerations for discovery.
  – The remote system identity in the remote system configuration must be set to the serial number of the IBM BladeCenter server, which can be found on the label on the server. For information about changing the remote system configuration, see "Changing remote system configuration properties" on page 210.
  – The enclosure identity in the service processor configuration can be set to the IBM BladeCenter enclosure (chassis) serial number.
  – The Management Module service processor in IBM BladeCenter must be discovered before any server blades can be discovered. Parameters in the service processor configuration determine the method of the Management Module discovery. For information about changing these properties, see "Changing service processor configuration properties" on page 213.

  After the Management Module is discovered, the i5/OS operating system gathers information about the server blades contained in the enclosure. The remote system identity is used to discover the individual server blade.
* The Management Module or Advanced Management Module supports the following security methods:
  – Password. For more information, see "Changing a service processor password for an integrated server" on page 216.
* See the IBM BladeCenter Systems Management Redpaper (www.redbooks.ibm.com/abstracts/redp3582.html) for more information about IBM BladeCenter Systems Management.

Service processor discovery for integrated servers

Service processor discovery is the process by which the i5/OS operating system locates the initiator blade or System x hardware on the network. Several discovery methods are available.

Service processor discovery methods

Table 2. Advantages and disadvantages of service processor discovery methods

Discovery method	Advantages	Disadvantages	Compatible service processor types
Discovery by IP address (unicast)	This discovery method is very simple if the service processor's IP address is known and configured into the service processor.	The IP address must be configured into the service processor.	• BladeCenter Management Module (MM) or Advanced Management Module (AMM) • BMC • RSA II
Discovery by host name (unicast)	If a DNS server is available, a specific IP address need not be maintained in the i5/OS remote system configuration.	• The host name must be configured into the service processor via the service processor's web interface. • A Domain Name System (DNS) server is required.	• BladeCenter Management Module (MM) or Advanced Management Module (AMM) • RSA II
Service Location Protocol (SLP) (multicast)	• Only the serial number, which can be obtained from a label on the server, is needed to discover the remote server. • If the service processor obtains its IP address from a DHCP server and the network supports IP multicasting, then the factory default settings of the service processor can be used.	• Routers and switches located between the service processor and the System i LAN adapter must be configured to support multicast addressing. If not properly configured, routers will not propagate multicast packets. • Not supported when you use the Service Processor Manager function of i5/OS Integrated Server Support to discover the service processor.	• RSA II • BladeCenter Management Module (MM) or Advanced Management Module (AMM)

iSCSI network for integrated servers

This physical network connects Ethernet iSCSI adapters in the hosting i5/OS partition with Ethernet iSCSI adapters in the initiator (System x or BladeCenter) system.

The iSCSI network is typically a simple, switched, Gigabit Ethernet network. For environments with i5/OS V6R1 or later, the iSCSI HBAs can be connected directly to each other without a switch. Two kinds of traffic flow over this connection: storage (SCSI) and virtual Ethernet (LAN).

On one side of the network is an iSCSI adapter or adapters controlled by the i5/OS operating system. Each iSCSI adapter port has two IP addresses: one for SCSI and one for LAN. You configure the IP addresses and other attributes of an adapter in an i5/OS device description object known as the network server host adapter (NWSH). For more information, see "Network server host adapters" on page 42. Each iSCSI adapter controlled by i5/OS needs its own object. Every iSCSI adapter contains a TCP/IP stack implemented in hardware that is independent of the normal i5/OS TCP/IP stack. When you vary on a network server host adapter (NWSH), an iSCSI adapter controlled by i5/OS uses the configured values. If you want different values to take effect, you must change the configuration and vary on the server host adapter again. The i5/OS TCP/IP stack is unaware of the IP addresses configured for the iSCSI adapters.

On the other side of the network is an iSCSI adapter or adapters for the initiator system. You configure the IP addresses and other attributes of these adapters in an i5/OS object known as the remote system configuration. For more information, see "Remote system configuration" on page 42. This configuration differs from the i5/OS network server adapter object in several ways:

- You can configure an iSCSI adapter port in an initiator system with 1 or 2 IP addresses: SCSI, LAN, or both. There must be at least one SCSI and one LAN IP address among all of the configured adapters.
- Whenever you configure an IP address for an iSCSI adapter in an initiator system, you must also configure the corresponding adapter MAC address. Each adapter has a label that shows its MAC addresses. Be careful to configure MAC addresses correctly.
- You configure all of the iSCSI adapters for an initiator system in the same i5/OS remote system configuration object. When the integrated server is subsequently varied on, the product automatically ensures that iSCSI adapters in the initiator system are using values in the i5/OS remote system configuration. If you want different values to take effect, you must change the configuration and vary on the server again.
- On integrated Windows servers, SCSI traffic uses the iSCSI adapter's hardware TCP/IP stack, but LAN traffic uses the Windows TCP/IP stack. Consequently, the Windows TCP/IP stack is unaware of the SCSI IP address, but is aware of the LAN IP address.

Note:

1. In i5/OS configuration objects, network interface information is labeled as local or remote. These terms are relative to i5/OS. Local interface information is for the i5/OS side. Remote interface information is for the initiator system side.
2. The NWSH and the remote system configuration define IP address information for opposite sides of the iSCSI network. When connected by a simple, switched network, the following rules apply:
   - The SCSI internet addresses in these two objects that are connected by a switch must be in the same subnet. For example, with IP addresses of the form a.b.x.y and 255.255.255.0 subnet masks, a.b.x must be the same value for both objects.
   - The LAN internet addresses in these two objects that are connected by a switch must be in the same subnet.
   - In the NWSH, the gateway elements can be any unassigned IP address in any subnet if you don't have a gateway in your network.
   - In the remote system configuration, the gateway elements should be blank if you don't have a gateway in your network.

Scaling the iSCSI Network

After you have installed an integrated server, you can scale the iSCSI network.

The basic installation process addresses iSCSI attached servers that use one target (System i) HBA and up to two initiator System x or blade) iSCSI HBAs. After the server is installed, you can configure additional target or initiator iSCSI HBAs if needed.

- Configure multipath I/O for the integrated server storage. See "Multipath I/O for iSCSI-attached integrated servers running Windows or VMware ESX Server" on page 21
- Refer to the Scaling your iSCSI network chapter in the Implementing Integrated Windows Server

   through iSCSI to System i5® (www.redbooks.ibm.com/abstracts/sg247230.html) Redbooks® publication for more information.

Integrated DHCP server

There are several methods for delivering boot information to the initiator system. The default method of delivering IP and storage information to boot the integrated server uses an integrated Dynamic Host

Configuration Protocol (DHCP) server on the i5/OS side of the iSCSI network. For more information, see "Integrated DHCP server for integrated servers" on page 36.

Even with DHCP, the IP address may be considered static because the DHCP server associates a single IP address with a MAC address. For more information, see "Boot modes and parameters" on page 14.

Performance and maximum transmission unit (MTU)

High bandwidth and low latency is desirable for the iSCSI network. Virtual Ethernet can take advantage of an MTU up to a 9000-byte 'jumbo' frame if the network supports the larger MTU. The iSCSI network normally uses standard 1500-byte frames.

Each iSCSI HBA contains a hardware implementation of TCP/IP. This hardware implementation allows iSCSI HBAs that use 1500-byte frames to have similar storage capabilities to iSCSI HBAs that use larger frames. You might be able to configure your switch to use larger frame sizes. If you are not sure that your switch performs well with larger frames, use the default settings for 1500 byte frames. If you use a larger frame size than your switch supports, storage and virtual Ethernet traffic performance might decrease.

Managing i5/OS iSCSI adapter function

Paths configured in the network server description control what storage traffic, if any, and what virtual Ethernet traffic, if any, can flow over an i5/OS iSCSI adapter. For more information, see "Managing iSCSI target and initiator usage for integrated servers" on page 222.

Multiple initiator systems can use an i5/OS iSCSI adapter simultaneously if multiple network server descriptions use the same NWSH object.

Managing initiator system iSCSI adapter function

You can configure an iSCSI adapter in an initiator system with a SCSI IP address, a LAN IP address, or both. A SCSI IP address enables storage traffic, and a LAN IP address enables virtual Ethernet traffic.

Use of the iSCSI adapter as a general-purpose external network connection, is not supported. For more information about external network connections, see "Physical networks for integrated servers" on page 37.

For integrated Windows servers, each virtual Ethernet adapter is automatically assigned to a physical iSCSI adapter. There is an option on the advanced properties tab of each virtual Ethernet adapter. With the option, a particular physical iSCSI adapter can be selected. See "Managing iSCSI initiator allocation at the Windows side of the iSCSI network" on page 224.

Other considerations

The following items are additional considerations for iSCSI adapters.
* The iSCSI network only uses Internet Protocol version 4.
* The frame format is Ethernet version 2.
* The iSCSI network does not support Network Address Translation.

Security

For information about securing storage and virtual Ethernet traffic, see "Network security for integrated servers" on page 35.

Network communications between i5/OS and iSCSI-attached integrated servers

The i5/OS operating system uses network connections to communicate with integrated servers for some administrative functions. Integrated Windows servers use a point-to-point virtual Ethernet network, and integrated VMware and Linux servers use a physical network.

Point-to-point virtual Ethernet for integrated Windows servers

The i5/OS operating system uses the point-to-point virtual network to communicate with integrated Windows servers. This type of virtual Ethernet network is specifically for integrated Windows servers and is different from the virtual Ethernet networks used for inter-partition communication on your System i product.

The i5/OS operating system communicates with integrated Windows servers over a point-to-point virtual Ethernet network. When an integrated server is installed, a special virtual network is created between the integrated server and a controlling i5/OS partition. This network is called point-to-point because it has only two end points (the integrated server, and the System i server). Another reason that this network is called point-to-point is because, like a virtual Ethernet network, the network is emulated within the System i product and no additional physical network adapters or cables are used. In the i5/OS operating system, it is configured as an Ethernet line description with Port Number value *VRTETHPTP.

When you run the Install Windows Server (INSWNTSVR) command, it configures a point-to-point virtual Ethernet.

A point-to-point virtual Ethernet connection and a virtual Ethernet network are different in the following ways:
- A point-to-point virtual Ethernet is configured differently and can only have two end points (the System i server and an integrated server).
- A point-to-point virtual Ethernet only supports the TCP/IP protocol, and by default uses restricted IP addresses in private domains, so the addresses are not passed through gateways or routers.

For iSCSI-attached servers, these addresses take the form of 192.168.xxx.yyy, where xxx ranges from 100 to 254 and results in a unique class C network. In our example, the i5/OS operating system side of the point-to-point network is given the IP address 192.168.100.1, and the Windows operating system side has 192.168.100.2. As you define multiple line descriptions for the same hardware resource, yyy is incremented.

You can use the INSWNTSVR command to automatically assign these IP addresses or manually configure them to prevent TCP/IP address collisions with other hosts on the system.

Physical network for integrated Linux and VMware servers

Integrated Linux and VMware servers use a physical network to communicate between the System i product and a network adapter that is installed in the integrated server hardware.

Virtual Ethernet networks for integrated Windows servers
Integrated servers can use a virtual Ethernet network that is configured on a System i product to communicate with the hosting i5/OS partition, another partition, or other integrated servers.

Virtual Ethernet networks that do not include more than one logical partition
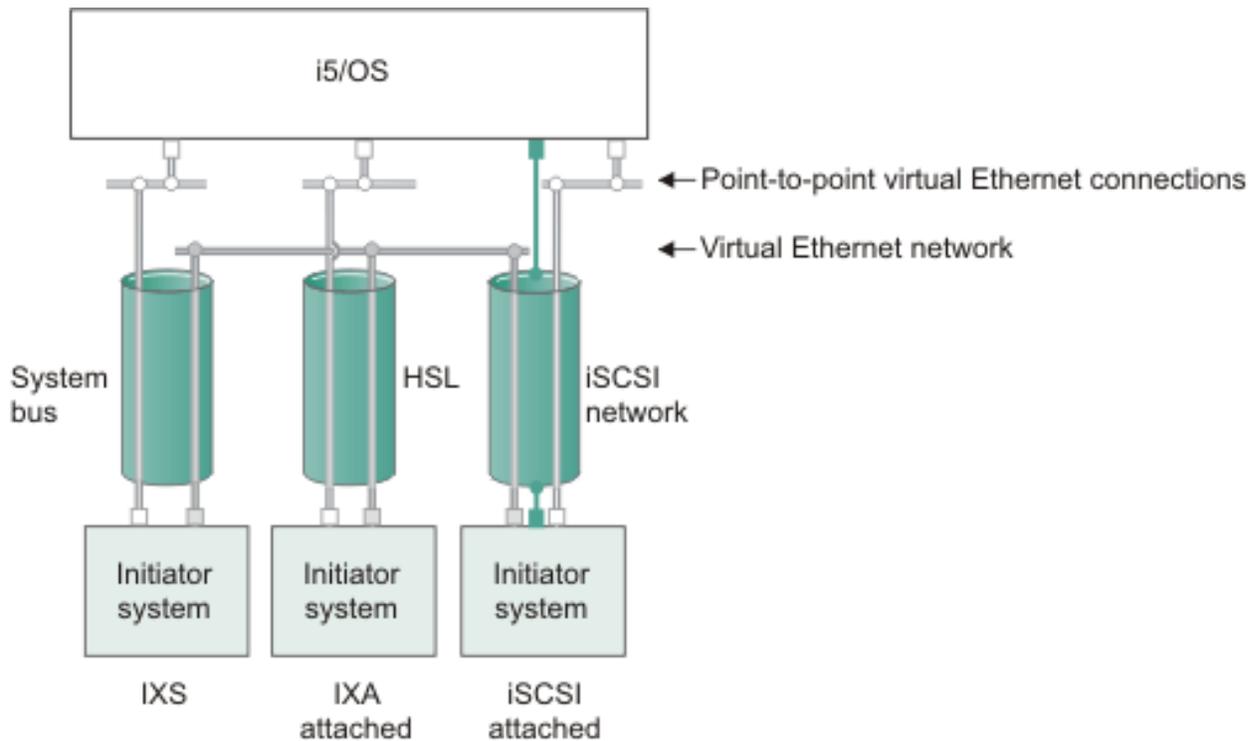
Figure 7. System bus, HSL, and iSCSI network tunnels

Integrated xSeries servers (IXSs), IXA-attached systems, and iSCSI-attached systems can all participate in virtual Ethernet networks and can communicate with each other.

- For IXSs, virtual Ethernet traffic flows over buses for System i products.
- For IXA-attached servers, virtual Ethernet traffic flows through HSL cables.
- For iSCSI-attached servers, virtual Ethernet traffic is tunneled through a physical iSCSI network. Virtual Ethernet is needed when an iSCSI network is present for several reasons:
  - Virtual Ethernet can work with other virtual Ethernet support on your System i product.
  - Virtual Ethernet can provide multiple isolated virtual networks through each iSCSI HBA even when switches in the iSCSI network do not support IEEE 802.1Q VLANs
  - Integrated servers can communicate with each other even if they are each attached by Ethernet switches that are not connected to each other.
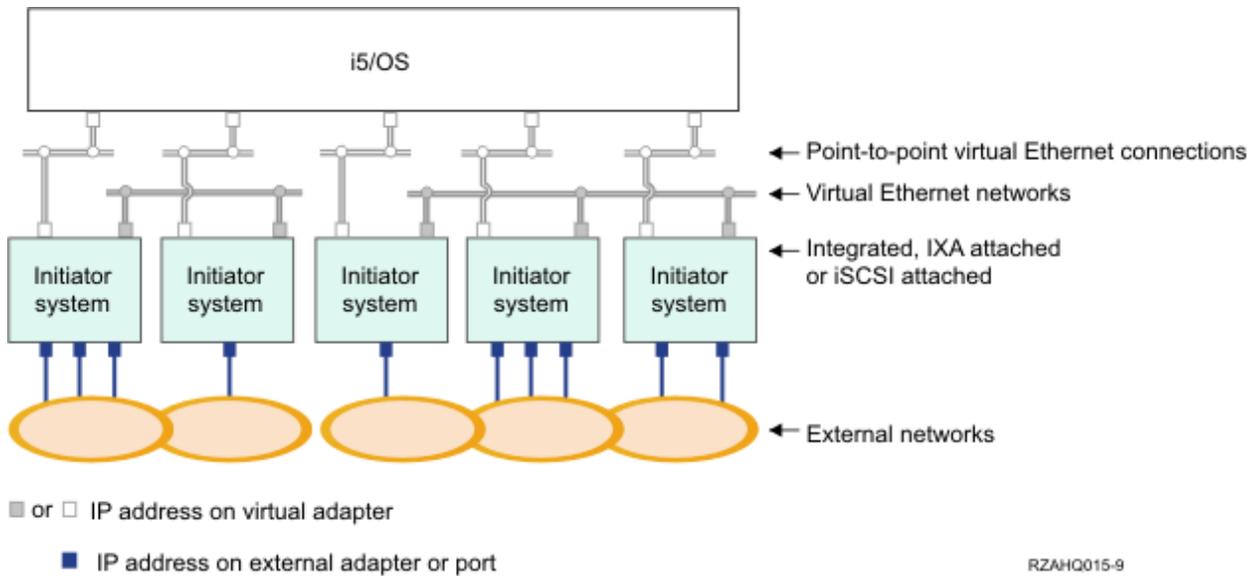
Figure 8. Two isolated groups of integrated Windows servers on the same System i product. Each group has its own virtual Ethernet network.

This figure illustrates how virtual networks work within the System i product. There are five separate integrated Windows servers. They are all connected to the single controlling i5/OS partition with point-to-point virtual Ethernet networks. The boxes on the bottom of the integrated servers represent physical network adapter cards that allow the machines to make external network connections. The ovals to which they are connected represent external networks. Finally, there are two separate virtual Ethernet networks. Each integrated server can participate in up to four virtual Ethernet networks simultaneously.

Like point-to-point virtual Ethernet, virtual Ethernet networks are configured through Ethernet line descriptions. An integrated server is connected to a virtual Ethernet network when its i5/OS configuration (NWSD) is configured to have an Ethernet line description port number with a value of *VRTETH0 through *VRTETH9. Integrated servers that have NWSDs configured with the same port number values are connected to the same virtual Ethernet network. When you install a new integrated server, the Install Windows server (INSWNTSVR) command can automatically create the required line descriptions and assign them IP addresses. In the figure, the i5/OS side of the line descriptions is not shown. Unlike when you use virtual Ethernet, configure a TCP/IP address on the i5/OS side of a line description that is used in a virtual Ethernet network.
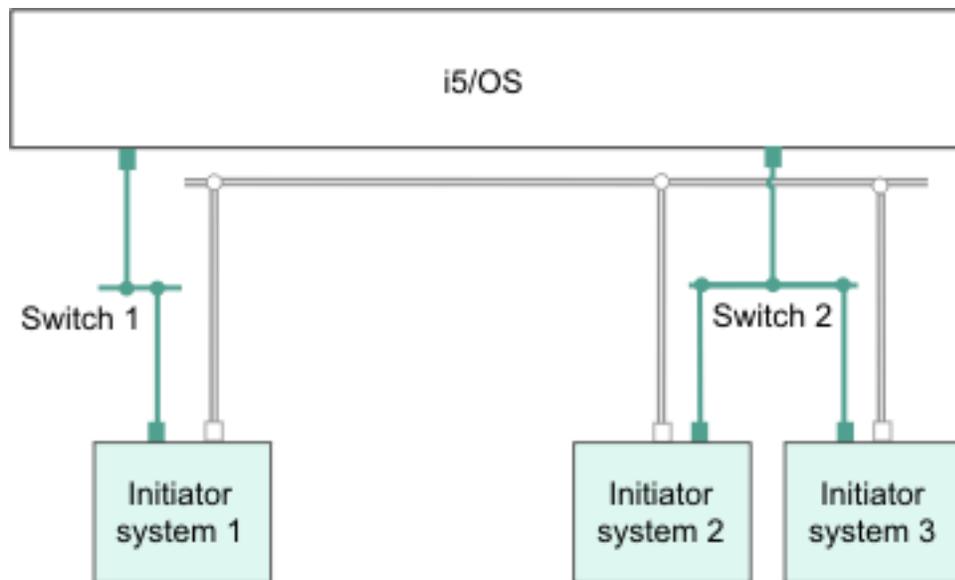
Figure 9. Virtual Ethernet tunneled through iSCSI networks

Virtual Ethernet tunneled through iSCSI networks has some special characteristics that are illustrated in Figure 9.

- Initiator system 1 can communicate with Initiator system 2 and with Initiator system 3, even though separate iSCSI networks (separate physical switches) are involved.
- Virtual Ethernet communication between Initiator system 2 and Initiator system 3 involves the System i product, even though both of these initiator systems are connected to the same physical switch.

Virtual Ethernet networks that include more than one logical partition
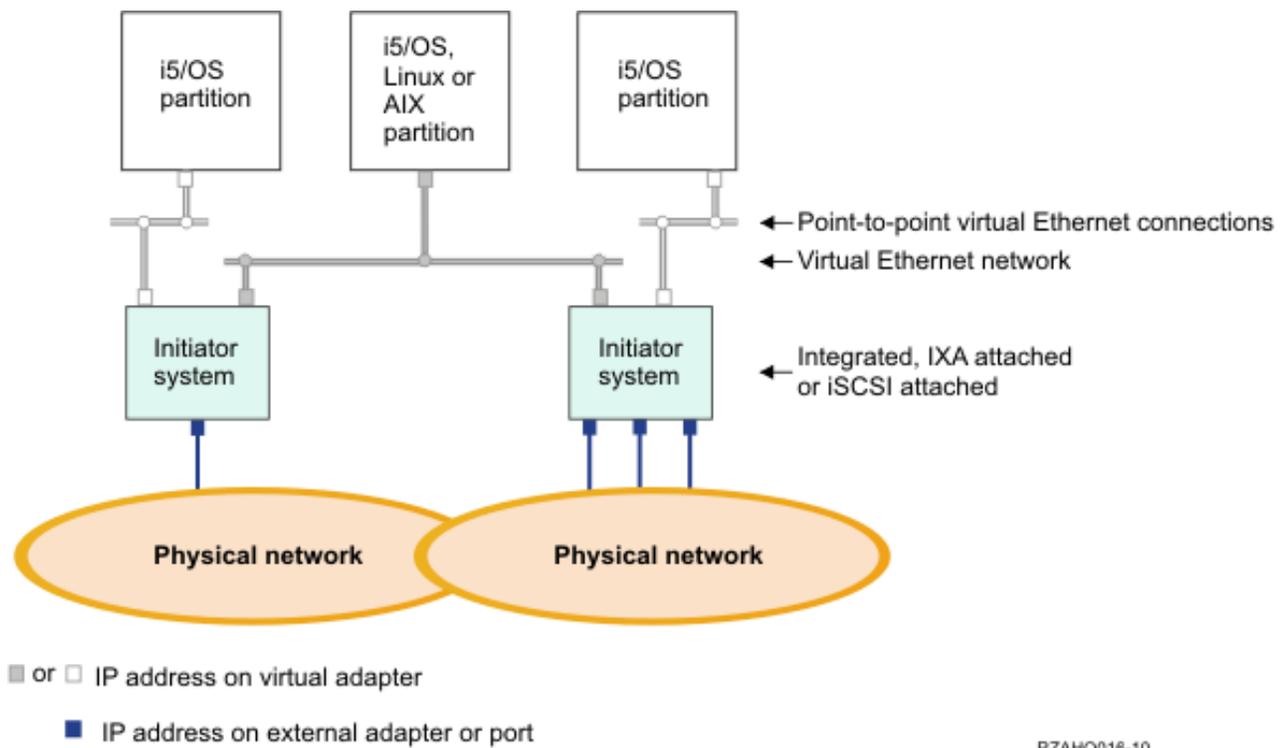
Figure 10. A simple, inter-partition virtual Ethernet network.

Now the System i product has been partitioned, and three separate virtual i5/OS logical partitions have been created inside the System i product. Three virtual networks are represented in the figure; two point-to-point virtual Ethernet networks and one virtual Ethernet network. Each integrated server has a point-to-point virtual Ethernet network for communicating with its controlling partition. In this example, the virtual Ethernet network has three participants: two integrated servers, each controlled by a different i5/OS partition, and a third partition running i5/OS or another operating system. This is called an inter-partition Ethernet network.

Inter-partition connections exist between partitions or integrated servers that are assigned the same virtual LAN ID at the Hardware Management Console (HMC). Participating integrated servers do not support virtual LAN IDs directly. Instead, each participating integrated server needs an Ethernet line description that associates a port value such as *VRTETH1 with a virtual adapter that has a virtual LAN ID. You create the virtual adapter using the HMC. For more information, see Partitioning on systems with POWER5™ or POWER6™ processors and Configuring a virtual Ethernet adapter using version 6 or earlier of the HMC in the IBM Systems Hardware Information Center. If you migrate inter-partition virtual Ethernet from a server without HMCs to a server with an HMC, you need to create virtual Ethernet adapters using the HMC and additional Ethernet line descriptions to provide appropriate associations. Note that within the same partition, Windows servers can still communicate with each other by using the same virtual Ethernet port number.

Related tasks

"Configuring and managing virtual Ethernet and external networks" on page 131
Use these tasks to configure and manage the Ethernet networks for integrated Windows servers.

"Configuring IP address, gateway and MTU values for integrated servers" on page 131
Learn which console to use and how to configure networking values for integrated Windows servers.

"Configuring virtual Ethernet networks between integrated Windows servers" on page 132
Do these steps to configure a virtual Ethernet network between integrated servers that are configured in the same logical partition.

"Configuring inter-partition virtual Ethernet networks for integrated servers" on page 133
If you want an integrated server to communicate with other logical partitions, or with integrated servers controlled by other i5/OS partitions, you need to configure one or more inter-partition networks.

Network security for integrated servers

iSCSI-attached servers use two types of networks. You can add security to both the service processor connection and the iSCSI network.

Service processor connection security

Service processor security can involve one or more of the following mechanisms:
- Service processor password
- Network isolation and physical security

iSCSI network security

Consider the following types of iSCSI network traffic:
- Storage security can involve one or more of the following mechanisms:
  - network isolation, physical security, and security gateways
  - Challenge Handshake Authentication Protocol (CHAP)
  - firewalls
- Virtual Ethernet security can involve one or more of the following mechanisms:
  - network isolation, physical security, and security gateways
  - firewalls
  - Secure Sockets Layer (SSL) connection for sensitive data during user enrollment and remote command submission

Network isolation and physical security

Network isolation minimizes the risk of data that is accessed by unauthorized devices and data that is modified when it traverses the network. You can create an isolated network by using a dedicated Ethernet switch or a dedicated virtual local area network (VLAN) on a physical VLAN switch or network. When you configure a VLAN switch, treat an iSCSI HBA that is installed on a System i product as a VLAN-unaware device.

Physical security involves physical barriers that limit access to the network equipment and the network end points at some level (locked rack enclosures, locked rooms, locked buildings, and so on).

Service processor password

This password is managed by the i5/OS operating system and is used when your System i product starts a conversation with the service processor of the initiator system. The service processor checks the password to ensure that the i5/OS configuration is authentic. New service processors have a default name and password. i5/OS provides a way to change the password.

Secure Sockets Layer (SSL) connection between i5/OS and Windows

The i5/OS Integrated Server Support option includes user enrollment and remote command submission functions, which may transfer sensitive data over the point to point virtual Ethernet. These applications

automatically set up an SSL connection to encrypt their sensitive network traffic, and to ensure that each side of the conversation is authentic, based on automatically installed digital certificates. This security feature is provided by default and is not configurable. File data, command results, and traffic for other applications are not protected by this SSL connection.

Challenge Handshake Authentication Protocol (CHAP)

CHAP protects against the possibility of an unauthorized system using an authorized system's iSCSI name to access storage. CHAP does not encrypt network traffic, but rather limits which system can access an i5/OS storage path.

CHAP involves configuring a secret that both i5/OS and the hosted system must know. Short CHAP secrets may be exposed if the CHAP packet exchange is recorded with a LAN sniffer and analyzed offline. The CHAP secret should be random and long enough to make this method of attack impractical. i5/OS can generate an appropriate secret. A hosted system uses the same CHAP secret to access all of its configured i5/OS storage paths.

You can configure either target or bidirectional CHAP. Target CHAP authenticates the iSCSI initiator HBAs that connect to the target iSCSI HBA in the System i product. Bidirectional CHAP involves both target CHAP and initiator CHAP. Initiator CHAP authenticates the target iSCSI HBAs that connect to the initiator iSCSI HBA in the System x or blade hardware.

CHAP is not enabled by default, but it is strongly recommended.

Firewalls

A firewall can be used between a shared network and the System i product to protect the System i product from unwanted network traffic. Similarly, a firewall can be used between a shared network and the initiator system protect the initiator system from unwanted network traffic.

iSCSI attached system traffic has the following attributes that should be helpful when configuring a firewall:
- iSCSI HBAs have static IP addresses (there is a DHCP boot mode, but the IP addresses involved are statically pre-configured)
- UDP and TCP ports that are deterministic and configurable. Each virtual Ethernet adapter on the hosted system uses a different UDP port to tunnel through the iSCSI network. Virtual Ethernet packets are encapsulated as follows, from outer header to inner header:
  - MAC and IP header for the iSCSI HBA using LAN (not SCSI) addresses.
  - UDP header. See "Configuring a firewall to allow integrated server connections" on page 216 for information about optionally controlling UDP port selection.
  - MAC and IP headers for the virtual Ethernet adapter.

Integrated DHCP server for integrated servers
The IBM Integrated Server Support option provides an integrated DHCP server that is used for communication with iSCSI HBAs in integrated servers. This server cannot be used for other types of networking. You should use the default configuration for most environments.

Advanced integrated DHCP server concepts

The iSCSI-attached server uses an integrated DHCP server when it is configured to use the default or DHCP boot mode. This integrated DHCP server is not a general purpose server. It is intended to exclusively deploy boot parameters to the hosted server iSCSI initiator. The server is automatically configured with the parameters that are provided in the remote system configuration when a network server description (NWSD) is varied on.

The server is used to deploy boot parameters to the hosted-server iSCSI initiator, when the Dynamically delivered to the remote system through DHCP option is specified in the i5/OS remote system configuration object and when AUTO or DHCP mode is specified in the hosted-server iSCSI initiator.

The DHCP server responds only to the iSCSI initiator DHCP client of the hosted server. All of the requests from the iSCSI initiator DHCP client use an IBM-defined vendor ID. The server is programmed to respond to requests that use the default vendor ID, and ignore any other requests from other devices in the network.

In addition to the vendor ID, the integrated DHCP server uses the MAC address to deploy boot parameters. MAC address is part of the specific scope that is required to ensure proper parameter deployment.

The scope that the vendor ID and MAC address provide can be changed. Advanced and sophisticated users can more specifically configure this setting, when required. The default vendor ID can be configured to other values. Configuration screens are available in the iSCSI initiator configuration function of the hosted server and the corresponding remote system configuration object. This advanced function is compliant with the RFC 2132 specification. For more details about advanced configuration, see the iSCSI install read me first Web page.

When the integrated DHCP server receives an incoming DHCP request and all of the required scope is matched, the integrated DHCP server provides the DHCP client with the IP addresses for the boot target device. The boot target device is the network server host adapter (NWSH) where the boot virtual disk is configured. The server also provides the IP address for the initiator or DHCP client. The iSCSI initiator is the adapter in the hosted server and it is used to boot over iSCSI.

In addition, the integrated DHCP server provides the globally unique iSCSI Qualified Names (IQNs) that represent the target and initiator devices to the iSCSI initiator of the hosted system .

Both of these sets of IP addresses and IQNs are in the i5/OS configuration objects used to define the hosted server. The target IP address is defined in the NWSH object. The initiator IP address and initiator IQN are defined in the remote system configuration object. The target IQN is automatically configured and defined in the NWSD object. For more information about these objects refer to "Network server description" on page 41.

The integrated DHCP server is a key and integral component when implementing hot spares. The DHCP boot mode enables automatic deployment of the required parameters defined in the i5/OS configuration objects, eliminating the need to manually configure a server when boot parameters (IP addresses and IQNs) change.

Physical networks for integrated servers

Integrated servers can use an integrated Ethernet controller, a network adapter installed in a PCI slot, or a BladeCenter I/O module to connect to an external network.

These are the normal networks which all integrated servers use, created by networking through physical adapters controlled by the integrated server operating system.

In an iSCSI-attached integrated server you can use any integrated network adapter or install a network adapter card as you would in a PC.

Performance concepts for integrated servers

Integrated server performance is affected by the configuration of the storage and network for the integrated server.

The iSCSI-attached systems have their own memory and one or more processors, but share the System i hard disk storage through virtual (simulated) disk drives. The disk drives are allocated integrated servers by creating an i5/OS virtual disk (network server storage space). The major difference between the integrated servers and stand-alone servers is that stand-alone servers tend to use dedicated disk drives and the integrated servers use System i storage spaces as virtual disks. Integrated servers also include optional features such as drivers to share System i tape, CD and DVD drives. Integrated Windows servers can use high-speed virtual Ethernet networks to communicate with other integrated servers or System i logical partitions.

The use of System i storage spaces (virtual drives) provides performance benefits that are not typically available in stand-alone environments without significant storage fabric investment and maintenance costs. However, it also imposes some limitations. You should consider these limitations when planning and configuring integrated servers. The information below highlights some considerations affecting performance.

Storage performance for integrated servers

Storage performance depends on the configuration of the integrated server environment.

For performing processor or memory intensive work on an integrated server, the performance characteristics are equivalent to a stand alone server using dedicated disk drives. Since the integrated server disk drives are allocated out of System i storage, the disk performance is dependent on the System i product.

Greater disk performance capacity with System i shared disks

On most standalone servers a few disks are dedicated to each server. For applications with a small average disk load, the performance is adequate. However, there can be periods of time where the server performance is limited by the capacity of those few dedicated disks.

When the same group of servers is integrated with the System i, the virtual disks are spread across more System i hard disks. The total average disk load does not need to be any greater than for a group of servers with dedicated disks. But, when an individual server temporarily needs more disk performance capacity, it is available through the larger set of System i disks.

On servers with dedicated disks, the disk response times tend to be relatively steady.

On integrated Windows servers, you might take advantage of the predictable response time and configure the Windows Performance Monitor to produce alerts when disk response times exceed typical thresholds and indicate exceptional conditions which might need your attention.

On an integrated server, the System i storage, CPU and memory are shared between the integrated server and System i applications. It is normal for disk response to swing through a larger range. Short periods might occur where I/O operations from multiple integrated servers, or other System i operations contend for the same disk. Some disk intensive System i applications (like SAV and RST), can reduce the disk performance seen on the integrated server for a period of time. This can make it more difficult to choose a threshold value for short time periods.

Storage space balancing for integrated servers

The disks in the pool may be configured to be unprotected, parity protected (RAID-5), or with mirrored protection. Unprotected disks provide no protection against disk failures. Parity protected disks maintain parity sets which allow the recovery if a disk fails in a parity set (but at a performance cost). Mirroring provides protection against disk failures, but with much better performance than parity. The integrated server gains the benefits of the efficient System i storage architecture, regardless of how an ASP or independent ASP is configured.

The i5/OS operating system has functions to help maintain the efficient spread of data across the disks. One example is the Start Disk Reorganization (STRDSKRGZ) operation, which balances disk storage utilization. Another is the "Add units to ASPs and balance data" available when hard disk resources are assigned to an ASP. On integrated servers, a storage space will only be moved or rebalanced across disks while the linked server is varied off.

The location of the data associated with a storage space is usually automatically managed by the i5/OS operating system. There is no need to configure striped volumes or software RAID of the disks within the integrated server operating system. Configuring these features in the integrated server operating system might actually slow the effective disk operations. For integrated Windows servers, continue to defragment the associated disk on Windows to maintain efficient file-system data structures.

You can monitor how well the i5/OS operating system is fulfilling the integrated server's disk requirements by using the Work with Disk Status (WRKDSKSTS), Work with Network Server Storage Spaces (WRKNWSSTG), and Work with Network Server Status (WRKNWSSTS) commands.

For integrated Windows servers, you can use the Microsoft Windows Performance Monitor as you would on any other server. See your Microsoft Windows documentation for information about using the Performance Monitor.

Consider the entire group of disks when you evaluate storage bottlenecks for integrated Windows servers

The System i product storage space appears as one disk drive within Windows. When the Physical Disk average queue length (in Windows Performance Monitor) exceeds two, the server performance is not necessarily disk constrained. Assuming that memory paging issues have been ruled out, a queue length of two or a Windows disk utilization of 100% only points to a storage bottleneck if there is only one physical disk drive to perform the operations. There are usually multiple disks on the System i product in the storage space ASP operating in parallel. Typically, two times the number of disks in the ASP might point toward a disk bottleneck. You might also need to account for the average queue lengths of all the servers using the storage ASP.

Virtual Ethernet performance for integrated Windows servers

The Virtual Ethernet point-to-point connection is the default virtual network connection between the hosting i5/OS partition and each integrated Windows server. The-point-to-point connection is used primarily for administrative operations which are part of the integration environment.

The System i and Windows CPU utilization cost of using the point-to-point connection is similar to the utilization cost of using a hardware network adapter. The connection is high speed, but total bandwidth is always shared with disk, tape and other integrated server operations. When you use internet SCSI (iSCSI), you can separate virtual Ethernet operations by using another iSCSI HBA channel.

A Virtual Ethernet connection between two or more integrated servers uses the System i CPU to switch the traffic between servers, even when the System i product is not an endpoint of the traffic. For most connections this utilization won't be significant. If you expect high sustained network loads across the virtual Ethernet connection between integrated Windows servers, you might want to balance the cost of using the Virtual Ethernet internal switch against external network adapters on the integrated servers.

Maximum transmission unit considerations for iSCSI network

The default MTU size for iSCSI-attached integrated servers is 1500 bytes. You can configure the network to use other Ethernet frame sizes to adjust network performance.

The MTU setting affects the frame size that storage and virtual Ethernet use on the iSCSI network.

Note: The frame sizes discussed here do not include the Ethernet 14 byte MAC header.

In general, the maximum frame size used on the iSCSI network is configured only at each initiator iSCSI HBA. The target iSCSI HBAs negotiate an MTU that is compatible with initiators using TCP/IP protocol. In contrast to the 9000 byte jumbo frames provided in IXS and IXA-attached servers, initiator iSCSI HBAs default to a smaller frame size that can be transported in a standard 1500 byte Ethernet frame.

If the iSCSI network is capable of a larger frame size, you can configure an initiator iSCSI HBA to use a larger frame size. However, under heavy traffic, many Ethernet switches and networks do not perform well with larger frames, potentially decreasing the performance of both storage and virtual Ethernet. If you are not sure that your switch performs well with larger frames, use the standard 1500-byte frame size. In a complex iSCSI network, there may be a mix of maximum frame sizes depending on the network topology and the equipment.

Related tasks

"Configuring virtual Ethernet for applications that support frame sizes larger that 1500 bytes" on page 226
Do these steps to configure virtual Ethernet to support jumbo frames for an integrated server.

"Configuring virtual Ethernet for iSCSI networks that have a maximum frame size that is less than 1500 bytes" on page 227
Do these steps to configure virtual Ethernet for iSCSI networks that have a maximum frame size that is less than 1500 bytes.

"Configuring virtual Ethernet to support non-TCP applications that do not negotiate MTU" on page 227
Do these steps to configure virtual Ethernet for an integrated server to support applications that do not use TCP and do not negotiate maximum transmission unit (MTU).

Software concepts and configuration objects for iSCSI-attached integrated servers

The i5/OS operating system uses objects to represent and control integrated server hardware, software, and storage.

The following figure shows the objects that i5/OS uses to configure iSCSI-attached integrated servers.
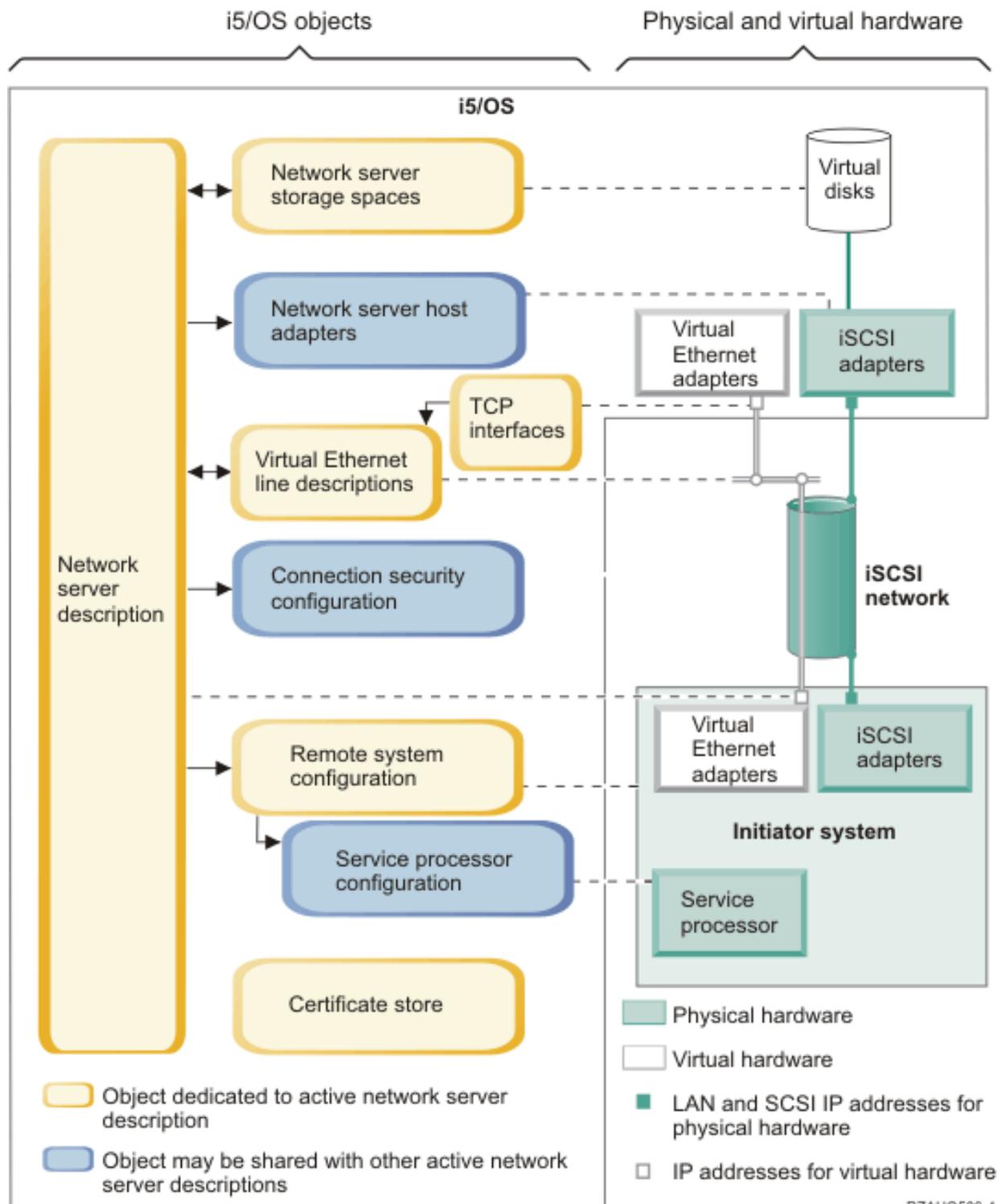
Figure 11. iSCSI configuration objects in i5/OS with network security

Network server description

The network server description (NWSD) object is the main configuration object for an integrated server.
- It contains a reference to a remote system configuration object.
- It contains references to the iSCSI and virtual Ethernet data paths for the integrated server.

- You can define one or more storage paths. These storage paths reference the NWSH objects that are associated with the iSCSI HBAs that are used by the integrated server. You can choose which storage path is used for the SCSI data flows for each virtual disk drive. By associating your virtual disk drives with different storage paths, you can spread the overall server SCSI data flow workload across the storage path iSCSI HBAs for greater bandwidth. See "Multipath I/O for iSCSI-attached integrated servers running Windows or VMware ESX Server" on page 21.
  - You can define one or more virtual Ethernet paths. These virtual Ethernet paths also reference the NWSH objects that are used by the integrated server. You can choose which NWSH is used for each virtual Ethernet port that the integrated server uses. By associating different virtual Ethernet ports with different NWSHs, you can spread the overall server virtual Ethernet data flow workload across the virtual Ethernet path iSCSI HBAs for greater bandwidth.
- The iSCSI attached System x or BladeCenter hardware is controlled by the i5/OS operating system.
  - An iSCSI-attached server is turned on and off by starting or stopping the NWSD for that server.
  - The i5/OS operating system uses an Ethernet network to communicate with the service processor (SP) for the System x hardware or the BladeCenter management module for aBladeCenter server to perform the start and shut down tasks.

  Note: In case of a hardware failure, you can change the remote system configuration name that is specified in the NWSD and restart the server using spare hardware. See "Hot spare support for integrated servers" on page 44.

Network server host adapters

A network server host adapter (NWSH) device description object represents the iSCSI host bus adapter (HBA) that is used by the System i side of the iSCSI connection.
- It identifies the System i Network Server Host Port resource name (for example, CMNxx) for the iSCSI HBA.
- It defines how communications errors are logged and communications recovery information.
- It defines the internet addresses, ports, and so on. for the SCSI and LAN interfaces on the iSCSI HBA.

The System i product can have multiple iSCSI HBAs. Each port on an iSCSI HBA has an associated NWSH object.
- Each NWSH can be shared by multiple integrated servers. In configurations where bandwidth is not a concern, this results in a lower cost solution.
- Each integrated server can use multiple NWSHs. This allows multiple SCSI and virtual Ethernet data paths between the System i and the System x or blade system, which can provide greater bandwidth and connection redundancy.

Remote system configuration

The remote system network server configuration (NWSCFG type RMTSYS) object contains information that identifies the integrated server hardware to the i5/OS operating system.
- It identifies the server hardware by serial number and type and model.
- It contains configuration information for the iSCSI host bus adapters (HBAs) that are used by the System x or blade hardware.
- It contains values required to boot the server (such as specifying which iSCSI adapter to boot from).
- It contains a reference to the service processor NWSCFG object (see below) that is used to control the System x or blade hardware.
- Challenge handshake authentication protocol (CHAP) configuration values that are used to authenticate the remote system when it initially accesses storage.

The System x or blade server can have multiple iSCSI HBAs. This allows multiple SCSI and virtual Ethernet data paths between the System i and the System x or blade hardware, which can provide greater bandwidth and connection redundancy.

The remote system configuration object for an integrated server is referenced via a parameter in the NWSD.

Service processor configuration

A service processor network server configuration (NWSCFG type SRVPRC) object represents the System x service processor or the BladeCenter management module.

The service processor configuration object contains the following information:
- It identifies the service processor or management module hardware by serial number and type and model.
- It defines how to find the service processor or management module on the Ethernet network using an internet address or host name.
- It contains a service processor user name and password that are used to sign on to the service processor.

Note: For iSCSI attached System x product, there is a one-to-one relationship between the service processor object and the remote system configuration, since each service processor controls only one System x product. However, for iSCSI attached BladeCenter systems, there can be a one-to-many relationship between the service processor object and the remote system configuration, since each management module can control any of the BladeCenter systems that are contained within the BladeCenter chassis. Therefore, with iSCSI attached BladeCenter systems it would be common for several remote system configurations to share (refer to) the same service processor object.

Connection security configuration

This object is used by the system. Do not configure any parameters for this object.

Certificate stores

Certificates are used to secure communications between i5/OS and the initiator system for various functions. The certificates are kept in the following i5/OS certificate store:

A certificate store that is associated with the network server description.
This certificate store is created and maintained automatically for you. It is used to store certificates that are generated and used internally by the i5/OS Integrated Server Support (for example, certificates that are used when enrolling users to the hosted system). The certificates in this certificate store are used only when communicating with hosted systems that use the corresponding network server description.

Network server storage spaces

A network server storage space (NWSSTG) represents a virtual disk for an integrated server. Virtual disks can vary in size from 1 MB to 1000 GB each. Up to 64 virtual disks can be linked to a server, depending on the server configuration, so the storage capacity of an integrated server can range from several gigabytes to many terabytes. The virtual disks are first created as stand-alone objects and then linked to the integrated server by identifying the NWSD of the integrated server that uses them.

Each server will have at least 2 virtual disk drives that are automatically created by the Install Windows server (INSWNTSVR) or Install Linux server (INSLNXSVR) command, but can also have user-defined virtual disk drives.

- The system drive (typically the C: drive) contains the integrated server operating system (such as Linux, Windows, or VMware ESX Server).
- The install drive is used every time the server is started to pass configuration information from i5/OS to the server. For integrated Windows servers, it also contains the i5/OS Integrated Server Support (5761-SS1 option 29) code that runs on the Windows server. For some versions of Windows, the install drive also contains a copy of the Windows server installation media.
- Additional user-defined drives are typically used for server applications and data.
- When linking the virtual disk drive to the NWSD, it is necessary to identify which of the NWSD's storage paths to use for the SCSI data flows for that virtual disk drive.
- You can choose a specific storage path, the multi-path group or let the default storage path be used.

The actual disk storage for the virtual disks is allocated from the i5/OS integrated file system. The virtual disk drives can be allocated from the default system disk pool (also known as the system auxiliary storage pool, or system ASP) or from a user defined disk pool or an independent disk pool (independent ASP).

See "Storage management for integrated servers" on page 15 for more information about virtual disks.

Note:

1. Since virtual disks are objects in the i5/OS integrated file system, an entire virtual disk drive image can be backed up and restored using the i5/OS Save (SAV) and Restore (RST) commands. You can also do a file-level backup for the Linux or Windows operating systems or you can configure applications at the integrated server console. For more information, see "Backing up and recovering integrated servers from i5/OS" on page 194.
2. Even though storage spaces are allocated out of the integrated file system, storage operations are not performed by IFS while the integrated server is varied on. This means that operations like journaling are not enabled.

Data flows

SCSI and virtual Ethernet data between the i5/OS operating system and the iSCSI-attached integrated server travel over an Ethernet network.

In essence, the disk drive SCSI and virtual Ethernet protocols are encapsulated or tunnelled within the normal Ethernet network protocols.

High availability concepts for integrated servers

Integrated servers can be made highly available through hot spare hardware, clustering, multipath storage connections, or by configuring the integrated server as a switchable device.

Related tasks

"Configuring high availability for integrated servers" on page 217
Use these tasks to configure high availability iSCSI-attached integrated servers.

i5/OS clustering for integrated servers

You can include the disks that store integrated server in an i5/OS cluster.

For more information, see the High availability topic collection.

Hot spare support for integrated servers

If your integrated server hardware fails, you can configure your integrated server to use replacement hardware with your existing storage spaces.

Hot spare hardware provides a way to quickly recover from certain types of hardware failures. This can reduce the server downtime from hours or days to minutes.

If the System i target iSCSI host bus adapters (iSCSI HBA) that the System x or blade system is using has a hardware failure, you can quickly switch the hosted system to use a spare iSCSI HBA and restart the hosted system.

Related tasks

"Using hot spare integrated server hardware" on page 203
If there is a problem with your System x or blade hardware, use these steps to change your i5/OS configuration objects to point to new hardware.

"Using hot spare iSCSI HBAs for integrated servers" on page 204
If there is a problem with your System i iSCSI HBA, use these steps to change your i5/OS configuration objects to point to another iSCSI HBA.

User and group concepts for iSCSI-attached integrated servers

Learn about how i5/OS users and groups interact with integrated servers.

One of the main advantages of using integrated Windows servers is the user administration function for i5/OS and Windows user profiles. The user administration function allows administrators to enroll existing i5/OS user and group profiles to Microsoft Windows.

Enrollment

Enrollment is the process by which an i5/OS user or group profile is registered with the integration software.

The enrollment process happens automatically when triggered by an event such as running the CHGNWSUSRA command to enroll a user or group, an enrolled Windows user updating their i5/OS user profile password or user attributes, or restarting the integrated server. If the integrated Windows server is active, the changes are made immediately. If the integrated server is varied off, the changes occur the next time the server is started.

Windows domains and local servers

Enrollment can be made to either a Windows domain or a local server. A Windows domain is a set of resources (applications, computers, printers) which are networked together. A user has one account across the domain and needs only to log onto the domain to gain access to all the resources. An integrated server can be a member server of a Windows domain and integrate i5/OS user accounts into the Windows domain.

On the other hand, if you enroll i5/OS users to an integrated server which is not part of a domain, it is called a **local server**, and user accounts will only be created on that integrated server.

Note: In Windows networking, groups of local servers can be loosely affiliated by using Windows workgroups. For example, if you open My Network Places and click Computers Near Me, you will see a list of the computers in the same workgroup as you.

Microsoft Windows i5/OS groups

Two groups of users are created in Microsoft Windows as part of the installation to an integrated server.

AS400_Users

Every i5/OS user, when first enrolled to the Windows server, is placed in the AS400_Users group. You can remove a user from this group in the Windows server; however, the next time an update occurs from the System i product, the user will be replaced. This group is a useful place to check which i5/OS user profiles are enrolled to the Windows server.

AS400_Permanent_Users

Users in this group cannot be removed from the Windows server by the System i product. It is provided as a way to prevent Windows users from being accidentally

deleted by actions taken within i5/OS. Even if the user profile is deleted from i5/OS, the user will continue to exist in the Windows server. Membership in this group is controlled from the Windows server, unlike the AS400_Users group. If you delete a user from this group, it will not be replaced when an i5/OS update is performed.

Using the i5/OS user profile LCLPWDMGT attribute

There are two ways to manage user profile passwords.

Traditional user

You may choose to have i5/OS passwords and Windows passwords be the same. Keeping the i5/OS and Windows passwords the same is done by specifying the i5/OS user profile attribute value to be LCLPWDMGT(*YES). With LCLPWDMGT(*YES), enrolled Windows users manage their passwords in i5/OS. The LCLPWDMGT attribute is specified using the i5/OS Create or Change user profile (CRTUSRPRF or CHGUSRPRF) commands.

Windows user

You may choose to manage enrolled Windows profile passwords in Windows. Specifying LCLPWDMGT(*NO) sets the i5/OS user profile password to *NONE. This setting allows enrolled Windows users to manage their password in Windows without i5/OS overwriting their password.

See "User and group concepts for iSCSI-attached integrated servers" on page 45.

Using i5/OS Enterprise Identity Mapping (EIM)

There are two ways to take advantage of the i5/OS EIM support. You can automatically create an EIM association using functions in the EIM Windows registry. Defining EIM associations allows i5/OS to support Windows single sign-on using an authentication method such as Kerberos. Auto-creation and deletion of Windows EIM source associations are done when the i5/OS Create, Change, or Delete user profile (CRTUSRPRF, CHGUSRPRF, or DLTUSRPRF) commands are used specifying the EIMASSOC parameter values of *TARGET, *TGTSRC, or *ALL.

You may manually define EIM associations in the EIM Windows registry. When an EIM i5/OS target association and Windows source association is defined for an i5/OS user profile, the enrolled i5/OS user profile may be defined as a different user profile name in Windows.

Note: SBMNWSCMD, QNTC, and file level backup operations only work with EIM Kerberos associations. i5/OS user profiles mapped to different Windows user names using an EIM Windows registry are not recognized. Those operations still attempt to use equivalent names.

For more information see "Configuring Enterprise Identity Mapping for integrated Windows servers" on page 143.

Enrolling existing Windows user profiles

You can also enroll a user who already exists in the Windows server. The password for the user must be the same on i5/OS as for the already existing Windows user or group. See "i5/OS password considerations for integrated Windows servers" on page 47.

User enrollment templates

You can customize the authorities and properties a user receives during enrollment through the use of user enrollment templates. See "User enrollment templates for integrated Windows servers" on page 49. If you do not use a template when you enroll users, they receive the following default settings:

- Users become members of the AS400_Users group and either the Users group either in a local integrated Windows server or in the Domain Users group on a Windows domain.
- i5/OS keeps track of the user's i5/OS password, password expiration date, description, and enabled or disabled status.

Enrolling i5/OS groups

Up to this point, only the enrollment of individual i5/OS user profiles to the Windows server has

been discussed. You can also enroll entire i5/OS groups. Then, when you add users to those i5/OS groups that have been enrolled to the Windows server, you automatically create and enroll those users in the Windows server as well.

Enrolling to multiple domains

You may enroll users and groups to multiple domains, but typically this is unnecessary. In most Windows servers, multiple domains set up trust relationships with each other. In such cases, you only need to enroll the user in one domain because trust relationships automatically give the user access to other domains. See your Windows documentation for additional information about trust relationships.

Saving and Restoring enrollment information

Once you have defined your user and group enrollments, you need to save the enrollment definitions. You may save the enrollment information using options 21 or 23 on the GO SAVE menu, by using the SAVSECDTA command, or by using the QSRSAVO API. Restoring the user profiles is done using the RSTUSRPRF command and specifying USRPRF(*ALL) or SECDTA(*PWDGRP) values.

Using the PRPDMNUSR parameter

If you have multiple servers which are members of the same domain, you may prevent duplicate domain enrollment from occurring on each member server. Use the Propagate Domain User (PRPDMNUSR) parameter in the Change Network Server Description (CHGNWSD) or Create Network Server Description (CRTNWSD) commands. See "Configuring the QAS400NT user for user enrollment on integrated Windows servers" on page 139 for more information.

Using the DSBUSRPRF parameter

You can specify whether you want user profiles on integrated Windows servers to be disabled when the corresponding i5/OS user profiles are disabled. Use the Disable User Profile parameter on the Change Network Server Description (CHGNWSD) or Create Network Server Description (CRTNWSD) commands. See "Configuring the QAS400NT user for user enrollment on integrated Windows servers" on page 139 for more information.

QAS400NT or QFPAD user and integrated servers

The i5/OS operating system uses the QAS400NT (Windows) or QFPAD (Linux) user to sign on to the integrated server operating system.

QAS400NT user

The QAS400NT user is used to enroll i5/OS users in groups or domains for i5/OS NetServer to apply updates to the integration software. See "Configuring the QAS400NT user for user enrollment on integrated Windows servers" on page 139 for more information.

QFPAD user

This QFPAD user is used to sign into integrated Linux servers that use the Extended Integrated Server Support licensed program.

i5/OS password considerations for integrated Windows servers

You can change i5/OS system values to configure the rules for passwords and ensure that they will work correctly for your environment.

1. Make sure that the i5/OS QRETSVRSEC system is set to 1. You can do this with the Work with System Values (WRKSYSVAL) command. If you do not do this, you will be unable to enroll users on your integrated Windows server until they sign on to i5/OS.

   Note: This system value is also required for iSCSI integrated server support.

2. The user should use i5/OS passwords containing only characters and password lengths allowed in Windows passwords if they want to enroll users. The password level of i5/OS can be set to allow for user profile passwords of 1 - 10 characters or to allow for user profile passwords of 1 - 128 characters. An i5/OS password level change of the system value QPWDLVL requires an IPL.

3. The i5/OS password level of 0 or 1 supports passwords of 1 - 10 characters and limits the set of characters. At password level 0 or 1, i5/OS converts passwords to all lowercase for Windows.

4. The i5/OS password level of 2 or 3 supports passwords of 1 - 128 characters and allows more characters including uppercase and lowercase characters. At level 2 or 3, i5/OS preserves password case sensitivity for Windows.

5. When the i5/OS passwords of enrolled users expire, their Windows passwords also expire. Users can change their passwords on Windows, but they must remember to also change their passwords on i5/OS. Changing the i5/OS password first automatically changes the Windows password.

6. If the i5/OS system value QSECURITY is 10, the Windows users that are created do not require passwords to sign-on. All other i5/OS QSECURITY levels require that a user object have a password to sign-on. You can find more information about security levels in the Security reference topic collection.

7. If you are using a language other than English, be aware that using anything but invariant characters in user profiles and passwords can cause unpredictable results. The i5/OS globalization topic contains information about what characters are in the invariant character set. This statement is only true when QPWDLVL is 0 or 1. When QPWDLVL is 2 or 3, invariant characters can be used without causing any problems.

User accounts for integrated Windows servers

You can manage passwords for Windows users in either Windows or the i5/OS operating system.

Traditional user (password managed by i5/OS)

By default users are set to this type. This user works in both Windows and i5/OS. The i5/OS password and Windows password will be synchronized. Each time that the integrated Windows server is restarted, the user's password will be reset to the i5/OS password. Password changes can only be made in i5/OS. This user type is recommended for running File Level Backup and remote Windows commands. To set a Windows user to this configuration, use WRKUSRPRF to set the user profile attribute LCLPWDMGT to *YES.

Windows password-managed user

This person does all or most of their work in Windows and may never, or rarely, sign on to i5/OS. If the user signs-on to i5/OS, they must use an authentication method such as Kerberos to access i5/OS. This is discussed in the next section: Windows user with Enterprise Identity Mapping (EIM) configured.

When the user profile attribute LCLPWDMGT(*NO) is defined for an i5/OS user, the i5/OS user profile password is set to *NONE. The i5/OS enrollment password is saved until Windows enrollment is successfully completed. After the i5/OS user is enrolled to Windows, the Windows user may change and manage their password in Windows without i5/OS overwriting their password. Using this method allows for a more secure environment because there are fewer passwords being managed. To read how to create a user of this type, see "Changing the LCLPWDMGT user profile attribute" on page 143.

Windows user with Enterprise Identity Mapping (EIM) associations automatically configured

Specifying the user profile attribute of EIMASSOC to be *TGT, TGTSRC, or *ALL allows the integrated server to automatically define EIM Windows source associations. Using the automatic definitions of associations makes configuring EIM easier. To read how to create a user of this type, see "Configuring Enterprise Identity Mapping for integrated Windows servers" on page 143.

Windows user with Enterprise Identity Mapping (EIM) associations manually configured

The user may choose to manually define EIM Windows source associations. This method may be used to set the i5/OS user profile to be enrolled to a different Windows user profile name. The user must manually define an i5/OS target association for the i5/OS user profile and also a Windows source association for the same EIM identifier.

Table 3. Types of user configurations

User type	Function provided	User profile definition
Traditional	- Both i5/OS and Windows fully functional. - Easy to configure. - Password is changed from i5/OS. - i5/OS and Windows user ID and passwords will be identical. - Recommended for system administrators, users who frequently use i5/OS, or for systems which use i5/OS for back up and restoration of user profiles.	LCLPWDMGT(*YES) and no EIM Windows source associations defined.
Windows password-managed user	- Password can be changed from Windows. - Simple configuration. - Windows password administration makes this configuration more secure because the i5/OS password is *NONE. - i5/OS sign-on requires an authentication method such as System i Navigator provides by its support of i5/OS sign-on using Kerberos.	LCLPWDMGT(*NO)
Windows user with Enterprise Identity Mapping (EIM) associations auto configured	Automatic creation of Windows source associations makes it easier to set up and configure to use Kerberos enabled applications.	For example: EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)
Windows user with Enterprise Identity Mapping (EIM) associations manually configured	Allows the user to define EIM associations for enrolled i5/OS user profiles to be different user profiles in Windows.	Use System i Navigator to manually define EIM i5/OS target associations and Windows source associations.

User enrollment templates for integrated Windows servers
You can use templates to simplify the enrollment of new users to integrated Windows server.

Rather than manually configure many new users, each with identical settings, use a user enrollment template to automatically configure them. Each template is a Windows user profile that defines user privileges, such as group membership, directory paths, and organizational unit containers.

When you enroll users and groups from i5/OS to the Windows environment, you can specify a user template on which to base the new Windows users. For example, you could create a user template and name it USRTEMP. USRTEMP could be a member of the Windows server groups NTG1 and NTG2. On i5/OS, you could have a group called MGMT. You could decide to enroll the MGMT group and its

members to a Windows server. During the enrollment process, you could specify USRTEMP as the user template. During enrollment, you automatically add all members of the MGMT group to the NTG1 and NTG2 groups.

User templates save you from having to set up group memberships individually for each user. They also keep the attributes of enrolled users consistent.

You can make a user template a member of any Windows group, whether you enrolled that group from i5/OS or not. You can enroll users with a template that is a member of a group that was not enrolled from i5/OS. If you do this, however, the users become members of that nonenrolled group as well. i5/OS does not know about groups that were not enrolled from i5/OS. This means that you can only remove users from the group by using the User Manager program on Windows.

If you use a template to define a new user enrollment, and the template has a folder or directory **Path** or **Connect To** defined, the newly-created Windows user will have the same definitions. The folder definitions allow the user administrator to take advantage of folder redirection and to manage terminal service sign-on.

If you use a template when you define a new user enrollment, and the template is a user object in a Windows Active Directory organizational unit container, the newly created Windows user object will be in the same organizational unit container. An organizational unit provides a method to grant users administrative control to resources.

You can change existing user templates. Such changes affect only users that you enroll after you change the template.

You use templates only when you create a newly enrolled user in the Windows environment. If you perform enrollment in order to synchronize an existing Windows user with an i5/OS counterpart, Windows ignores the template.

Related tasks

"Creating user enrollment templates for integrated Windows servers" on page 141
Follow these steps to create user enrollment templates.

i5/OS NetServer for integrated Windows servers

You must configure i5/OS NetServer to enable updates to the IBM i5/OS Integrated Server Support software that runs on the Windows operating system. You can also configure print and file sharing.

i5/OS NetServer enables Windows clients to connect to i5/OS shared directory paths and shared output queues by way of TCP/IP. To install service packs, you must be signed on with a Windows account that corresponds to an i5/OS user profile with the same password, or you must have a guest NetServer user profile configured.

To set up i5/OS NetServer to perform maintenance tasks, use the method found in the Getting started with i5/OS NetServer topic.

Once you have set up i5/OS NetServer, you need to set up a Windows user with access to i5/OS NetServer, or you can set up an i5/OS NetServer guest user profile.

System i Access and integrated servers

System i Access enables you to connect to the System i product running the i5/OS operating system. System i Access provides support for System i Navigator. It also provides functionality such as an Open Database Connectivity (ODBC) driver that can be used for server-to-server applications between integrated servers and the i5/OS operating system.

It features a complete set of integrated functions that enable desktop users to use i5/OS resources as easily as their local PC functions. With System i Access, users and application programmers can quickly process information, applications, and resources for their entire company.

You can enable Open Database Connectivity (ODBC) to run as a Windows service by installing System i Access for Windows on your integrated server. This enables you to write server applications that call the ODBC device driver to access DB2 for i5/OS.

To enable ODBC to be started from a Windows service, run the CWBCFG command with the /s option after you install System i Access for Windows.

As a single user signed on to Windows, you have full support for all other System i Access for Windows features.

Additional information sources:
- See i5/OS NetServer vs System i Access for Windows in the i5/OS NetServer topic collection.

Software updates for integrated servers

There are several types of software updates for iSCSI-attached integrated servers.

Updates to i5/OS and firmware

You should update the following software and firmware for integrated servers.

Table 4. Methods for applying software updates for integrated servers

Component	Methods for applying software updates
i5/OS, and related licensed products	Apply PTFs. See i5/OS PTFs (www.ibm.com/ systems/i/bladecenter/ptfs.html) on the System i integration with BladeCenter and System x Web site for information about the latest PTFs.
IBM i5/OS Integrated Server Support option and the IBM i5/OS Extended Integrated Server Support licensed program software that run on the integrated server operating system	Apply i5/OS PTFs and then run a utility from the integrated server operating system. • "Installing updates to the Integrated Server Support software running on Microsoft Windows" on page 129 • "Maintaining the Linux integration code" on page 177 • "Updating the integration software for VMware ESX Server" on page 167
iSCSI initiator BIOS and firmware	To update the iSCSI initiator firmware in a System x or blade server, see the Updating iSCSI initiator firmware task in the iSCSI Initiator Hardware Configuration document.
System x or BladeCenter updates	You might need to update the firmware for the System x, blade, or BladeCenter hardware. See "Downloading updates for the blade server and the BladeCenter chassis" on page 93 or "Downloading firmware updates for System x hardware" on page 90.
Integrated server operating system	Apply updates at the integrated server console

Updates for integrated Windows servers

The updates for the i5/OS Integrated Server Support code that enables Microsoft Windows server to run on the integrated server are separate from the service packs for Windows itself, which you must get from Microsoft.

The process of installing code fixes on your integrated servers is called synchronization. When you synchronize an integrated server, the integration software ensures that the integration software on the integrated server is at the same service pack and release level as the i5/OS integration software. The level of code on the Windows side is dependent on the level of code on the i5/OS side.

When you use the integration software to synchronize an integrated server, there are four things that can happen:

1. If i5/OS has been upgraded to a new release, for example, from V5R4 to V6R1, the software for the new release will replace that of the old release.
2. If a new IBM i5/OS Integrated Server Support service pack has been installed on i5/OS, it will be copied over to the integrated server.
3. If an IBM i5/OS Integrated Server Support service pack has been removed from i5/OS, it will be removed from the integrated server as well, and replaced with the code currently existing in i5/OS.
4. If the i5/OS integration code and integrated server code are at the same level, the synchronization operation can still be performed. This allows for recovery of a deleted or damaged file on the integrated server.

In all cases the integrated server will be brought to the same level of software which exists in i5/OS.

Updates for integrated VMware servers

See "Updating the integration software for VMware ESX Server" on page 167 for information about updating the IBM integrated server support software.

Install updates to the VMware ESX operating system at the VMware console.

Updates for integrated Linux servers

See "Maintaining the Linux integration code" on page 177 for information about updating the IBM integrated server support software.

Install updates to the Linux operating system at the Linux console.

Related tasks

"Installing updates to the Integrated Server Support software running on Microsoft Windows" on page 129
IBM i5/OS Integrated Server Support includes components that run on i5/OS and the Windows operating system.

Related information

iSCSI Initiator Hardware Configuration

iSCSI-attached integrated server installation road map

This road map contains an outline of the tasks you will do to install the integrated server.

Check the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/) for updates before installing an integrated server.

iSCSI-attached integrated server installation checklist

__ Prerequisites

   __ Ensure that you have access to the required documentation. See "Documentation prerequisites for installing an iSCSI-attached integrated server" on page 90

   __ Review iSCSI concepts. See "Concepts for iSCSI-attached integrated servers" on page 5.

   __ Verify that you have access to the required i5/OS products, firmware, and updates. See "Software and firmware requirements for BladeCenter integration" on page 57 or "Software and firmware requirements for System x integration" on page 59.

   __ Load required i5/OS products, firmware, and updates. See "Installing the required i5/OS licensed programs and options for integrated servers" on page 106.

   __ Prepare i5/OS for use with integrated servers. See "Configuring i5/OS for iSCSI-attached integrated servers" on page 106.

   __ Obtain integrated server operating system installation media. See the iSCSI install read me first Web page.

__ Prepare for the hardware installation.

   __ Obtain System x, BladeCenter, network, and iSCSI HBA hardware. See "Hardware requirements for BladeCenter integration" on page 54 or "Hardware requirements for System x integration" on page 55.

   __ Obtain firmware updates and drivers for your hardware. See "Software and firmware requirements for BladeCenter integration" on page 57 or "Software and firmware requirements for System x integration" on page 59.

   __ Plan the iSCSI network. See "iSCSI Network Planning Guide" on page 62.

__ Hardware installation

   __ Install the System i iSCSI HBAs. See "Installing the iSCSI target in the server running i5/OS" on page 95.

   __ Install the BladeCenter or System x hardware and iSCSI HBAs. See "Installing the iSCSI initiator on the integrated server hardware" on page 95.

   __ Configure the BladeCenter or System x iSCSI HBAs. See "Updating the System x firmware and configuring the System x hardware" on page 95 or "Updating and configuring the BladeCenter chassis" on page 101.

   __ Cable the iSCSI network. See "Cabling the iSCSI network" on page 105.

__ Prepare for the operating system installation

   __ Create an NWSH object for each new System i iSCSI HBA. See "Creating an NWSH object for each new System i iSCSI HBA port" on page 110.

   __ Start the NWSH object for each System i iSCSI HBA port that the server will use. See "Starting the NWSH for each System i iSCSI HBA port that the server will use" on page 111.

   __ If you are using IBM Director for integrated server discovery and power control, ensure that IBM Director Server is started. See "Verifying that Director Server is installed and running" on page 228.

   __ Create and initialize a service processor configuration object. See "Creating and initializing a service processor configuration object for the integrated server hardware" on page 111.

   __ Create a remote system configuration object. See "Creating a remote system configuration object for an integrated server" on page 113.

   __ Verify the remote system configuration and that the remote system is powered off. See "Verifying that the initiator system is accessible and powered off or offline" on page 114.

   __ Create a connection security configuration object. See "Creating a connection security configuration object" on page 115.

__ Operating system installation

   __ Plan for the server operating system installation. See "Windows server installation advisor" on page 116 or "Installing the Linux operating system" on page 169.

   __ Review i5/OS memory requirements and plan for a shared data memory pool. See "i5/OS memory requirements" on page 60.

   __ Start the installation from the i5/OS console. Select one of the following tasks:

      • "Starting the Windows installation at the i5/OS console" on page 122

      • "Starting the VMware ESX Server installation from the i5/OS console" on page 165

      • "Starting the Linux installation at the i5/OS console" on page 170

__ Continue the installation from the integrated server console. Select one of these tasks.
- "Continuing the Windows Server 2003 installation from the integrated server console" on page 126
- "Continuing the Windows Server 2008 installation from the Windows console" on page 128
- "Continuing the installation at the VMware ESX console" on page 166
- "Continuing the installation from the Linux console" on page 175

__ After the operating system installation
__ Complete the server installation. Select one of these tasks:
- "Completing the Windows server 2003 installation" on page 126
- "Completing the Windows Server 2008 installation from the Windows console" on page 128
- "Running the post install utility" on page 167
- "Completing a SLES 10 installation" on page 175 or "Completing a RHEL5 installation" on page 176

__ Keep the i5/OS Integrated Server Support software up to date on i5/OS and on the integrated server operating system. See "Software updates for integrated servers" on page 51.
__ Scale the iSCSI network. See "Scaling the iSCSI Network" on page 28.

Planning for iSCSI-attached integrated servers

Use these tasks to plan for the hardware, software, and networking information that you will need to install an integrated server.

Hardware requirements for BladeCenter integration

Supported hardware, switches, and cables are required for integrated servers.

See the System i integration with BladeCenter and System x ![icon] (www.ibm.com/systems/i/bladecenter/) Web page for the latest information about hardware that has been tested with integrated server solutions.

Read BladeCenter and System x models supported with iSCSI ![icon] and the associated notes.

Supported BladeCenter hardware

Ensure that you have the following items before starting your installation:
- Diskless blade server.
- BladeCenter for housing blade servers.
- iSCSI expansion card or cards (also referred to as iSCSI HBA). Use one of these for each blade server you plan to attach. See the iSCSI host bus adapter (iSCSI HBA) ![icon] Web page for information about supported iSCSI HBAs.
- Management module installed in the BladeCenter to function as service processor hardware.
- I/O module in the appropriate BladeCenter I/O bay to support the network connection for the blade system iSCSI expansion card. This I/O module can be an integrated gigabit switch which can take the place of an external switch in the iSCSI network or a pass-through module which would require an external switch.
- Mouse, keyboard, and display, which can be attached using a KVM switch.
- The documentation that is included with your BladeCenter, blade server and options – hardcopy, CD, or both.

Supported iSCSI host bus adapter (HBA)

- iSCSI Host Bus Adapter. See the iSCSI host bus adapter (iSCSI HBA) ![icon] Web page for information about supported iSCSI HBAs.

- Network adapter

  Tip: The network adapter does not need to be dedicated to the iSCSI HBA and might already be installed.

Supported switches and cables

Ensure that you have the required hardware for networking.
- You need one or both of these items:
  - BladeCenter I/O module switch
  - Pass-through module, either connected to an external gigabit Ethernet switch, or available for direct connection to target HBAs in the System i product

    Note: iSCSI HBAs in a BladeCenter system have two ports. A single switch module or pass-through module enables the use of one port of all iSCSI HBAs in the BladeCenter system. A second switch module or pass-through module enables the use of the other port of all iSCSI HBAs in the BladeCenter system. A second switch module or pass-through module, along with multiple target iSCSI HBAs, is useful for multipath I/O.
- A network for the service processor and Ethernet ports on the blade systems
- Ethernet cables:
  - One cable from each target iSCSI HBA in the System i hardware to the iSCSI network (category 5e or better, or fiber optic).
  - One cable from each service processor hardware Ethernet port to the network providing the service processor connection.
  - One cable from a hosting System i network adapter to the network providing the service processor connection.
  - Any additional cables that you might need to connect the Ethernet ports on the blade systems to a network, if desired.

Network interface card (NIC) for iSCSI-attached VMware ESX Server and Linux servers

If you are running the Linux or VMware ESX operating system on the integrated server, you also need to use an integrated Ethernet adapter or install a network adapter in the integrated server hardware. The i5/OS operating system uses this adapter to communicate with the integrated server for administrative functions.

Additional hardware and supplies

Ensure that you have additional equipment and supplies you might need:
- Additional computer with a network interface capable of running web browser software (used to update and configure service processor hardware on the BladeCenter system.)
- Writable media diskettes or compact discs.

Hardware requirements for System x integration

Supported hardware, software, switches, and networking cables are required for System x integration.

See the System i integration with BladeCenter and System x ![icon] (www.ibm.com/systems/i/bladecenter/) Web page for the latest information about hardware that has been tested with integrated server solutions.

Read BladeCenter and System x models supported with iSCSI and the associated notes.

Supported System x hardware

Ensure that you have the following items before starting your installation:

- Diskless System x product.

- iSCSI Host Bus Adapter for System x product. See the iSCSI host bus adapter (iSCSI HBA) Web page for information about supported iSCSI HBAs.

- Service processor hardware. Refer to the System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/) Web page to determine which of the following type of service processor hardware are required:
  - One of three versions of Remote Supervisor Adapter II (RSA II,) depending on the System x type and model: RSA II, RSA II – EXA, RSA II SlimLine
  - Baseboard Management Controller for System x models that do not require the RSA II
- Mouse, keyboard, and display that can be attached through a KVM switch
- USB diskette drive. Some System x models do not have an integrated diskette drive and require a diskette drive for firmware updates
- The documentation that is included with your System x server (hardcopy or compact disc)

Supported iSCSI host bus adapter (HBA)

- iSCSI Host Bus Adapter. See the iSCSI host bus adapter (iSCSI HBA) Web page for information about supported iSCSI HBAs.
- Network adapter

  Tip: The network adapter does not need to be dedicated to the iSCSI HBA and might already be installed.

Network interface card (NIC) for iSCSI-attached VMware ESX Server and Linux servers

If you are running the Linux or VMware ESX operating system on the integrated server, you also need to use an integrated Ethernet adapter or install a network adapter in the integrated server hardware. The i5/OS operating system uses this adapter to communicate with the integrated server for administrative functions.

Supported switches and cables

Ensure that you have the required hardware for networking.

- If you are not using a direct connection between iSCSI HBAs, you will need one or more Gigabit Ethernet switches. Multiple switches, along with multiple iSCSI HBAs in both the System x and System i integration with BladeCenter and System x products, are useful for multipath I/O.
- A network for the service processor and Ethernet ports in the System x product.
- Ethernet cables:
  - One cable from each iSCSI HBA in the System x product to the iSCSI network (category 5e or better, or fiber optic).
  - One cable from each iSCSI HBA in the hosting System i server to the iSCSI network (category 5e or better, or fiber optic).
  - One cable from each service processor hardware Ethernet port to the network providing the service processor connection.
  - One from a hosting System i network adapter to the network providing the service processor connection.

– Any additional cables you might need to connect the Ethernet ports in the System x server to a network, if desired.

Additional hardware and supplies

Ensure that you have additional equipment and supplies you might need:
- Additional computer with a network interface capable of running web browser software. Use this system to update and configure service processor hardware on System x product.
- Writable media diskettes or compact discs.

Software and firmware requirements for BladeCenter integration

This topic lists the software and firmware requirements for integrating blade hardware.

i5/OS software

You need the following licensed programs and options for integrated servers. You will be prompted to install this software during the installation process.
- IBM i5/OS (5761-SS1)
- Extended Base Support (5761-SS1 option 1)
- Online Information (5761-SS1 option 2)
- Extended Base Directory Support (5761-SS1 option 3)
- Host Servers (5761-SS1 option 12)
- Integrated Server Support (5761-SS1 option 29)
- Qshell (5761-SS1 option 30)[1]
- Digital Certificate Manager (5761-SS1 option 34)
- IBM HTTP Server for i5/OS (5761-DG1)[1]
- IBM Developer Kit for Java™ (5761-JV1)[1]
- Java Developer Kit 1.4 (5761-JV1 option 6)[1]
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
- IBM System i Access for Windows (5761-XE1)[3]
- IBM Extended Integrated Server Support for i5/OS (5761-LSV)[2]
- Optional: IBM Director (5722-DR1) 5.20.2 or later[4,5]

Note:

1. This product is required for iSCSI-attached integrated servers
2. This product is required for running the Linux or VMware ESX Server operating systems.
3. Use the System i Navigator graphical interface to perform i5/OS iSCSI configuration tasks, whenever possible. System i Navigator is part of System i Access for Windows.

Attention: Use of System i Navigator is optional. Almost all of the tasks that the graphical interface supports have CL command equivalents, so you can use CL commands if you prefer to do so. However, the CL command prompter has permanent restrictions that adversely affect prompting of some commands, so the graphical interface is easier to use for some tasks. See the CRTNWSCFG and CHGNWSCFG Prompting Problems When Defining More Than One Remote Interface Software Knowledge Base document for more information.

Select either a full installation or install these components:
- Configuration and Service
- Network
- Integrated Server Administration

4. Release and installation media are separate from 5761-SS1. Install this licensed program using the i5/OS Restore Licensed Program (RSTLICPGM) command. See the Installing IBM Director Server on i5/OS topic collection in the IBM Systems Software Information Center for additional software requirements and updates. You do not need to install IBM Director Console.

5. IBM Director is not a required product if the Service Processor Manager function of i5/OS Integrated Server Support is used. See "Configuring i5/OS to use Service Processor Manager" on page 107 for more information.

For more information about the installation of required software, see the Installing, upgrading, or deleting i5/OS and related software topic collection.

Installation media for the integrated server operating system

You need access to installation media or an installation image for a supported operating system. The "iSCSI-attached integrated server installation road map" on page 52 tells you when and how to prepare the installation media.

See the iSCSI install read me first Web page for the latest information about supported operating systems.

Table 5. Operating systems that are supported on iSCSI-attached integrated servers

Operating system	Supported versions
Microsoft Windows	• x86 Microsoft Windows Server 2003 editions • x64 Microsoft Windows Server 2008 editions
VMware ESX Server	VMware ESX 3
Linux	• SUSE Enterprise Linux Server 10 for AMD64 and Intel EM64T (SLES 10) • Red Hat Enterprise Linux 5 for x86-64 (RHEL 5)

Firmware for the blade and BladeCenter chassis

You will need to download and install updates to the blade system and the BladeCenter chassis.

See "Downloading updates for the blade server and the BladeCenter chassis" on page 93.

iSCSI host bus adapter firmware

Download the firmware for the iSCSI host bus adapter (HBA) before you begin installing the integrated server. See "Downloading firmware updates for initiator iSCSI HBAs" on page 95.

Software and firmware requirements for System x integration

This topic lists the software and firmware requirements for System x integration.

i5/OS software

You need the following licensed programs and options for integrated servers. You will be prompted to install this software during the installation process.

- IBM i5/OS (5761-SS1)
- Extended Base Support (5761-SS1 option 1)
- Online Information (5761-SS1 option 2)
- Extended Base Directory Support (5761-SS1 option 3)
- Host Servers (5761-SS1 option 12)
- Integrated Server Support (5761-SS1 option 29)
- Qshell (5761-SS1 option 30)[1]
- Digital Certificate Manager (5761-SS1 option 34)
- IBM HTTP Server for i5/OS (5761-DG1)[1]
- IBM Developer Kit for Java (5761-JV1)[1]
- Java Developer Kit 1.4 (5761-JV1 option 6)[1]
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
- IBM System i Access for Windows (5761-XE1)[3]
- IBM Extended Integrated Server Support for i5/OS (5761-LSV)[2]
- Optional: IBM Director (5722-DR1) 5.20.2 or later[4,5]

Note:

1. This product is required for iSCSI-attached integrated servers
2. This product is required for running the Linux or VMware ESX Server operating systems.
3. Use the System i Navigator graphical interface to perform i5/OS iSCSI configuration tasks, whenever possible. System i Navigator is part of System i Access for Windows.

   Attention: Use of System i Navigator is optional. Almost all of the tasks that the graphical interface supports have CL command equivalents, so you can use CL commands if you prefer to do so. However, the CL command prompter has permanent restrictions that adversely affect prompting of some commands, so the graphical interface is easier to use for some tasks. See the CRTNWSCFG and CHGNWSCFG Prompting Problems When Defining More Than One Remote Interface Software Knowledge Base document for more information.

   Select either a full installation or install these components:
   - Configuration and Service
   - Network
   - Integrated Server Administration
4. Release and installation media are separate from 5761-SS1. Install this licensed program using the i5/OS Restore Licensed Program (RSTLICPGM) command. See the Installing IBM Director Server on i5/OS topic collection in the IBM Systems Software Information Center for additional software requirements and updates. You do not need to install IBM Director Console.
5. IBM Director is not a required product if the Service Processor Manager function of i5/OS Integrated Server Support is used. See "Configuring i5/OS to use Service Processor Manager" on page 107 for more information.

Installation media for the integrated server operating system

You need access to installation media or an installation image for a supported operating system. The "iSCSI-attached integrated server installation road map" on page 52 tells you when and how to prepare the installation media.

See the iSCSI install read me first Web page for the latest information about supported operating systems.

Table 6. Operating systems that are supported on iSCSI-attached integrated servers

Operating system	Supported versions
Microsoft Windows	• x86 Microsoft Windows Server 2003 editions
	• x64 Microsoft Windows Server 2008 editions
VMware ESX Server	VMware ESX 3
Linux	• SUSE Enterprise Linux Server 10 for AMD64 and Intel EM64T (SLES 10)
	• Red Hat Enterprise Linux 5 for x86-64 (RHEL 5)

Firmware for the System x product

Before beginning the installation, you should download a supported version of firmware for the System x product. See "Downloading firmware updates for System x hardware" on page 90.

iSCSI host bus adapter firmware

Firmware is required for the iSCSI host bus adapter (HBA).

See "Downloading firmware updates for initiator iSCSI HBAs" on page 95.

Windows Server 2008 iSCSI driver

If you are using either of the following iSCSI HBAs on your System x server and plan to install Windows Server 2008, first download the Windows Server 2008 iSCSI driver from the QLogic BladeCenter and

System x Software Updates for Integration with IBM i Web page. You need this driver during the operating system installation.
• QLogic iSCSI Single-Port PCIe HBA for IBM System x (PN 39Y6146)
• QLogic iSCSI Dual-Port PCIe HBA for IBM System x (PN 42C1770)

After you download the driver, extract the driver files into a local directory on your PC and copy them to a blank diskette, CD, DVD, or USB key. Choose media corresponding to a device that is available on your System x server. Then use this media to install the iSCSI driver when you install Windows Server 2008 on the server.

i5/OS memory requirements

iSCSI-attached integrated servers use a combination of memory in the i5/OS machine, base and optional shared data memory pools.

Create a shared data memory pool for iSCSI disk I/O, especially if you are planning to have an i5/OS partition with multiple iSCSI-attached servers or with an iSCSI-attached server that performs large amount of disk activity. Under some workloads, iSCSI virtual disk I/O operations might adversely impact other i5/OS applications that share the *BASE memory pool.

The machine memory pool is used for highly-shared machine and operating system programs. The machine memory pool provides storage for jobs the system must run that do not require your attention. If you set the size for these storage pools too small, you will impair system performance. You cannot set QMCHPOOL to less than 256 KB. The size for this memory pool is specified in the machine memory pool size system value (QMCHPOOL). No user jobs run in this memory pool.

See chapter 17 of the System i Performance Capabilities Reference Guide for background information about iSCSI-attached integrated servers and i5/OS memory pools.

Important: The System i Performance Capabilities Reference Guide mentions a QFPHIS subsystem description. It is used only on systems running i5/OS V5R4. Beginning with V6R1, a shared data memory pool is used.

You can display or change the machine pool size by using the Work With System Status (WRKSYSSTS) command. The first storage pool on the WRKSYSSTS display is the machine pool.

You can change the system value QPFRADJ so that the system automatically adjusts system pool sizes. However, because automatic performance adjustment can slow down a busy system, you probably want to limit its use to one of these times:

* The first couple days after the installation
* An hour or so at the time your system load changes from daytime (interactive emphasis) to nighttime (batch emphasis) and back

iSCSI virtual I/O shared data memory pool

By default, the iSCSI disk I/O uses the *BASE memory pool and can cause performance issues for any other applications that are also using the *BASE memory pool. The impact includes (but is not limited to) applications slowing down, applications stopping, and the system slowing down (depending on the number of iSCSI-attached servers and target iSCSI HBAs).

To move the iSCSI disk I/O out of the *BASE memory pool into its own memory pool, configure the shared data memory pool using the Work with Shared Pools (WRKSHRPOOL) command, and configure the iSCSI-attached servers to use it. This change can prevent the iSCSI disk I/O from adversely affecting the performance and any process that runs in the *BASE memory pool.

Select one of the unused general-purpose shared pools (*SHRPOOL*nn* where *nn* is the number of the pool) and specify a size with an activity level of *DATA selected. This allocates the memory to a shared data memory pool that does not allow any thread to run in the same shared memory pool. When installing or configuring the iSCSI-attached network server description, specify the configured shared data memory pool.

The amount of required memory depends on a number of factors, including the number of iSCSI network servers and the expected sustained disk activity for all servers. For most environments, you can use a shared data memory pool with a size of 10 000 KB that is shared among all of the iSCSI-attached servers on your system. If your system has more than five iSCSI-attached servers, allocate at least 4 MB for a shared data memory pool and 1 MB per active network server description.

Tested System i tape and optical devices iSCSI-attached integrated servers

See the System i integration with BladeCenter and System x Web page for information about tape and optical devices that have been tested with iSCSI-attached integrated Windows and Linux servers. iSCSI-attached VMware servers do not support System i tape or optical devices.

- For integrated Windows servers, see Tested tape devices for iSCSI attached Windows servers (www.ibm.com/systems/i/bladecenter/windows/iscsi_tape_support.html).

- For integrated Linux servers, see Tested tape devices for iSCSI attached Linux servers (www.ibm.com/systems/i/bladecenter/linux/iscsi_tape_support.html).

  Related tasks

  "Sharing devices between i5/OS and integrated Windows servers" on page 155
  Use these tasks to configure an integrated Windows server to use i5/OS tape and optical devices.

  "Configuring a System i tape drive for use by Linux" on page 180
  This topic describes the tasks you need to perform to set up a System i tape drive for use by an integrated Linux server.

Integrated server considerations

Learn about key differences between integrated server solutions and standalone systems.

Although an integrated server is much like a PC-based Windows server, here are a few differences that you need to consider:

- There might not be a diskette drive available. This means that you cannot use a startup diskette or an emergency repair diskette. However, you can use System i disk space to back up your files or the entire disk image.

- System i tape and disk devices are available.

- Installing the integrated operating system is different from a typical PC server installation. You first install the IBM i5/OS Integrated Server Support option, then start the operating system installation with the Install Windows Server (INSWNTSVR) command or the Install Linux Server (INSLNXSVR) command.

- On the i5/OS side of server management, an integrated server is represented by a network server description (NWSD), and network interfaces are represented by line descriptions. You can stop and restart the server from i5/OS by varying the NWSD off and on.

- For integrated Windows servers, virtual Ethernet networking allows TCP/IP communication with the System i product without requiring LAN adapters, cables, hubs, or switches. You can do a lot of your user administration tasks from i5/OS, such as creating Windows users.

- Because the i5/OS operating system manages storage differently than a PC server (see "Storage management for integrated servers" on page 15), some techniques necessary to administer storage on a PC server are unnecessary for integrated servers.

iSCSI Network Planning Guide

Use this guide to plan the network connections for the System i and blade or System x hardware.

You will fill in the work sheets at the end of this document with the values that will help you configure your servers later. Do not fill in the work sheets until directed to do so.

You can download this guide as a separate PDF. See System i integration with BladeCenter and System x: iSCSI Network Planning Guide.

The items in the planning work sheets are referred to throughout this document using item identifiers (IDs). For example the Name entry in the i5/OS service processor configuration object work sheet is referred to using item ID SP1. The following work sheet item ID naming convention is used throughout this guide:

SPn Items in the i5/OS service processor configuration object work sheet

XSPn Items in the BladeCenter or System x service processor configuration work sheet

RSn Items in the i5/OS remote system configuration object work sheet

| **CQ**_n_   Items in the iSCSI initiator work sheet

| **NH**_n_   Items in the i5/OS network server host adapter object work sheet

| **CS**_n_   i5/OS connection security configuration object work sheet

| Configuration objects

| i5/OS objects configure aspects of the integrated server connection and hardware.

| Figure 12 on page 64 shows the hardware, connections, and i5/OS objects for the integrated server. The
| item IDs for the fields in the iSCSI network planning work sheets are listed next to components in the
| image. Use this figure to identify the fields as you do the following tasks.
|
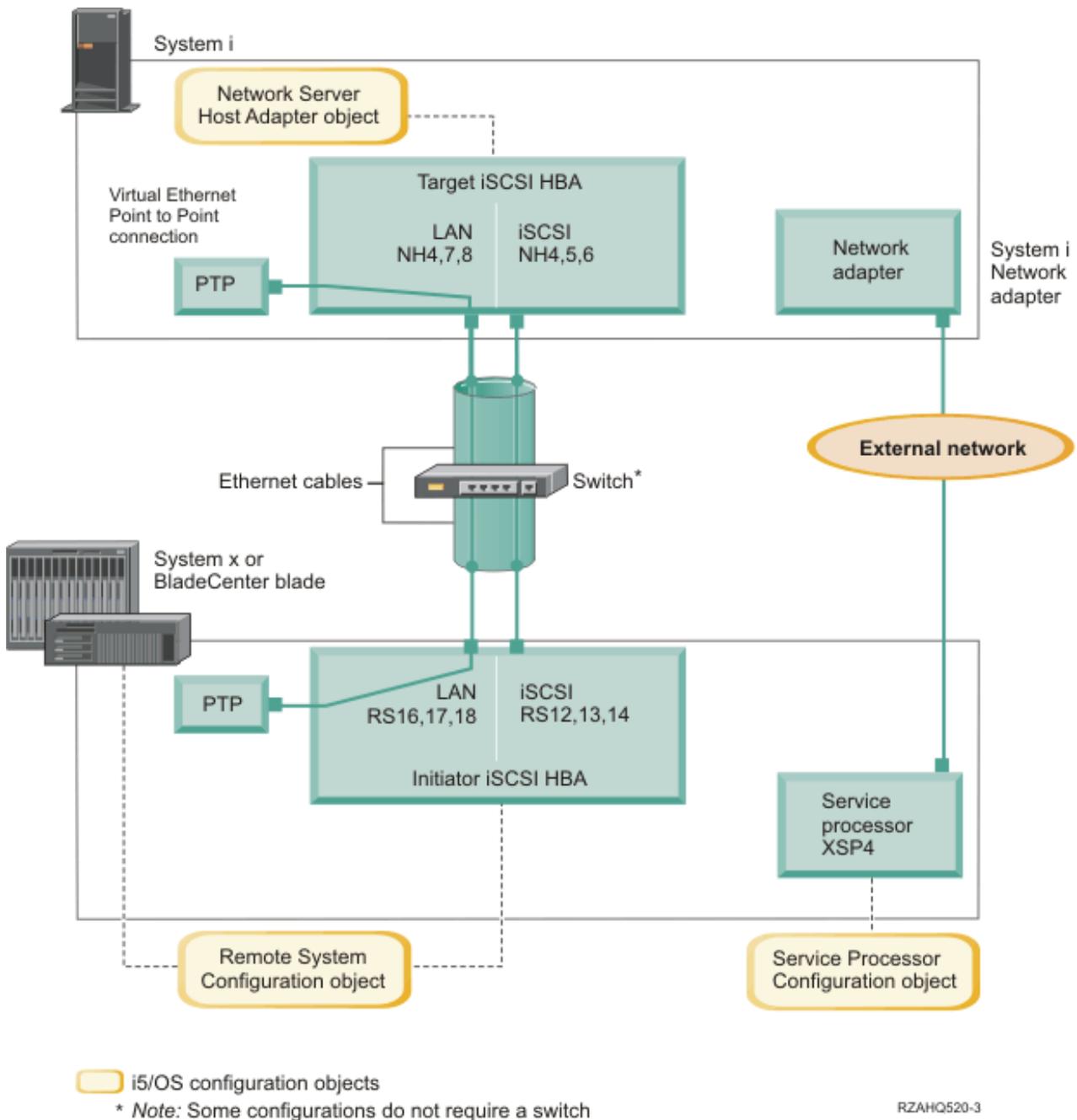
Figure 12. i5/OS configuration objects for iSCSI-attached integrated servers

Recording the configuration information

Do these tasks to select an addressing scheme for the iSCSI network for the integrated server.

You should be familiar with the information in Concepts for iSCSI-attached integrated servers.

Planning network addresses:

You need to specify some of the network addresses for the iSCSI network for the integrated server.

You need to define values for your iSCSI network that include addresses for all of the connections shown in "Configuration objects" on page 63. If you are not sure what value to use, you can use the values in "Selecting IP addresses for the System x or blade iSCSI initiator" on page 74 and "Selecting IP addresses for the System i iSCSI HBA" on page 77. These examples assume that your iSCSI network uses an isolated Ethernet switch and you do not have another network using IP addresses that start with 192.168.99.

If you plan to use your own address scheme, you can verify it with the addresses in the examples.

Planning for the service processor connection:

Do these steps to record the information for the service processor configuration object.
- If you have already created an i5/OS service processor configuration object for the BladeCenter management module or the System x service processor, do the following steps.
  1. Reuse the existing service processor configuration object.
  2. Record the existing service processor configuration object name in work sheet item **SP1**.
  3. Put a check in the box labeled **Existing** in work sheet item **SP1**.
  4. Continue to "Planning for the remote system configuration" on page 69.
- If you need to create a new i5/OS service processor configuration object:
  1. Put a check in the box labeled **New** in worksheet item **SP1**.
  2. Continue with the following tasks.

Identifying a BladeCenter or System x service processor type:

Do these steps to record the type of service processor that is installed in the integrated server hardware.

A BladeCenter enclosure (chassis) can have a:
- Management Module (MM)
- Advanced Management Module (AMM)

A System x model can have a:
- Remote Supervisor Adapter II (RSA II) and a Baseboard Management Controller (BMC)
- BMC only

If you are not sure whether your System x model has an RSA II or just a BMC (without an RSA II), see

the BladeCenter and System x models supported with iSCSI Web page (www.ibm.com/systems/i/ bladecenter/iscsi/servermodels/).
- If the Web page shows that your System x model has an **Included** or **Required** RSA II SlimLine service processor, then your service processor type is an RSA II.
- If the Web page shows that an RSA II SlimLine service processor is **Optional** for your System x model then you need to check your System x model order information to determine if an RSA II SlimLine service processor (part 73P9341) is included as part of your system configuration.

Put a check in the box next to your service processor type in worksheet item **XSP1**.

Selecting a service processor discovery method:

The service processor is a part of a BladeCenter server or a System x product. It has the interface used to power the server on and off. When i5/OS receives information, it saves the information and presents interfaces for interacting with and managing that server.

For the BladeCenter or System x service processor interface, use an external network, such as a company's campus LAN or intranet, rather than using the iSCSI network. The i5/OS operating system uses this interface to discover the service processor and to manage the state of the hosted system. i5/OS is not set up to run these tasks on the iSCSI network. See "Considerations for connecting service processors to i5/OS" on page 80 for considerations that might affect how you configure your network for i5/OS to service processor communications.

The i5/OS operating system can use the following methods to discover a server on its network. Not all options work for all types of service processors.

Discovery by IP address

- This discovery method is recommended since it supported by all types of service processors and does not require a DNS server or support for multicast addressing.

Discovery by host name

- You can use this discovery method for Remote Supervisor II (RSA II), Management Module, or Advanced Management Module service processors. The network that the service processor is connected to must include a DHCP server.

Discovery by service location protocol (SLP)

You can use this discovery method for Remote Supervisor II (RSA II), Management Module, or Advanced Management Module service processors. This discovery method is supported only if you use IBM Director to discover the server. If you use the Service Processor Manager function of i5/OS Integrated Server Support, then use either the discovery by IP address or discovery by host name method.

Decide the discovery method you will use for the service processor and do one of the following:

To check which methods work with which service processors, and to see more information on these methods see Service processor connection for integrated servers.

- If you select **discovery by IP address**, do the following steps.
  1. Put a check in the box labeled Internet address in work sheet item **SP4**.
  2. Optional: Record the service processor host name in work sheet item XSP2 (can be blank). If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.
  3. Put a check in the box labeled **Disabled (for DHCP)** in work sheet item **XSP3**.
  4. Fill in address values for work sheet items **XSP4**, **XSP5**, and **XSP6**.

     You need to choose a TCP/IP address subnet that allows the i5/OS operating system and the service processor to communicate readily.

     If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign an IP address to the service processor using your normal LAN IP address assignment policies, the same as if you were adding another PC to your network.

- If you **select discovery by host name**, do the following steps.
  1. Put a check in the box labeled Host name in work sheet item **SP3**.
  2. Record the service processor host name in work sheet item **XSP2**. If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.

     Important: Make sure that the service processor host name that you specify is registered in your network domain name server (DNS).

3. Put a check in the box labeled **Enabled** (for DHCP) in work sheet item **XSP3**.

4. Leave work sheet items **XSP4**, **XSP5**, and **XSP6** blank.

Recording the system serial number and type/model:

Do these steps to record the serial and type/model information for the integrated server hardware.

1. On the BladeCenter or System x chassis, find the label that contains the system serial number, type and model values. If you are installing a blade, find the values for the BladeCenter chassis. Do not use the label on the blade.

2. If you are installing a System x model with only a BMC service processor (no RSA II) installed, leave worksheet items **SP5** and **SP6** blank. Continue to "Assigning an i5/OS Server Processor Configuration object name."

3. For all other configurations, do the following steps.

   a. Record the serial number value in worksheet item **SP5**.

   b. Record the type and model values in worksheet item **SP6**. Do not include a space or dash ('-') in the type and model value. For example, record 88721RU for a System x model x460 with type 8872 and model 1RU.

Assigning an i5/OS Server Processor Configuration object name:

You need to assign a name to the i5/OS service processor configuration object that you will create to configure the i5/OS connection to the BladeCenter or System x service processor.

The service processor configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention to help you associate the service processor configuration name to the physical hardware (BladeCenter or System x model) that contains the service processor.

For example, you could use SP*sssssss* where *sssssss* is the last 7 characters of the BladeCenter chassis (not the blade) or the System x serial nmber.

Notes:

1. The service processor configuration name cannot match the associated i5/OS remote system configuration name.

2. Using the NWSD name as part of the service processor configuration name works fine for simple configurations where there is a one-to-one relationship between NWSDs and service processors. However, in more complex configurations, the same service processor configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same service processor hardware (multiple blades in a BladeCenter) or the NWSD could be switched to use different "hot spare" server hardware, so that the service processor configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the service processor configuration name.

Record values for the following work sheet items.

1. Fill in the name you choose in work sheet item **SP1**.

2. Fill in a description of the object (up to 50 characters) in item **SP2**.

Selecting a Login ID and Password for the Service Processor:

When you connect directly to the BladeCenter or System x service processor via a LAN, you must specify a login ID (user name) and password.

It is strongly recommended that you define a unique login ID that will be used only by the i5/OS partition or system that will control your BladeCenter or System x through its service processor. Each BladeCenter or System x service processor can only have one controlling partition or system. A BladeCenter Advanced Management Module (AMM) allows more than one controlling partition or system if properly configured – see "Considerations for multiple connections to a BladeCenter Advanced Management Module." Use a naming convention that ties the service processor login ID to the hosting i5/OS logical partition (or the system name for a non-partitioned system). For example, if the hosting i5/OS logical partition name is ROCH03, then the service processor login ID could be set to ROCH03.

You can use the system BIOS interface, the Management Module (MM) or Advanced Management Module (AMM), or the RSA II Web interfaces to set the login ID and password. You also need this information to synchronize the i5/OS service processor configuration with the BladeCenter or System x service processor before installing the operating system on the server. i5/OS uses the login ID and password to connect to the System x or blade model to do specific management tasks (for example, to start the server).

Important: In order for the unique login ID to be effective, it is strongly recommended that you do the following where instructed in later steps.

- Disable or change the default login ID. Service processors have a default login ID of USERID (upper case) with a password of PASSW0RD (upper case, where 0 is the number 0 instead of the letter O). This action protects against unauthorized access to your server.
- If the service processor is currently configured with login IDs that are used by management servers other than the local i5/OS host system (Service Processor Manager or IBM Director Server on another system), disable these login IDs.

If your company has multiple installations of management servers on the same network, take previously mentioned actions to ensure that the service processor does not refuse a connection from the i5/OS operating system. Connection refusal occurs when another management server is already connected. For more information, see Service Processor Connection Refused ➡️ in the IBM Software Knowledge Base.

1. Fill in the new **Login ID** and **Password** values for i5/OS to use in worksheet items **XSP7** and **XSP8**.
2. If the service processor is a Management Module in a BladeCenter or an RSA II in a System x model, you can configure **additional login IDs** and passwords for your administrators to access the service processor from any web browser connected on the same network. If you want to do this, fill in the new **Login ID** and **Password** values for your administrators to use in worksheet items **XSP9** and **XSP10**. You can create up to 12 login ID/password combinations in each service processor. For most environments, you should create an additional login ID and password for use by your administrators.

Considerations for multiple connections to a BladeCenter Advanced Management Module:

If you have a BladeCenter system with an Advanced Management Module (AMM) and firmware BPET23A or later, it can be configured to allow more than one controlling partition or system.

The AMM allows multiple concurrent command mode connections. These connections can be used to allow several management servers (Service Processor Managers or IBM Director Servers), to control the blades in the IBM BladeCenter system.

- Each blade within the BladeCenter should still be controlled (varied on) by a single partition or system at any one time.
- You should change the default Login ID and password for the AMM or disable it as mentioned above. Each partition or system can share Login IDs and passwords or each can have its own unique Login ID and password.
- Each partition or system will need its own i5/OS service processor configuration object for the BladeCenter AMM and each i5/OS service processor configuration object must be synchronized with the BladeCenter AMM.

The AMM must be configured to allow concurrent command-mode connections. The AMM Web interface is used to do this:

1. Sign on to the AMM web interface.
2. Select **Network Protocols** under **MM control**.
3. Page down to the **TCP Command Mode Protocol** section.
4. Change the **command mode** value to the number of desired concurrent connections.
5. Required: Restart the AMM. Use the **Restart MM** option under the **MM control** section.
6. Use the **Login Profiles** under **MM control** to add, change or disable Login IDs and passwords.

Planning for the remote system configuration:

The remote system configuration object defines the communications connections for iSCSI and virtual Ethernet traffic for the System x or blade hardware that will be connecting to the i5/OS operating system.

- If you have already created a remote system configuration object for the System x or blade hardware:
  - Reuse the existing remote system configuration object.
  - Record the existing remote system configuration object name in worksheet item **RS1**.
  - Put a check in the box labeled **Existing** in worksheet item **RS1**.
  - Continue with "Planning for the network server host adapter (NWSH) object" on page 76.
- If you need to create a new i5/OS remote system configuration object:
  - Put a check in the box labeled **New** in worksheet item **RS1**.
  - Continue with the following tasks.

Recording the blade system serial number and type/model:

Do these steps if you are installing a blade system.

1. Open the transparent cover on the front face of the blade server.
2. Record the blade serial number value in worksheet item **RS4**.
3. Record the blade type and model values in worksheet item **RS5**.

> **Note:** Do not include a space or dash (-) in the type and model value.
> For example, record 8843E9U for an HS20 blade with type 8843 and model E9U.

Selecting a name for the remote system configuration:

You need to assign a name to the i5/OS remote system configuration object that you will create to configure the attributes of the iSCSI attached BladeCenter blade or System x model.

The remote system configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention to help you associate the remote system configuration name to the physical server hardware (BladeCenter blade or System x model).

An example naming convention that provides the suggested hardware association is RS*sssssss* where *sssssss* is the last 7 characters of the BladeCenter blade (not chassis) or System x serial number. The appropriate serial number was previously recorded in worksheet item **SP5** for a System x model or worksheet item **RS4** for a blade.

Notes:
1. The remote system configuration name cannot match the associated i5/OS service processor configuration name.

2. You can use the NWSD name as part of the remote system configuration name for simple configurations where there is a one-to-one relationship between NWSDs and the hardware that they use.

   However, in more complex configurations, the same remote system configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same remote system hardware (multiple production or test servers defined to use the same System x hardware at different points in time) or the NWSD could be switched to use different "hot spare" server hardware, so that the remote system configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the remote system configuration name.

1. Fill in the name you choose in worksheet item **RS1**.
2. Fill in a description of the object (up to 50 characters) in item **RS2**.

Selecting a boot parameter delivery method:

An integrated server iSCSI HBA must be configured after it is installed in the System x or blade hardware. Do these steps to select the parameters that you will use.

Before you begin, you need to decide whether to use dynamic addressing (the default) or to use manual addressing for your iSCSI initiator. See Boot modes and parameters for more information about dynamic addressing using the built-in DHCP server. After you begin installing the integrated server, use the iSCSI initiator configuration interface to specify parameters.

You can select either dynamic or manual addressing.

You can use dynamic addressing for most environments. This method requires fewer manual configuration steps and allows some configuration information to be automatically generated, such as iSCSI qualified names (IQNs). With dynamic addressing, the iSCSI attached server uses an integrated DHCP server and you do not need to have a general purpose DHCP server in your network. The integrated DHCP server is intended exclusively to deploy boot parameters to the iSCSI initiator and is not a general purpose DHCP server. When a network server description (NWSD) is varied on, the initiator system is automatically configured with the parameters provided in the i5/OS remote system configuration object.

If you use manual addressing method, some integrated server functions are more difficult to implement, such as the integrated server hot spare capability.

You need the values that you record in the iSCSI network planning work sheets for either method.
- If you use **dynamic** addressing, you configure the parameters in the i5/OS remote system configuration object and the system sends them to the initiator system.
- If you use **manual** addressing, you need to configure both the remote system configuration object in i5/OS and the iSCSI initiator.
1. Put a check in the box next to the boot parameter delivery method you choose in work sheet item **RS6**.
2. Based on your choice for item **RS6**, do one of the following:
   - If you chose **Dynamically delivered to remote system via DHCP**:
     a. Put a check in the box next to the **Dynamic column** heading in the iSCSI initiator work sheet.
     b. Put a check in the box next to DHCP for Port 1 in work sheet item **CQ9**.
   - If you chose **Manually configured on remote system**:
     a. Put a check in the box next to the **Manual** column heading in the iSCSI initiator work sheet.
     b. Put a check in the box next to **Manual** for Port 1 in worksheet item **CQ9**.

Only one of the iSCSI initiator ports can be configured as the boot device during the server installation (the adapter boot mode is set to DHCP or Manual in the iSCSI initiator configuration utility). All other ports must be disabled for boot (the adapter boot mode is set to Disabled in the iSCSI initiator configuration utility), but can be used for non-boot storage or virtual Ethernet traffic.

Note: After the server installation is completed, if the server operating system supports multipath I/O, then additional ports can be enabled for boot.

Selecting Challenge Handshake Authentication Protocol (CHAP) settings:

Challenge Handshake Authentication Protocol (CHAP) is used to authenticate the connection between the System x or blade initiator and the System i target.

CHAP protects against the possibility of an unauthorized system using an authorized system's iSCSI name to access storage. CHAP does not encrypt network traffic, but rather limits which system can access an i5/OS storage path.

There are two types of CHAP authentication.

One-way CHAP
The target (System i) authenticates the initiator (System x or blade).

Bidirectional CHAP
In addition to the one-way CHAP authentication described above, the initiator (System x or blade) also authenticates the target (System i). Bidirectional CHAP is supported in environments that use i5/OS V6R1 or later.

If you do not want to use CHAP, select **Disabled** for "i5/OS remote system configuration object work sheet" on page 84 items **RS7** and **RS10**. Continue with "Selecting maximum transmission unit (MTU) setting for the iSCSI network" on page 72.

Selecting parameters for target CHAP authentication for iSCSI-attached integrated servers:

Do the following steps to select parameters for target CHAP authentication.
1. Put a check next to **Enabled** in "i5/OS remote system configuration object work sheet" on page 84 item **RS7**.
2. Record the CHAP name in "i5/OS remote system configuration object work sheet" on page 84 item **RS8**. You can use the remote system configuration object name from item **RS1** as the CHAP name.
3. Record the CHAP secret.

   There are two approaches to assigning a CHAP secret. The strength of the CHAP secret that you should use depends on your environment.
   - If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in "i5/OS remote system configuration object work sheet" on page 84 item **RS9**.
   - If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in "i5/OS remote system configuration object work sheet" on page 84 item **RS9** and leave the CHAP secret value blank for now.

Selecting parameters for initiator CHAP authentication for iSCSI-attached integrated servers:

Use this information to select settings for initiator CHAP authentication.

If you do not want to configure initiator CHAP, select **Disabled** for "i5/OS remote system configuration object work sheet" on page 84 configuration item **RS10**. Continue with "Selecting maximum transmission unit (MTU) setting for the iSCSI network."

If you want to configure initiator CHAP, do the following steps to select parameters.

1. Put a check next to **Enabled** in "i5/OS remote system configuration object work sheet" on page 84 item **RS10**.

2. Record the CHAP name in "i5/OS remote system configuration object work sheet" on page 84 item **RS11**. You can use the remote system configuration object name from item **RS1** as the CHAP name.

3. Record the CHAP secret.

   There are two approaches to assigning a CHAP secret. The strength of the CHAP secret that you should use depends on your environment.

   - If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in "i5/OS remote system configuration object work sheet" on page 84 item **RS12**.

   - If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in "i5/OS remote system configuration object work sheet" on page 84 item **RS12** and leave the CHAP secret value blank for now.

Selecting maximum transmission unit (MTU) setting for the iSCSI network:

The iSCSI network MTU value can be set to 1500 (normal frames) or 9000 (jumbo frames).

The iSCSI network normally uses standard 1500 byte frames. It is possible to configure iSCSI HBAs to use larger frames on the iSCSI network. However, under heavy traffic, many switches do not perform well with larger frames, degrading performance of both storage and virtual Ethernet. If you are not sure that your switch performs well with larger frames, it is recommended that you use the default settings for 1500 byte frames. As long as switch limitations are not affecting performance, setting the iSCSI HBA and switch MTU configuration to 9000 typically improves performance, especially virtual Ethernet performance. If you plan to use jumbo frame support, you need to configure it on the switch, if not already enabled.

Do the following steps to record the MTU settings that you will use.

1. Put a check in the box next to your Port 1 MTU choice in worksheet item **CQ16**.

2. If your server has a second port (for example, a blade with a dual port iSCSI HBA), then also put a check in the box next to your Port 2 MTU choice in worksheet item **CQ16**.

Recording iSCSI initiator (local adapter) MAC addresses:

Do these steps to record the iSCSI initiator local adapter (MAC) address for your remote system configuration object. Depending on your iSCSI HBA type, do one of the following:

Depending on the iSCSI initiator adapter type, look in the following locations for the adapter address.

- For a System x model, the iSCSI initiator is either an iSCSI HBA or an Ethernet Network Interface Card (NIC). Note the label that is attached to the tail stock (or on the system unit for an embedded Ethernet NIC) with sets of 12–digit hexadecimal values. These are unique addresses that are assigned for the adapter.

   Important: The System x iSCSI HBA parts 30R5201 and 30R5501 look identical to the System i iSCSI HBA features 5783 and 5784, but they have different firmware, so they are not

interchangeable. If you get them mixed up and use an iSCSI HBA in the wrong system, it does not work. If you are not sure which system type a particular iSCSI HBA is for, look for the CCIN values on the tail stock of the iSCSI HBA card. See iSCSI host bus adapter

(iSCSI HBA) for a list of iSCSI HBAs and the associated CCIN values.

- For a blade model, the iSCSI initiator adapter is either an iSCSI HBA I/O expansion module on the blade or an Ethernet NIC on the blade. There are labels on the box of the adapter and on the adapter itself. The label has sets of 12–digit hexadecimal values. These are unique addresses that are assigned for the adapter. For iSCSI HBAs with two ports, the label shows four addresses. Each port has an iSCSI address and a TOE address. For Ethernet NICs with two ports, the label shows two addresses.

For more information about these addresses, see iSCSI Network.

Note: Record the MAC addresses. Later on, you use the iSCSI initiator configuration function to configure the adapters and you can verify the values. The management Module Web interface can show the addresses (use the Hardware VPD link and look under the BladeCenter Server MAC addresses).

For an iSCSI HBA, perform the following steps to record the iSCSI initiator local adapter (MAC) address.

1. Look for the word 'iSCSI' on the label. Record the address information in pairs of digits in work sheet item **RS13**. A portion of the address is filled in for you, one example is for a System x adapter and the other is for a blade adapter. Choose the example that matches the first 3 sets of characters. The iSCSI connection is used for disk traffic.
2. Look for the word 'TOE' on the label. Record the address information in pairs of digits in work sheet item **RS17**. A portion of the address is filled in for you, one example is for a System x adapter and the other is for a blade adapter. Choose the example that matches the first 3 sets of characters. TOE stands for TCP Offload Engine. Think of it as an I/O processor for the adapter. The TOE is used for virtual Ethernet LAN traffic.

For an Ethernet NIC that is used as an iSCSI initiator, look for the word MAC on the label. Record the address information in pairs of digits in work sheet items RS13 and RS17. Note that the same adapter address is used for both the SCSI and LAN interfaces.

Selecting IP addresses for the System x or blade iSCSI initiator:

You need to select an IP address scheme for SCSI and LAN interfaces of the iSCSI initiator before you configure your server. You can use the sample information in this table or use your own scheme.

You can use the convention in this example for up to 19 hosted systems connected to the same switch. The shaded portions signify addressing for additional adapters in the same server. If you want to plan for more than 19 hosted systems on the same switch, see "Expanding on the iSCSI network addressing scheme for integrated servers" on page 79.

Notes:

1. The last digits of the Internet address is a concatenation of a system number and a port number (for example, system 1, port 1 = 11. Add 4 to this for the LAN addresses). If you use this convention, you can assign any numbers to systems, ports, and iSCSI initiators within the indicated ranges.

2. This table gives sample IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your Hardware Management Console (HMC), it should not be on the same subnet as the iSCSI or virtual Ethernet networks.

Table 7. Sample address scheme for the iSCSI network

	Configuration parameter	iSCSI port 1	iSCSI port 2	iSCSI port 3	iSCSI port 4
Hosted system 1	SCSI interface				
	Internet address	192.168.99.**11**	192.168.99.**12**	192.168.99.**13**	192.168.99.**14**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**15**	192.168.99.**16**	192.168.99.**17**	192.168.99.**18**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
Hosted system 2	SCSI interface				
	Internet address	192.168.99.**21**	192.168.99.**22**	192.168.99.**23**	192.168.99.**24**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**25**	192.168.99.**26**	192.168.99.**27**	192.168.99.**28**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
...	...	...	...	...	...
Hosted system 19	SCSI interface				
	Internet address	192.168.99.**191**	192.168.99.**192**	192.168.99.**193**	192.168.99.**194**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**195**	192.168.99.**196**	192.168.99.**197**	192.168.99.**198**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank

Note: You can leave the gateway address blank because these System x and blade iSCSI initiators are on the same switch and subnet as the System i iSCSI targets. Routers are not supported in the iSCSI network.

Do these steps to record IP addresses.

1. Fill in the **SCSI interface internet address and subnet mask** from the table above (or use your own value) in work sheet items **RS14** and **RS15**.
2. Fill in the **LAN interface internet address** and subnet mask from the table above (or use your own value) in work sheet items **RS18** and **RS19**.

Selecting the initiator iSCSI Qualified Name (IQN):

If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item RS6, then you need to configure the initiator (System x or blade) iSCSI Name (IQN) value manually.

The initiator iSCSI Name (IQN) format is:

iqn.1924-02.com.ibm:*sssssss*.i*p*

where

- *sssssss* is the serial number of the System x (see item SP5) or blade (see item RS4) server in lower case characters
- *p* is the System x/blade iSCSI HBA interface/port number (0=first interface/port).

Record the initiator IQN values in worksheet item **CQ6.**

Selecting the target iSCSI Qualified Name (IQN):

If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item **RS6**, then you need to configure the target (System i) iSCSI Name (IQN) value manually.

The target iSCSI Name (IQN) format is

iqn.1924-02.com.ibm:*sssssssi.nnnnnnnnn*.t*p*

where

- *sssssss* is the System i serial number in lower case letters.

  Note: You can display the System i serial number by entering DSPSYSVAL QSRLNBR at the i5/OS command line.
- *i* is the System i logical partition ID.
- *nnnnnnnn* is the network server description (NWSD) name in lower case.
- *p* is the storage path number from the NWSD (1=first and only storage path for new installations).

Record the target IQN value in worksheet item **CQ10**.

Planning for the network server host adapter (NWSH) object:

The network server host adapter (NWSH) device description defines the communications connections for iSCSI and virtual Ethernet traffic to i5/OS.

An NWSH object represents a port for an iSCSI host bus adapter (HBA) that is installed inside the System i product or its associated expansion units.
- If you have already created a NWSH device description for the port for the target iSCSI HBA installed in the System i product, use the existing object.
  1. Record the existing NWSH object name in worksheet item **NH1**.
  2. Put a check in the box labeled **Existing** in worksheet item **NH1**.
  3. Look up the local SCSI interface internet address in the NWSH and record it in worksheet item **NH5**. See Displaying network server host adapter properties.
  4. Go to "Planning for the i5/OS connection security configuration object" on page 78.
- If you need to create a new i5/OS remote system configuration object:
  1. Put a check in the box labeled **New** in worksheet item **NH1**.
  2. Continue with the following tasks.

Selecting a name for the NWSH:

You need to assign a name to the i5/OS network server host adapter (NWSH) device description object that you will create to configure the System i iSCSI HBA.

The NWSH name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention for the NWSH name.

An example naming convention that associates the NWSH with the iSCSI HBA hardware is:

NH*sssssss*

where *sssssss* is the last 7 characters of the System i iSCSI HBA serial number.
1. Fill in the name you choose in worksheet item **NH1**.
2. Also fill in a description of the object (up to 50 characters) in item **NH2**.

Selecting a hardware resource name:

The iSCSI HBA hardware resource name will not be available until the iSCSI HBA is actually installed in the System i platform.

Leave worksheet item **NH3** blank. You will fill in this value after you install the target iSCSI HBA in the System i product.

Selecting a connection type for the NWSH:

There are two ways that iSCSI HBAs in a System i product can physically connect to a System x or a blade system.
- If this Network server host adapter (NWSH) object will be connected to an Ethernet switch, put a check in the box by **Network** in "i5/OS network server host adapter object work sheet" on page 88 item **NH9**.
- If this Network server host adapter (NWSH) object will be connected directly to an iSCSI HBA port in a System x product or to a pass through module in a blade system, put a check in the box next to **Direct** in "i5/OS network server host adapter object work sheet" on page 88 item **NH9**.

Selecting IP addresses for the System i iSCSI HBA:

Use this information to select IP addresses for the target iSCSI HBA installed in the System i product.

The information from the table below can be used to configure SCSI and LAN interfaces for your System i iSCSI HBA(s). You can use the convention in this example for up to 19 System i HBAs connected to the same switch. If you want to plan for more than 19 System i HBAs on the same switch, see section 4.1 Expanding on the iSCSI network addressing scheme, for additional considerations. The shaded columns designate having more than one iSCSI HBA in the System i platform.
- For System i i iSCSI HBAs, the last digit is 200 + an iSCSI HBA number (+ 20 more for LAN). If you use this convention, you can assign numbers to systems, ports and iSCSI HBAs within the indicated ranges any way you want.
- This table gives suggested IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your HMC, it should not be on the same subnet as the iSCSI or virtual Ethernet networks.

Table 8. Suggested IP addresses for the physical iSCSI network

	Configuration parameter	iSCSI HBA 1	iSCSI HBA 2	iSCSI HBA 3	...	iSCSI HBA 19
System i	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	...	255.255.255.0
	SCSI interface					

Table 8. Suggested IP addresses for the physical iSCSI network (continued)

	Configuration parameter	iSCSI HBA 1	iSCSI HBA 2	iSCSI HBA 3	...	iSCSI HBA 19
	Internet address	192.168.99.**201**	192.168.99.**202**	192.168.99.**203**	...	192.168.99.**219**
	Gateway address[1]	blank[1]	blank[1]	blank[1]	...	blank[1]
	LAN interface					
	Internet address	192.168.99.**221**	192.168.99.**222**	192.168.99.**223**	...	192.168.99.**239**
	Gateway address[1]	blank[1]	blank[1]	blank[1]	...	blank[1]

Note:

1. You can leave the gateway address blank because these System x and blade iSCSI HBAs will be on the same switch and subnet as the System i HBAs. Routers are not supported in the iSCSI network.

1. Fill in the **Subnet mask** in worksheet item **NH4**.
2. Fill in the **SCSI interface internet address** and **gateway** in worksheet items **NH5** and **NH6**.
3. Fill in the **LAN interface internet address** and **gateway** in worksheet items **NH7** and **NH8**.

Planning for the i5/OS connection security configuration object:

A connection security configuration object is required for iSCSI-attached integrated servers. All of the iSCSI-attached integrated servers on your system can share the same connection security configuration object.

You should not change any settings for this object.

1. If you have an existing connection security configuration object:
   a. Reuse the existing connection security configuration object.
   b. Record the existing connection security configuration object name in work sheet item **CS1**.
   c. Put a check in the box labeled **Existing** in work sheet item **CS1**.
   d. Skip the remainder of this section.
2. If you need to create a new i5/OS connection security configuration object:
   a. Put a check in the box labeled **New** in worksheet item **CS1**.
   b. Continue with the following task.

Assigning a connection security configuration object name:

Select a name for the i5/OS connection security configuration object.

The connection security configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

Use the same connection security object for all iSCSI attached servers that are connected to your i5/OS partition. It is recommended to use a fixed name such as NOIPSEC for the connection security configuration object.

Do the following steps to record the name.
1. Fill in the name you choose in worksheet item **CS1**.
2. Also fill in a description of the object (up to 50 characters) in item **CS2**.

Advanced planning topics

Consider the following items when planning for an iSCSI network.

Expanding on the iSCSI network addressing scheme for integrated servers:

Consider these things if you are planning for an iSCSI network that might support multiple switches or more than 19 iSCSI HBA ports.

- If you use a second switch and do not connect it directly to a switch in the 192.168.99 network, you can repeat the IP addressing convention shown in the tables in "Selecting IP addresses for the System x or blade iSCSI initiator" on page 74 and "Expanding on the iSCSI network addressing scheme for integrated servers." Use IP addresses that start with 192.168.98 instead of 192.168.99. This is a separate IP subnet.
- With a subnet mask of 255.255.255.0 there are 254 IP addresses available. IP addresses with a last digit of 0 or 255 should not be used with this subnet mask.
- If you anticipate eventually having an iSCSI network with more than 19 System i iSCSI HBAs or more than 19 hosted systems, you may modify the IP address convention in the tables to maximize the use of all 254 available IP addresses.
- If you anticipate eventually needing more than 254 IP addresses, consider using a different subnet mask to begin with, to avoid the need to change this later.
  - For 510 IP addresses, use a subnet mask of 255.255.254.0
  - For 1022 IP addresses, use a subnet mask of 255.255.252.0
  - For 65534 IP addresses, use a subnet mask of 255.255.0.0
  - For the above subnet masks, you must use IP addresses that start with a number less than 192.
- In IP networking, different subnets may be interconnected using routers. IBM does not currently support routers in the iSCSI network. However, if you want to design your iSCSI network to maximize hot spare potential involving the future possibility of routers in the iSCSI network, you should modify the IP address convention in the tables slightly. Routers typically do not forward packets sent to IP addresses that are reserved for private networks. This includes all IP addresses that start with the following digits:
  - 10
  - 172.16 through 172.31
  - 192.168

Therefore, consider using IP addresses that start with different digits, such as 192.169.

Considerations for connecting service processors to i5/OS:

Use this information to compare configurations between i5/OS and the service processor for the integrated server.

You might want to consider using an isolated network, instead of your company's campus LAN or intranet, for connecting your BladeCenter and System x service processors with your i5/OS logical partition. This decision involves considerations of hardware, remote management, security, and multiple management server (Service Processor Manager or IBM Director Server). The following table summarizes different connection methods. Different service processors are shown to illustrate scalability.

Table 9. Connection methods

	Campus LAN or Intranet		Physically isolated network	
Network Hardware Configuration	Any-to-any network	Logically isolated network For example, this network might include VLAN switches configured with a unique VLAN ID.	One switch for both iSCSI HBAs and service processor connections	Separate switches for iSCSI HBAs and service processors
Flexibility of remote management by using a Web Browser[3]	Better ←			→ Worse
	Browser can be anywhere on the campus LAN.	Browser must be connected to the logically isolated LAN.	Browser must be connected to the switch providing the service processor connection.	Browser must be connected to the switch providing the service processor connection.
Security[4]	Worse ←			→ Better
	Highest risk.	Lower risk than any-to-any network.	Low risk. Requires access to the switch providing the service processor connection.	Low risk. Requires access to the switch providing the service processor connection.
Multiple Management Server Coexistence[5] (Shared SP Login ID)	Worse ←			→ Better
	Any management server connected to the campus LAN might interfere.	Only management servers connected to the logically isolated LAN might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.
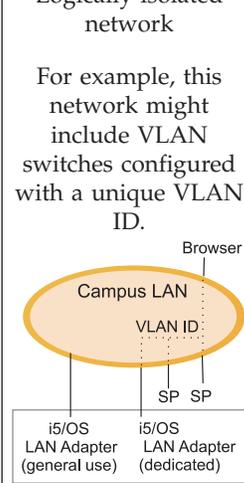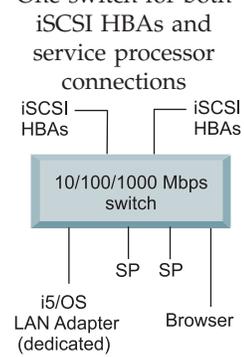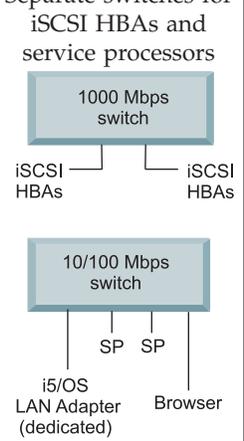
Note:

1. *Browser* is a Web browser used for remote management.
2. *SP* is a System x RSA II or BladeCenter Management Module service processor.

3. The web browser management interface is supported by the BladeCenter Management Module and System x RSA II. It is not available for a System x model that only has a BMC service processor.

4. For example, consider the possibility of a LAN sniffer attack seeking a service processor password.

5. If your company has multiple management servers (Service Processor Managers or IBM Director Servers), pay attention to the following situations:

   • If you change the default login ID of the service processor as mentioned in "Selecting a Login ID and Password for the Service Processor" on page 67, then no other management servers interfere and this item does not apply to you.

   • If you do not change the default login ID of the service processor as mentioned in "Selecting a Login ID and Password for the Service Processor" on page 67, this item shows which management servers might interfere with the ability of i5/OS to access a service processor (especially a Management Module).

6. The Multiple Management Server Coexistence[5] (Shared SP Login ID) row applies to you only if you do not change the default service processor login ID.

iSCSI network planning work sheets

Use these work sheets to record the parameters you will use to install the integrated server.

i5/OS service processor configuration object work sheet:

Use this work sheet to record the values for the i5/OS service processor configuration object.

This information is used to configure how the i5/OS operating system communicates with the BladeCenter or System x service processor. They are not used for the System i service processor.

Table 10. i5/OS service processor configuration object values

Item	Item Description	Value	
	General:		
SP1	Name[1,2,3]		☐ New ☐ Existing
SP2	Description[4]		
	Service processor connection[5]		
SP3	☐ Hostname	Refer to item **XSP2** value	
SP4	☐ Internet address	Refer to item **XSP4** value	
	Enclosure identity:[6,7]		
SP5	Serial number [6,7]		
SP6	Manufacturer type and model [6,7]		

Notes:

1. For example, use the naming convention: SP*sssssss* where *sssssss* is the last 7 characters of the BladeCenter chassis (not blade) or System x serial number.
2. For an existing service processor configuration, do not fill out the remaining values in this worksheet.
3. On the CRTNWSCFG command, this is called "Network server configuration".
4. On the CRTNWSCFG command, this is called "Text 'description'".
5. On the CRTNWSCFG command, specify *YES for the enable unicast (ENBUNICAST) parameter.
6. Use the BladeCenter chassis (not blade) or System x serial number and type/model values.
7. Items **SP5** and **SP6** must be blank for a System x model if it only has a BMC service processor (no RSA II).
8. On the CRTNWSCFG command, specify *NONE for the initialize service processor (INZSP) parameter.

BladeCenter or System x service processor work sheet:

Use this work sheet to plan the values for the BladeCenter or System x service processor.

Table 11. Parameters for the System x or BladeCenter service processor.

Item	Item Description	Value	
	General:		
XSP1	Service processor type [1]	☐ MM (BladeCenter Management Module) ☐ AMM (Advanced Management Module) ☐ RSA II with BMC (System x model) ☐ BMC (System x model without an RSA II)	
XSP2	Host name[2]		
XSP3	DHCP	☐ Enabled	☐ Disabled
XSP4	IP address	N/A	
XSP5	Subnet mask	N/A	
XSP6	Gateway address	N/A	
	Login for **i5/OS** to connect to the service processor.		
XSP7	Login ID[3,4]		
XSP8	Password		
	Login for **administrators** to use to connect to the service processor (optional):		
XSP9	Login ID[3]		
XSP10	Password		

Notes:

1. Put a check in the box next to the type of service processor being used.
2. For an RSA II, MM or AMM, the hostname is optional if DHCP is disabled. The hostname is not supported for a System x model that has only a BMC service processor (no RSA II).
3. The login ID is called "User name" for a BMC or when using the web browser interface for an RSA II, MM or AMM.
4. Suggested naming convention for this login ID is to use the i5/OS logical partition name or system name.

i5/OS remote system configuration object work sheet:

Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Table 12. i5/OS remote system configuration object parameters

Item	Item Description	Value	
	General:		
RS1	Name[1,2,3]		☐ New ☐ Existing
RS2	Description [4]		
RS3	Service processor configuration	XXXXXX (Refer to item **SP1** value)	
	Remote system identity:[5]		
RS4	Serial number[5]		
RS5	Manufacturer type and model [5]		
	Boot Parameters:		
RS6	Boot parameter delivery method	☐ Dynamically delivered to remote system via DHCP[6] ☐ Manually configured on remote system	
	CHAP Authentication		
RS7	Target CHAP	☐ Enabled ☐ Disabled[11]	
RS8	CHAP name[7]		
RS9	CHAP secret		☐ Generate
RS10	Initiator CHAP	☐ Enabled ☐ Disabled[12]	
RS11	CHAP name[7]		
RS12	CHAP secret[8]		☐ Generate
	Remote Interfaces:	**Interface (Port) 1**	**Interface (Port) 2**
	Remote SCSI Interface:		
RS13	Adapter address[9]	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __
RS14	Internet address		
RS15	Subnet mask		
RS16	Gateway address	(Leave blank)	(Leave blank)
	Remote LAN interface:		
RS17	Adapter address[10]	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __
RS18	Internet address		
RS19	Subnet mask		
RS20	Gateway address	(Leave blank)	(Leave blank)

Notes:

1. For example, you can use the naming convention RS*sssssss* where *sssssss* is the last 7 characters of the blade (not chassis) or System x serial number.

2. For an existing remote system configuration, do not fill out the remaining values in this work sheet.

3. On the Create Network Server Configuration (CRTNWSCFG) command, this is called "Network server configuration".

4. On the Create Network Server Configuration (CRTNWSCFG) command, this is called "Text 'description'".

5. This information is only required for blades. Use the blade (not chassis) serial number and type/model values.

6. Uses an integrated DHCP server. It does not require a general purpose DHCP server in your network.

7. You can use the remote system configuration name from work sheet item **RS1** as the CHAP name.

8. The CHAP secrets for target and initiator CHAP must not match.

9. For an iSCSI HBA, get this value from the System x or blade iSCSI label. For an Ethernet Network Interface Card (NIC), get it from the Ethernet NIC label.

10. For an iSCSI HBA, get this value from the System x or blade TOE label. For an Ethernet NIC, get it from the Ethernet NIC label.

11. On the Create Network Server Configuration (CRTNWSCFG) command, specify *NONE in the target CHAP name (CHAPAUT) to disable target CHAP.

12. On the Create Network Server Configuration (CRTNWSCFG) command, specify *NONE in the initiator CHAP name (INRCHAPAUT) to disable bidirectional CHAP.

iSCSI initiator work sheet:

Select the parameters to configure the iSCSI initiator in the System x or blade hardware.

The values that should be filled into this work sheet are indicated by the Dynamic and Manual columns: R=Required, O=Optional and N/A=Not applicable.

Table 13. Parameters for the iSCSI initiator configuration function

Item	Item Description	Addressing mode[1]		Value
		☐ Dynamic	☐ Manual	
	Adapter settings:			
CQ1	LUNs per Target	O	O	**64**
CQ2	Initiator IP address by DHCP	R	R	**NO**[2]
CQ3	Initiator IP address	N/A	R	XX (Refer to item **RS14** values) XX
CQ4	Subnet mask	N/A	R	XX (Refer to item **RS15** values) XX
CQ5	Gateway IP address	N/A	R	Leave this field empty
CQ6	Initiator iSCSI Name[3]	N/A	R	**Port 1:** iqn.1924-02.com.ibm:_____.i0 **Port 2** iqn.1924-02.com.ibm:_____.i0
CQ7	Initiator Chap Name	O	O	Leave this field empty
CQ8	Initiator Chap Secret	O	O	Leave this field empty
	iSCSI Boot Settings:			
CQ9	Adapter Boot Mode[1]	R	R	**Port 1:**☐ DHCP ☐Manual **All other ports: Disabled.**[4]
CQ10	Target IP	N/A	R	XX (Refer to item **NH5** value) XX
CQ11	Target iSCSI Name[6]	N/A	R	iqn.1924-02.com .ibm:_____._____.t1
CQ12	Chap	R	R	☐ Enabled ☐ Disabled
CQ13	Chap Name	O	O	XX (Refer to item **RS8** value) XX
CQ14	Chap Secret	O	O	XX (Refer to item **RS9** value) XX
CQ15	Bidirectional CHAP	O	O	XX (Refer to item **RS10** value) XX
	Advanced Adapter Settings:			
CQ16	MTU	O	O	**Port 1:** ☐1500 ☐ 9000 **Port 2:** ☐1500 ☐9000

Notes:

1. The value for item **RS6** determines the Addressing Mode and the value for item **CQ9**. See "Selecting a boot parameter delivery method" on page 70.
2. The Initiator IP address by DHCP value must always be set to NO.
3. The initiator iSCSI Name (IQN) format is: iqn.1924-02.com.ibm:*sssssss*.i*p* where:
   - *sssssss* is the serial number of the System x (see item SP5) or blade (see item RS4) server in lower case
   - *p* is the System x/blade iSCSI HBA interface/port number (0=first interface/port).

4. Only one port can have the boot mode set to DHCP or Manual during the server installation. For all other ports, the adapter boot mode must be set to **Disabled**. Once the server installation is completed, if the server operating system supports multipath I/O, then additional ports can be enabled for boot.

5. The target iSCSI Name (IQN) format is: iqn.1924-02.com.ibm:*sssssssi.nnnnnnnn.tp* where:

    - *sssssss* is the System i serial number in lower case.

    - *i* is the System i logical partition ID.

    - *nnnnnnnn* is the network server description (NWSD) name in lower case letters.

    - *p* is the storage path number from the NWSD (1=first and only storage path for new installations).

i5/OS network server host adapter object work sheet:

Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Table 14. Parameters for the NWSH object

Item	Item Description	Value	
	General:		
NH1	Name[1,2,3]	☐ New ☐ Existing	
NH2	Description[4]		
NH3	Hardware resource name	CMN___	
	Local Interfaces:		
NH4	Subnet mask		
	Local SCSI Interface		
NH5	Internet address		
NH6	Gateway address		
	Local LAN Interface		
NH7	Internet address		
NH8	Gateway address		
NH9	Cable connection	☐ Network ☐ Direct	

Notes:

1. For example, a naming convention might be NH*sssssss* where *sssssss* is the last 7 characters of the serial number for the target iSCSI HBA that is installed in the System i product.
2. For an existing NWSH, also fill in item NH5 by looking at the NWSH properties, but do not fill in the remaining values in this worksheet.
3. On the CRTDEVNWSH command, this is called "Device description".
4. On the CRTDEVNWSH command, this is called "Text 'description'".

i5/OS connection security configuration object work sheet:

Use this work sheet to record the parameters for the network security configuration object.

Table 15. Values for the i5/OS connection security configuration object

Item	Item Description	Value	
	General:		
CS1	Name[1,2,3]		☐ New ☐ Existing
CS2	Description[4]		

Notes:

1. Since IP security (IPSec) is not supported, the suggested name is: **NOIPSEC**.
2. For an existing connection security configuration, do not fill out the remaining values in this worksheet.
3. On the Create Network Server Configuration (CRTNWSCFG) command, this is called `Network server configuration`.
4. On the Create Network Server Configuration (CRTNWSCFG), this is called `Text 'description'`.

Planning for the integrated server operating system

Plan the configuration for the integrated server operating system.

Installation command planning

Use this information to help you select parameters for the Install Windows Server (INSWNTSVR) or Install Linux Server (INSLNXSVR) commands for installing the operating system for an integrated server.

Considerations for all types of integrated servers

- Specify to use an existing service processor configuration. Use the name from item **SP1** in the "i5/OS service processor configuration object work sheet" on page 82.
- Specify *NONE for the service processor security initialization method, since the service processor configuration was already synchronized in an earlier step.
- Specify to use an existing remote system configuration. Use the name from item **RS1** in the "i5/OS remote system configuration object work sheet" on page 84.
- Specify to use an existing connection security configuration. Use the name from item **CS1** in the "i5/OS connection security configuration object work sheet."
- For both the storage path and the point to point virtual Ethernet LAN, use the network server host adapter name from item **NH1** in the "i5/OS network server host adapter object work sheet" on page 88.

Considerations for installing the Microsoft Windows operating system

- Specify the full (*FULL) install type.
- If you are installing Windows Server 2003, the source directory is the location of the System i optical device or IFS directory that corresponds to the Windows install media that you obtained in the Obtain server operating system install media step of the "iSCSI-attached integrated server installation road map" on page 52.

Selecting a language for the integrated server operating system installation

You can select the language that Integrated Server Support will use with your integrated server.

For most environments, the integrated server should use the same language as i5/OS. For information about supported language versions, see Install Windows Server (INSWNTSVR) for integrated Windows servers or Install Linux Server (INSLNXSVR) for integrated Linux or VMware servers.

Prerequisites for installing an iSCSI-attached integrated server

You need to have software, hardware, and documentation before your begin installing an integrated server.

Documentation prerequisites for installing an iSCSI-attached integrated server

You should have these documents available when you install the integrated server.

- iSCSI install read me first web page [graphic] (www.ibm.com/systems/i/bladecenter/iscsi/readme/) Web page
- System i integration with BladeCenter and System x topic collection.

  See System i integration with BladeCenter and System x: iSCSI-attached System x and blade Systems

  [graphic] to print a PDF version of this information.
- iSCSI Network Planning Guide

  See "iSCSI Network Planning Guide" on page 62 or System i integration with BladeCenter and System

  x: iSCSI network planning guide [graphic] to print a PDF version of this information.
- PCI adapters topic collection in the IBM Systems Hardware Information Center

  This topic collection contains information about installing the iSCSI HBA in the System i product.
- The Installing IBM Director Server on i5/OS topic collection in the IBM Systems Software Information Center, if you are using IBM Director for integrated server discovery and power control.
- BladeCenter or System x hardware setup documents. These documents are normally included in hard copy form with your BladeCenter or System x model. The actual document titles and contents will depend on your BladeCenter or System x hardware.

Reviewing integrated server concepts

You should be familiar with "Concepts for iSCSI-attached integrated servers" on page 5 before starting the installation.

Downloading firmware updates

Use these tasks to download and save updates for the integrated server hardware. You will need to update both the iSCSI HBA firmware and the System x or blade firmware.

Downloading firmware updates for System x hardware

Download the firmware updates for the System x product before you begin installing your integrated server.

You should have access to a web browser.

The BIOS firmware updates may be available in a number of formats, employing different bootable media:

- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Download the system BIOS update by following these steps:

1. Go to the BladeCenter and System x models supported with iSCSI (www.ibm.com/systems/i/systemx/iscsi/servermodels/) Web page.
2. Locate the System x and type and model in the table.
3. Click the **download firmware**link. The *Software and device drivers* page for the selected server is displayed.
4. Find the **BIOS** heading and column for the appropriate hardware, if necessary and select the link for **Flash BIOS Update (DOS Version)** or **Flash BIOS Update (Diskette image)**. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
5. Click the link for the README text file and print a copy for use as a reference when actually performing the update.
6. Click the browser's Back button to return to the previous page.
7. Click the link to download one of the update versions on the page for the BIOS update.
8. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
9. Click on the browser's Back button to return to the *Software and drivers* page.

Downloading BIOS updates for System x hardware:

Download updates for the System x system BIOS and the iSCSI host bus adapter (HBA) before you begin installing the integrated server.

The following procedure is performed on a computer using a common web browser, while accessing the following web page http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the System x system type and model in the models supported with iSCSI table. Click on the **download firmware** link. The *Software and device drivers* page for the selected server is displayed.

The BIOS firmware updates may be available in a number of formats, employing different bootable media:
- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Download the system BIOS update by following these steps:
1. Find the **BIOS** heading and column for the appropriate hardware, if necessary and select the link for **Flash BIOS Update (DOS Version)** or **Flash BIOS Update (Diskette image)**. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. Click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Click on the link to download one of the update versions on the page for the BIOS update.
5. Create the update media by performing the appropriate action for the file type from the following methods:

- .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
- .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
- .iso file: Use a CD burning utility to create a bootable update CD.
6. Click on the browser's Back button to return to the *Software and drivers* page.

Downloading updates for Baseboard Management Controller (BMC) service processors:

Do these steps download updates for the Baseboard Management Controller service processor before you begin installing the integrated server.

The following procedure is performed on a computer using a common Web browser. Access the IBM i integration with BladeCenter and System x Web page. Start by locating the System x server type and model in the System x models supported with iSCSI table. Click the **download firmware** link. The *Support* page for the selected server is then displayed.

The Baseboard Management Controller needs to be updated in all System x servers, including those with remote supervisor adapter II (RSAII) installed. Use the following procedures to accomplish this task.

The Baseboard Management Controller firmware updates may be available in a number of formats, employing different bootable media:
- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.
1. Find the **BMC** heading. If there is no **BMC** heading, look for the **Advanced Systems Management** heading. Select the link for **Baseboard Management Controller Update** from the appropriate hardware column.

   Note: Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. Click on the link for the README text file on the next page, and print a copy for use as a reference when actually performing the update.
3. Click Back, on the browser, to return to the previous page.
4. Click on the link to download one of the update versions on the page for the Baseboard Management Controller update. There may be multiple links for a single update version.
5. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
6. Click Back, on the browser, to return to the *Software and drivers* page.

Downloading updates for RSA II service processors:

Download updates for an RSA II service processor before you begin installing the integrated server.

The RSA II firmware update will reside in a .zip file.

The following procedure is performed on a computer using a common web browser, while accessing the following web page http://www.ibm.com/systems/i/systemx/iscsi/servermodels/. Start by locating the System x server type and model in the System x models supported with iSCSI table. Click on the **download firmware** link. The *Software and device drivers* page for the selected server will then be displayed.

Download the RSA II firmware update by following these steps:

1. Find the **Remote Supervisor Adapter II** heading. Select the link that is not associated with an operating system. You will complete the update before an operating system is installed on your server.

   Note: If a DOS update is listed select that link.

2. On the **firmware update** page, click on the link for the readme text file and print a copy for use as a reference when actually performing the update.

3. Click Back on your browser to return to the **firmware update** page.

4. Click on the link for the .zip file containing the firmware updates to download the file. You will use this file to update the RSA II firmware.

Downloading updates for the blade server and the BladeCenter chassis

Do these tasks to download and save updates.

The following procedure is performed on a computer using a common web browser, while accessing the

BladeCenter and System x models supported with iSCSI (www.ibm.com/systems/i/bladecenter/iscsi/servermodels/) Web page. Start by locating the blade server type or model in the BladeCenter blade models supported with iSCSI table. Click on the **download firmware** link. The Software and device drivers page for the selected blade server will then be displayed.

The BIOS and Baseboard Management Controller firmware updates may be available in a number of formats, employing different bootable media.

- .exe file(s): create a bootable update diskette.
- .img file(s): create a bootable update diskette.
- .iso file: create a bootable update CD.

Other firmware will have a single file type.

Downloading the blade system BIOS:

Learn how to locate, select, and download the BIOS updates for your blade server using the procedure in this section.

1. On the next page, find the **BIOS** heading and column for the appropriate hardware, if necessary and select the link for **Flash BIOS Update (DOS Version)** or **Flash BIOS Update (Diskette image)**. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.

2. On the next page, click on the link for the README text file and print a copy for use as a reference when actually performing the update.

3. Click on the browser's Back button to return to the previous page.

4. Again, on the page for the BIOS update, click on the link to download one of the update versions.

5. Perform the appropriate action to create the update media

   a. .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.

   b. .img file(s): Use an image-to-disk utility such as EMT4W32 to create the update diskette from the file.

c. .iso file: Use a CD burning utility to create the update CD.
6. Click on the browser's **Back** button to return to the Software and drivers page.

Downloading BMC firware for blade systems:

The BMC should be updated even though the BladeCenter has also has a Management Module. Do these steps to download the update.

1. From the blade server *Sofware and device drivers* page, find the BMC heading. If there is no BMC heading, look for the Advanced Systems Management heading. Select the link for Baseboard Management Controller Update from the appropriate hardware column, if multiple columns are present. Do not select any of the operating system update versions, since this update will be done prior to the operating system installation.
2. On the next page, click on the link for the README text file and print a copy for use as a reference when actually performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Again, on the page for the BMC update, click on the link to download one of the update versions. There may be multiple links for a single update version.
5. Click your browser's back button until you are at the software and device drivers page.
6. Create the update media by performing the appropriate action for the file type from the following methods:
   - .exe file(s): Run these on the computer used to download and follow the directions to create a bootable update diskette.
   - .img file(s): Use an image-to-disk utility such as EMT4W32 to create a bootable update diskette from the file.
   - .iso file: Use a CD burning utility to create a bootable update CD.
7. Click on the browser's Back button to return to the Software and drivers page.

Download the BladeCenter I/O module firmware update:

Do these steps to locate, select, and download BladeCenter I/O module firmware updates.

1. From the BladeCenter software and device drivers page find the **Networking** heading and select the appropriate link for the I/O module installed in the BladeCenter chassis.
2. On the firmware update page, click on the link for the README text file and print a copy for use as a reference when performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Next, click on the link of the firmware update to download the file. This file will be used later to update the firmware.

Downloading updates for BladeCenter I/O modules:

Learn how to locate, select, and download BladeCenter I/O module firmware updates using the procedure in this section.

1. From the BladeCenter software and device drivers page find the **Networking** heading and select the appropriate link for the I/O module installed in the BladeCenter chassis.
2. On the firmware update page, click on the link for the README text file and print a copy for use as a reference when performing the update.
3. Click on the browser's Back button to return to the previous page.
4. Next, click on the link of the firmware update to download the file. This file will be used later to update the firmware.

Downloading firmware updates for initiator iSCSI HBAs

Do these steps to download firmware updates for the HBA that is installed in the integrated server hardware.

Once the iSCSI HBA is installed and the operating system is installed and running on the integrated server, System x server, updates are applied through PTFs to the i5/OS Integrated Server Support option.

Restriction: The following procedure is only for use during the installation of the iSCSI HBA. Unpredictable results might occur if you attempt this procedure on an installed and running iSCSI HBA.

1. Using a computer and Web browser go to BladeCenter and System x models supported with iSCSI ![icon] (www.ibm.com/systems/i/bladecenter/iscsi/servermodels).
2. Click the **Download iSCSI HBA firmware** link.
3. Click the README text file link on the next page, and print a copy for use as a reference when you perform the update.
4. Click **Back** on the browser to return to the previous page.
5. Click on the link to download the iSCSI HBA update. This will be in the form of a .iso file.
6. Create a compact disc (CD) containing the update using a CD burning utility.

Installing the iSCSI target in the server running i5/OS

Install the iSCSI HBA in the server running i5/OS and verify that it is assigned to the correct i5/OS logical partition.

This step corresponds to slide 8 in the BladeCenter ![icon] or System x ![icon] iSCSI Installation Overview animation on the iSCSI install read me first ![icon] (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

If new target iSCSI HBAs need to be installed in the This step corresponds to slide 8 in the product, do the steps in the PCI adapter topic in the IBM Systems Hardware Information Center to install the iSCSI HBAs in your System i model.

If your System i platform is partitioned, make sure that the newly installed iSCSI HBAs are assigned to the i5/OS logical partition that will host the BladeCenter or System x model.

Installing the iSCSI initiator on the integrated server hardware

Use these tasks to install the iSCSI HBA in the integrated server hardware and configure it to communicate with the iSCSI HBA in the System i hardware.

Updating the System x firmware and configuring the System x hardware

Update the BIOS for the System x firmware and verify that the system is correctly configured to communicate on the iSCSI network.

Updating the System x BIOS

Update the System x BIOS and configure it to work in an integrated server environment.

If you have not downloaded the BIOS update or printed the readme file see "Downloading firmware updates for System x hardware" on page 90.

Refer to the file named README you printed during the BIOS update download procedure. Use the README file instructions along with the steps below to perform the update. The README file contains any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

Do these steps for each System x product that you integrate.

1. Plug the System x product ac power cords into a power source. Refer to System x documentation to complete this step.
2. Turn on the System x product and insert the Flash BIOS update media in the appropriate drive. Refer to the server documentation to complete this step.
3. The system will start off of the media and present a window where you select **1 - Update POST/BIOS**.
4. On the next panel select 'Y' to move the current POST/BIOS image to the backup ROM location. The current code is copied to the backup bank immediately.
5. Select N for the next several display prompts until the **Save current flash code to disk prompt** is displayed.
6. Select N for the prompt to **Save current flash code to disk**.
7. Select the appropriate language, if prompted, or select the **Update BIOS** option. The update begins.
8. When the update is complete, remove the update media and turn the System x product power off. Refer to System x documentation to complete this step.

Updating System x Baseboard Management Controller firmware

Update the System x Baseboard Management Controller (BMC) firmware.

Refer to the README file printed earlier during the Baseboard Management Controller firmware download. If you have not already downloaded the README file or the firmware see "Downloading updates for Baseboard Management Controller (BMC) service processors" on page 92. Use the README instructions along with the following steps to perform the update. The README file contains any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur. The Baseboard Management Controller firmware should be updated whether or not an RSA II is installed in the System x product.

This procedure should be performed on the System x product.

1. Turn on the power for the System x product and insert the Baseboard Management Controller firmware update media in the appropriate drive. Refer to the System x product documentation to complete this step.
2. The update will load and start automatically. It can take several minutes to complete.
3. When the update completes, remove the media from the drive and turn off the System x product power. Refer to the System x product documentation to complete this step.

Updating firmware and configuring System x Remote Supervisor Adapter II

Update and configure the Remote Supervisor Adapter II (RSA II) service processor to communicate with the System i hardware.

You can skip this topic if the System x hardware does not have an RSA II installed. Refer to "i5/OS service processor configuration object work sheet" on page 82 item **XSP1** to determine whether or not to continue with this section.

If the System x product requires you to install a Remote Supervisor Adapter II (RSA II) option, install it before updating the firmware. After the RSA II is installed, connect it using an Ethernet cable to the Ethernet port on the computer containing the RSA II firmware update. Refer to the RSA II documentation to complete this action.

Tip: You might need a switch or hub to complete these connections depending on the location of the System xSystem x hardware and the computer containing the update.

If you have not already downloaded the RSA II update see "Downloading updates for RSA II service processors" on page 92.

The procedure below assumes the RSA II is set to its factory default values. If the RSA II IP address is no longer known, it can be set back to the defaults, using the Setup utility, by following the instructions in the section "Alternate method to update Remote Supervisor Adapter II network configuration to defaults" on page 222.

Refer to the README file printed earlier during the RSA II firmware download. Use the README file instructions along with the steps below to perform the firmware update. The README file will contain any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

Note: The following steps are performed on the computer containing the update package (not on the System x console):

Updating RSA II firmware:

Do these steps to upgrade RSA II firmware for integrated server hardware.

Refer to the README file printed earlier during the RSA II firmware download. Use the README file instructions along with the following steps to perform the firmware update. The README file can contain any changes necessary to the following instructions. Follow the directions in the README file wherever differences occur.

Note: The following steps are performed on the computer containing the update package (not on the System xconsole).

1. Configure the IP address and networking information for the RSA II. See "Configuring the RSA II IP address and DHCP settings" on page 99.
2. Extract the files from the .zip file that you downloaded earlier to unpack the firmware update files.
3. Ensure the System x ac power cords are attached to a power source. Refer to System x documentation to complete this step. Wait at least 30 seconds following this step to allow the RSA II hardware to start.
4. Open a Web browser. In the address field, type the IP address of the RSA II to which you want to connect. The Enter Password window opens.
5. Type the user name and password on the Enter Password window. The RSA II has a default user name of USERID and password of PASSW0RD (where 0 is a zero not the letter O).
6. Select a timeout value on the next screen and click continue.
7. If the next window is the **System Status** window, on the navigation pane on the left, under **Tasks**, click **Firmware Update**. If the RSA II firmware does not support the server on which it is installed, a warning window stating that the RSA II does not have firmware that supports the server is displayed. Click **OK** to continue.
8. At the next display, select **Browse** and navigate to the files containing the firmware update. The files will have an extension of .PKT; and there might be multiple files with this extension.
9. Select one of these files, and then click **Open**. The full path of the selected file is displayed in the Browse field.
10. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Remote Supervisor Adapter II. A confirmation window is displayed when the file transfer is complete.
11. Verify that the file shown on the Confirm Firmware Update window is the one you want to update. If not, click **Cancel**.

12. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the Remote Supervisor Adapter II is copied. A confirmation window is displayed when the update completes.

13. Repeat the update procedure for any other .PKT files.

Configuring the RSA II:

Configure the user name, password, and other information that allow the i5/OS operating system to communicate with the integrated server hardware.

Read "Planning for the service processor connection" on page 65 for information required to configure the RSA II.

You need the "iSCSI network planning work sheets" on page 81 to complete this task.

This process picks up from any of the screens after signon on the RSA II web browser interface.

Note: If this is the first time that you are signing into the RSA II service processor, you might need to configure the IP address and DHCP settings. See "Configuring the RSA II IP address and DHCP settings" on page 99.

1. Open a Web browser. In the address field, type the IP address of the RSA II to which you want to connect. The Enter Password window opens.

2. Select **Login Profiles** from under **ASM Control** in the navigation pane on the left side of the screen.

3. From the list of login IDs, find the entry for the default login ID value of **USERID** and click that entry. The Login Profile window is displayed

4. Do the following steps.

   a. Change the **Login ID** (worksheet item **XSP7**) and fill in the **Password** (worksheet item **XSP8**) and **Confirm password** fields based on the information entered in the "BladeCenter or System x service processor work sheet" on page 83.

   b. Ensure the **Authority Level** is set to **Supervisor**.

   c. Click **Save**.

5. On the navigation pane on the left side of the window, select **Network Interfaces** under **ASM Control** to start the configuration.

6. Use the values in the "BladeCenter or System x service processor work sheet" on page 83 to complete the following steps:

   a. Select **Enabled** from the **Interface** list.

   b. From the **DHCP** list select and set one of the following (worksheet item **XSP3**):

      1) **Disabled - Use static IP configuration**.

      2) **Enabled - Obtain IP config from DHCP server**. This option requires an operating DHCP server when you install the operating system.

   c. Enter a name for this RSA II in the **Hostname** (worksheet item **XSP2**) field.

   d. Enter a value for the following fields under the **Static IP Configuration** heading need to be filled in if the **Disabled – Use static IP** configuration value was selected for the **DHCP** field above:

      • **IP address** – type in the IP address (worksheet item **XSP4**).

      • **Subnet mask** – type in the desired subnet mask (worksheet item **XSP5**).

      • **Gateway address** – type in the gateway address (worksheet item **XSP6**).

   e. Click **Save** to complete configuring the network interfaces.

7. Select **System Settings** under **ASM Control** on the navigation pane on the left side of the window.

8. On the next window under the **ASM Information** heading, use the **Host OS** list to select a value of **Other**.

9. On the same window, under the heading **ASM Date and Time**, click **Set ASM Date and Time**.

10. On the next window, set the current date and time (using a 24-hour clock) and use the **GMT offset** list to select the appropriate time zone. Also, select the box to automatically adjust for daylight savings time, if necessary. Click **Save** to complete.

11. When all the updates and configuration steps are complete, select **Restart ASM** on the navigation pane to restart the Remote Supervisor Adapter II.

12. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter II. A window is displayed advising that the browser window will be closed. Click **OK** to continue.

Configuring the RSA II IP address and DHCP settings:

If you are using a new RSA II service processor with your integrated server hardware, you might need to configure networking settings before you can sign into it with the web interface.

Do the following steps to configure the RSA II.

1. Turn on the System x product. Refer to the system documentation to complete this step.
2. Press F1 when prompted to start Setup.
3. Highlight **Advanced Setup** using the up or down arrow keys and press Enter to select.
4. Highlight **RSA II Settings** (this option is only available when RSA II hardware is installed in the system) using the up or down arrow keys and press Enter to select.
5. Highlight **DHCP Control** using the up or down arrow keys and use the left or right arrow keys to change the value to **Use Static IP**.
6. Highlight **Static IP Address** using the up or down arrow keys and use the backspace key to position the cursor and enter an IP address.
7. Highlight **Save Values and Reboot RSA II** using the up or down arrow keys and press Enter to select and perform the action. A screen will display confirming the action.
8. Press Esc two times to return to the main setup menu.

Updating iSCSI initiator firmware

To update the iSCSI initiator firmware in a System x or blade server, see the Updating iSCSI initiator firmware task in the iSCSI Initiator Hardware Configuration manual.

Related information

↪ iSCSI Initiator Hardware Configuration

Setting the System x start options

Configure the options that your System x product will use to start and communicate on the iSCSI network.

It is recommended that you disable the Pre-Boot Execution Environment (PXE) option for all integrated Ethernet ports. You must turn the boot fail counter and virus detection off.

1. Turn on the System x model. Refer to the server documentation to complete this step.
2. Press F1 when prompted to enter setup. This will be shortly after the IBM eServer™ logo appears on the display.
3. Highlight **Start Options** using the up or down arrow keys and press Enter to select.
4. If you are installing Windows Server 2008, select **Start Sequence Options** and configure the boot order to first **Harddisk 0**, and then **CD-ROM/DVD**.
5. Highlight **Planar Ethernet PXE/DHCP** using the up or down arrow keys. Use the right or left arrow keys to change the value to **Disabled**.
6. Highlight **Boot Fail Count** using the up or down arrow keys and use the right or left arrow keys to change the value to **Disabled**.

7. Highlight **Virus Detection** using the up and down arrow keys and use the right or left arrow keys to change the value to **Disabled**.

8. Press the Escape (Esc) key to return to the main setup menu.

Configuring the Baseboard Management Controller

These steps are required only for System x products that do not also have a Remote Supervisor II (RSA II) service processor installed.

Refer to worksheet item XSP1 in the *iSCSI Network Planning Worksheets* to determine which type of service professor is installed.

1. From the main setup menu, highlight **Advanced Setup** using the up or down arrow keys and press Enter to select.

2. Look for **RSA II Settings**.
   - If **RSA II Settings** exist, this indicates RSA II hardware is installed and the Baseboard Management Controller does not need to be configured. In this case, skip to the last step of this procedure.
   - If there are no **RSA II Settings**, RSA II hardware is not installed and you must continue with this procedure to configure the Baseboard Management Controller.

3. Highlight **Baseboard Management Controller (BMC) Settings** using the up or down arrow keys and press Enter.

4. Highlight **BMC Network Configuration** using the up or down arrow keys and press Enter to select.

5. Highlight **Static IP Address** (worksheet item XSP4) using the up or down arrow keys and use the backspace key to position the cursor for entry of the IP address from the *iSCSI Network Planning Worksheets*.

6. Highlight **Subnet Mask** (worksheet item XSP5) using the up or down arrow keys and use the backspace key to position the cursor for entry of the subnet mask from the *iSCSI Network Planning Worksheets*.

7. Highlight **Gateway** (worksheet item XSP6) using the up or down arrow keys and use the backspace key to position the cursor for entry of the gateway address from the *iSCSI Network Planning Worksheets*.

8. Highlight **Save Network Settings in BMC** using the up or down arrow keys and press Enter to select and perform the action. This will bring up the **BMC Settings saved!** screen.

9. Press Enter to return to the **Baseboard Management Controller (BMC) Settings** menu.

10. Highlight **User Account Settings** using the up or down arrow keys and press Enter.

11. Highlight **UserID 2** using the up or down arrow keys and press Enter.

12. On the **UserID 2 Account Settings** screen, highlight **UserID 2** using the up or down arrow keys and use the left or right arrow keys to change the value to **Enabled**.

13. Highlight **Username** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from worksheet item XSP7 in the *iSCSI Network Planning Worksheets*.

14. Highlight **Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from worksheet item XSP8 in the *iSCSI Network Planning Worksheets*.

15. Highlight **Confirm Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the same password as above.

16. Highlight **Privileged Limit** using the up or down arrow keys and use the left or right arrow keys to change the value to **Administrator**.

17. Highlight **Save User Account Settings to BMC** using the up or down arrow keys and press Enter.

18. The **BMC User Account Settings Saved!** Screen will be displayed. Press Enter to return to the **User Account Settings** menu.

19. Press Esc to return to the **Baseboard Management Controller (BMC) Settings** menu.

20. Press Esc to return to the *Advanced Setup* menu.
21. Press Esc to return to the main setup menu.

Updating and configuring the BladeCenter chassis

Use these tasks to prepare your blade hardware for integration with i5/OS and the System i hardware.

The management module must be set to the factory default values to perform the procedure in this section. If the management module IP address is no longer known, it can be set back to the defaults, using the IP reset button on the management module. Refer to management module documentation to complete this task.

Refer to the README file printed earlier during the management module firmware download. Use the README instructions along with the steps below to perform the firmware update. The README will contain any changes necessary to the general instructions listed below. Follow the directions in the README wherever differences occur.

Also at this time, the management module must have an Ethernet cable plugged into its Ethernet port. Refer to BladeCenter or management module documentation to complete these tasks. Plug the other end of this cable into the Ethernet connector of the computer containing the downloaded management module update package. In some cases, a switch or hub may also be necessary to connect.

Note: The following steps are performed on the computer containing the update package and not on the BladeCenter console.

1. Set the IP address to something in the same subnet as the management module default IP address of 192.168.70.125 such as 192.168.70.101 and set the subnet mask to 255.255.255.0
2. Unpack the .zip file you downloaded earlier to extract the firmware update files.
3. Ensure the BladeCenter AC power cords are plugged into an appropriate power source to provide power for the management module. Refer to BladeCenter documentation to complete this step. Allow about 30 seconds after performing this step for the management module to boot.
4. Open a Web browser. In the address or URL field, type the IP address (192.168.70.125) of the management module to which you want to connect. The Enter Password window will open.
5. Type the user name and password on the Enter Password window. The management module has a default user name of USERID and password of PASSW0RD (where 0 is a zero, not the letter O).
6. Select a timeout value on the next screen and click continue.

Once you have completed these steps, continue with the following tasks.

Updating the BladeCenter management module firmware

Use the Web interface to update the BladeCenter management module firmware.

You can being this procedure from any management module (MM) Web browser window.

1. Click **Firmware Update** on the navigation pane on the left, under **MM Control**.
2. On the Update MM Firmware window, select **Browse** and navigate to the files containing the firmware update. The files will have an extension of .PKT; and there might be multiple files with this extension.
3. Highlight one of these files and click the **Open** button. The README text may specify a particular order to select these files. If so, follow the README file instructions. The full path of the selected file is displayed in the Browse field.
4. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation window will be displayed when the file transfer is complete.
5. Verify that the file shown on the *Confirm Firmware Update* window is the one you want to update. If not, click **Cancel**.

6. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the Management Module is flashed. A confirmation window will be displayed when the update has successfully completed.

7. The README file text might direct you to restart the MM after completing the .PKT file update. If so, click **Restart** MM on the navigation pane on the left side of the window. Click **OK** to confirm the reset. The Web browser window will then close. A new Web browser window will have to be started and signed onto to continue.

8. Repeat the update procedure for any other .PKT files (steps 1 through 7).

Configuring the management module

Sign into the BladeCenter management module and configure it to work with integrated servers.

1. Select **Login Profiles** under **MM Control** in the navigation pane on the left side of the window.

2. On the next window will be a list of Login IDs, find the entry for the default login ID value of **USERID** and click on that entry.

3. A Login Profile window is displayed. Change the **Login ID** (worksheet item XSP7) and fill in the **Password** (worksheet item XSP8) and **Confirm password** fields based on the information entered in the *iSCSI Network Planning Worksheets* . Also, make sure the **Authority Level** is set to **Supervisor**. Click **Save** to complete this step

4. To configure the MM network settings, select **Network Interfaces** under **MM Control** in the navigation pane on the left side of the screen.

5. Use the values in the *iSCSI Network Planning Worksheets* to complete the following steps:

   a. Select **Enabled** from the **Interface** list.

   b. From the **DHCP** list select and set one of the following (worksheet item XSP3):

      1) **Disabled - Use static IP configuration**.

      2) **Enabled - Obtain IP config from DHCP server**. This option requires an operating DHCP server when you install the operating system.

   c. Enter a name for this MM in the **Hostname** (worksheet item XSP2) field.

   d. Enter a value for the following fields under the **Static IP Configuration** heading need to be filled in if the **Disabled – Use static IP** configuration value was selected for the **DHCP** field above:

      • **IP address** – type in the IP address (worksheet item XSP4).

      • **Subnet mask** – type in the desired subnet mask (worksheet item XSP5).

      • **Gateway address** – type in the gateway address (worksheet item XSP6).

   e. Click **Save** to complete configuring the network interfaces.

Updating the blade server Baseboard Management Controller firmware

Update the firmware for the Baseboard Management Controller (BMC) service processor on your blade system.

You should have already downloaded the blade server Baseboard Management Controller firmware was downloaded previously onto removable media. An alternate method of updating the blade server Baseboard Management Controller can be found in the related procedures section. The update media is required to do the update and should be accessible from the computer that is running the management module (MM) Web browser interface. This procedure starts from any MM Web browser window.

1. Select **Firmware Update** under **Blade Tasks** on the navigation pane on the left of the window.

2. On the Update Blade Firmware window, first click the pull-down in the **Target** field and highlight the desired blade server to update. Next, click **Browse** and navigate to the media containing the firmware update.

3. There should be a file with a .PKT extension on one of the update media, highlight it and click **Open**. The full path of the selected file will be displayed in the **Browse** field.

4. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation window will be displayed when the file transfer is complete.

5. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the blade server is copied. The update can take several minutes. A confirmation window is displayed when the update has successfully completed.

Verifying management module configuration information

Verify that the management module is correctly configured for an integrated server environment and that the configuration matches the information in the *iSCSI network planning worksheets*.

You should have completed the *iSCSI network planning worksheets*.

You can begin this procedure from any management module (MM) Web browser window.

1. Select **Hardware VPD** under Monitors on the navigation pane on the left side of the screen.

2. Scroll down to find the BladeCenter Hardware VPD heading.

3. Find the row in the **Blade Servers** portion of the displayed table corresponding to the blade server bay or bays to be attached.

4. Verify the information in the **Machine Type/Model** (worksheet item RS5) and **Machine Serial No.** (worksheet item RS4) columns in the table with the information in the "iSCSI network planning work sheets" on page 81. Correct any discrepancies on the worksheet and also in any i5/OS remote system configuration objects that may have been created. Refer to "Changing remote system configuration properties" on page 210 for information on how to make the configuration object corrections.

5. Scroll down the page to the **BladeCenter Server MAC Addresses** heading.

6. Find the row in the **Blade Servers** (worksheet item **RS5**) portion of the displayed table corresponding to the blade server bay(s) to be attached.

7. Verify the information for blade servers.

   - If you are using an iSCSI HBA expansion card, follow these steps:

     a. Locate **Daughter Card or Exp Card** in the Name column below the **Blade Servers** row.

     b. Verify the information in the **Daughter Card or Exp Card** row with the "i5/OS remote system configuration object work sheet" on page 84.

        – **MAC Address 1** corresponds to the iSCSI address for port 1 (work sheet item **RS13**).
        – **MAC Address 2** corresponds to the LAN address for port 1 (work sheet item **RS17**).
        – **MAC Address 3** corresponds to the iSCSI address for port 2 (work sheet item **RS13**).
        – **MAC Address 4** corresponds to the LAN address for port 2 (work sheet item **RS17**).

   - If you are using an embedded Ethernet NIC or an Ethernet NIC expansion card for iSCSI, follow these steps:

     a. Locate **Daughter Card or Exp Card** in the Name column below the **Blade Servers** row.

     b. Verify the information in the **Daughter Card or Exp Card** row with the "i5/OS remote system configuration object work sheet" on page 84.

        – **MAC Address 1** corresponds to the iSCSI and LAN addresses for port 1 (work sheet items **RS13** and **RS17**).
        – **MAC Address 2** corresponds to the iSCSI and LAN addresses for port 2 (work sheet items **RS13** and **RS17**).

8. Correct any discrepancies on the worksheet and also in any i5/OS remote system configuration objects that might be created. Refer to "Changing remote system configuration properties" on page 210 for information on how to make the configuration object corrections.

9. Select **Restart MM** on the navigation pane on the left side of the screen to restart the Management Module.

10. Click **OK** to confirm that you want to restart the Management Module. A window is displayed advising that the browser window will be closed. Click **OK**.

Updating and configuring the BladeCenter I/O module

Configure the BladeCenter I/O module to work in the integrated server environmnet.

1. Select **Admin/Power/Restart** under I/O Module Tasks on the navigation pane on the left side of the screen.

2. Scroll down the next page to find the **I/O Module Advanced Setup** heading. Use the **Select a module** pulldown to select the appropriate I/O module (**I/O module 3** for the first port on the iSCSI expansion card, **I/O module 4** for the second port on the card).

   Note: Make sure the pulldown for External ports has Enabled selected.

3. Click the **Save** button on the extreme lower right of the screen to save the values to the I/O module.

4. I/O module software may be updated at this time. The procedure varies depending on the manufacturer of the I/O module. Refer to the README text printed earlier along with the I/O module documentation to complete this task.

Configuring a blade system for an integrated server environment

Configure a blade system to work in an integrated server environment.

Updating the blade server BIOS

Update the system BIOS for the integrated server hardware.

Refer to the README file printed earlier during the BIOS update download. Use the README file instructions along with the following steps to perform the update. The README file will contain any changes necessary to the general instructions listed below. Follow the directions in the README file wherever differences occur.

1. Plug the BladeCenter's ac power cords into a power source. Refer to the BladeCenter documentation to complete this step.

2. Assign the KVM and Media Tray to the blade server to be updated. Refer to the blade server documentation to complete this step.

3. Insert the media containing the BIOS update in the drive and turn on the blade server. Refer to the blade server documentation to complete this step.

4. The server will boot off of the disk and present a window, choose **1 - Update POST/BIOS** from the list of options.

5. On the next window, you will be asked if you would like to move the current POST/BIOS image to the backup ROM location. If you select ′**Y**, the current code will be copied in to the backup bank immediately.

6. Select **N** for the next several display prompts until the **Save current flash code to disk** prompt is displayed.

7. Select **N** for the prompt to Save current flash code to disk.

8. Select the appropriate language, if prompted, or select the **Update BIOS** option. The update begins.

9. When the update is complete, remove the media and turn off the blade server's power. Refer to the blade server documentation to complete this step.

Updating iSCSI initiator firmware

To update the iSCSI initiator firmware in a System x or blade server, see the Updating iSCSI initiator firmware task in the iSCSI Initiator Hardware Configuration manual.

Related information

➥ iSCSI Initiator Hardware Configuration

Setting the blade start options

Configure the blade to work in the integrated server environment.

1. Turn on the blade server. Refer to the server documentation to complete this step.
2. Press F1 when prompted, after the IBM eServer logo appears on the display.
3. Highlight **Start Options** using the up or down arrow keys and press Enter.
4. If you are installing Windows Server 2008, select **Start Sequence Options** and configure the boot order to first **Harddisk 0**, and then **CD-ROM/DVD**.
5. Highlight **Planar Ethernet PXE/DHCP** using the up or down arrow keys. Use the right or left arrow keys to change the value to **Disabled**.
6. Highlight **Boot Fail Count** using the up or down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
7. Highlight **Virus Detection** using the up and down arrow keys and use the right or left arrow keys to change the value to **Disabled**.
8. Press the Esc key to return to the main setup menu.

Installing and configuring the iSCSI initiator

Complete these tasks to install a new iSCSI initiator in the System x or blade product and configure the initiator to communicate on the iSCSI network.

Refer to the iSCSI Initiator Hardware Configuration manual for the following tasks:
- Configuring the boot iSCSI initiator port
- Configuring advanced iSCSI initiator port settings
- Disabling boot for additional iSCSI initiator ports

Related tasks

"Completing the replacement iSCSI initiator configuration" on page 220

After you have updated the *iSCSI Network Planning Worksheets* with the new information from the procedures Replacing a System X or blade server iSCSI and Collecting and updating remote system network server configuration, you can complete the configuration of the iSCSI initiator by following the procedure in Installing and configuring the iSCSI initiator.

Related information

iSCSI Initiator Hardware Configuration

Cabling the iSCSI network

Use the information in this section to understand the basic concepts of cabling the network after you have installed and configured the iSCSI HBA.

Once the System x or blade system has been configured, the network needs to be cabled to complete the configuration. The first step is to locate the ports that need to be cabled into the network.

Before you cable the network locate each point or port that you will connect from the following:
- The i5/OS partition network interface; either a new adapter or an existing adapter being used for a TCP/IP connection.
- The System x or blade server service processor. Depending on which server you are attaching the location of the service processor will vary. You will need to refer to your System x or blade server documentation to complete this connection.
  - For a System x product, the RSA II or the BMC might be used as the service processor.
  - For blade hardware located in a BladeCenter the management module is used as a service processor.
- The iSCSI HBA connection is as follows:

- In the i5/OS partition and the System x product the port to connect to is located on the tailstock of the iSCSI adapter.
- In the blade server the port to connect is located on the module plugged into I/O bay number 3. This might be an internally wired port on an integrated switch or a fan-out cable from a pass-through module. Refer to the I/O module documentation to complete this connection.

There are many different ways to cable the network – the iSCSI configuration could even be added to an existing Ethernet network. All the possibilities won't be covered here. There are a couple of important considerations that must be observed when cabling the iSCSI configuration:

- Ensure each iSCSI HBA to be used in the System i hardware is reachable from at least one iSCSI HBA in the System x or blade system.
  - Ensure any iSCSI HBA in the System i product that is required for integrated server installation or boot is reachable from at least one boot iSCSI HBA port in the System x or blade system.
  - For maximum availability, ensure that alternate paths are present upon failure of an individual cable, iSCSI HBA, or switch in the iSCSI network. After you install the server, you can also use multipath input/output (I/O) and enable boot on multiple HBAs.
  - If you want to take advantage of spare iSCSI HBAs for integrated servers, ensure that the spare iSCSI HBAs in the System i product are reachable from iSCSI HBAs in the System x or blade system. See "Using hot spare iSCSI HBAs for integrated servers" on page 204.
- Ensure that the System i product network interface card and the service processor connection reside in the same network.

For help understanding different external switch considerations see Ethernet switches for iSCSI (www.ibm.com/systems/i/bladecenter/iscsi/switches.html).

Configuring i5/OS for iSCSI-attached integrated servers

Configure i5/OS settings to work with your integrated server.

Before you begin installing the integrated server, "i5/OS memory requirements" on page 60 for information about performance and memory use.

Important: If the QRETSVRSEC system value is not enabled, change the QRETSVRSEC system value on i5/OS to ensure that i5/OS keeps passwords (this prevents delays when users sign on).
1. On the i5/OS command line, enter the command `WRKSYSVAL SYSVAL(QRETSVRSEC)`
2. To change the value, enter a `2` in the `Option` field and press Enter.
3. Change the value of `Retain server security data` to 1.

Do these tasks to prepare the i5/OS operating system to work with integrated servers.

Installing the required i5/OS licensed programs and options for integrated servers

Do these steps to install the i5/OS licensed programs for iSCSI-attached integrated servers.

You need access to the licensed programs and options listed in "Software and firmware requirements for BladeCenter integration" on page 57 or "Software and firmware requirements for System x integration" on page 59.
1. Insert the i5/OS media containing the licensed program or option in an available device.
2. Type `GO LICPGM` and press Enter.
3. Choose option `10` from the `Work with Licensed Programs` menu; then press Enter.

a. Determine which required licensed programs are already installed as the same release as the 5761-SS1 *BASE i5/OS.
   b. If you do not see the version number, press F11.
   c. Press F3 to return to the Work with Licensed Programs menu.
4. Choose option 11 from the Work with Licensed Programs menu; then press Enter.
5. Page down the list of licensed programs and enter a 1 in the Option field next to each required licensed program.
6. Press Enter.
7. Enter the name of the installation device in which you inserted the i5/OS install media.
8. Press Enter. The system installs the selected licensed programs.
9. After installing licensed programs, install the latest cumulative program temporary fix (PTF) package from IBM. Note that there should be no users signed on to i5/OS when you install PTFs. If your system uses logical partitions, load the PTFs on the secondary partitions on which you are installing i5/OS Integrated Server Support and set them for apply delay. Then load them on the primary partition. Refer to Install program temporary fixes on a system with logical partitions.
10. To install the latest PTF, complete the following steps:
    a. On the i5/OS command line, type GO PTF and press Enter.
    b. To install the program temporary fix package, type 8 and press Enter.
    c. In the Device field, enter the name of your optical device.
    d. Use the default *YES for Automatic IPL unless your system uses logical partitions. Press Enter to install all PTFs. Unless you changed the value to *NO, your system automatically shuts down and restarts.

    For more information about PTFs see Software fixes in the Basic system operations topic collection.
11. If you are upgrading i5/OS and have integrated Windows servers installed, you need to upgrade existing integrated Windows servers to the new level. See "Installing updates to the Integrated Server Support software running on Microsoft Windows" on page 129.
12. If you are upgrading i5/OS and have integrated Linux servers installed, you need to upgrade existing integrated Linux servers to the new level. See "Maintaining the Linux integration code" on page 177.

Configuring i5/OS to use Service Processor Manager

The Service Processor Manager function of i5/OS Integrated Server Support is used for integrated server discovery and power control.

Alternatively, an IBM Director Server running on your i5/OS system can be used for integrated server discovery and power control.

Determine whether to use Service Processor Manager or IBM Director Server based on the following items:
* If IBM Director is not installed on the i5/OS system, then Service Processor Manager is used by default. The Service Processor Manager function is provided by an i5/OS PTF. See the IBM i PTFs Web page for the latest PTFs.
* If IBM Director is installed on the i5/OS system, then IBM Director Server is used by default. If you want to use Service Processor Manager instead of IBM Director Server, see "Enabling Service Processor Manager on i5/OS systems with IBM Director" on page 108.

Notes:
   * If any of your i5/OS service processor configuration uses multicast discovery, see "Converting i5/OS service processor configurations to use unicast discovery" on page 108.

- If you do not need IBM Director on your i5/OS system for other purposes, see "Deleting IBM Director from i5/OS."
- Service Processor Manager might be required for some System x and BladeCenter configurations. See the BladeCenter and System x models supported with iSCSI ![icon] Web page to determine if your server model requires Service Processor Manager.
- If you want to switch back to IBM Director, see "Switching from Service Processor Manager to IBM Director."
- If you have iSCSI-attached System x servers that use only a BMC service processor (an RSA II service processor is not installed), then you must update the BMC firmware to the latest level.

Enabling Service Processor Manager on i5/OS systems with IBM Director

If you want to use Service Processor Manager instead of IBM Director Server, then create a QITDSMGR data area.

If IBM Director is installed on your i5/OS system, then IBM Director Server is used by default for integrated server discovery and power control. If you want to use Service Processor Manager instead of IBM Director Server, then create a QITDSMGR data area using the following command:

```
CRTDTAARA DTAARA(QUSRSYS/QITDSMGR) TYPE(*DEC) LEN(4 0) VALUE(2)
```

Deleting IBM Director from i5/OS

If you use Service Processor Manager for integrated server discovery and power control, and if IBM Director on i5/OS is not needed for other purposes, then you can remove IBM Director from i5/OS.

Complete the following steps to remove IBM Director from the i5/OS operating system:
1. Stop the IBM Director Server, using System i Navigator:
   a. Expand **Network** → **Servers** → **User-Defined**.
   b. Right-click **IBM DIRECTOR** and select **Stop**.
2. Ensure that the IBM Director Server is not set to automatical start, using System i Navigator:
   a. Expand **Network** → **Servers** → **User-Defined**.
   b. Right-click **IBM DIRECTOR** and select **Properties**.
   c. Clear the **Start when TCP/IP starts** check box and click **OK**.
3. Delete the IBM Director product from the i5/OS operating system, using the following command:
   ```
   DLTLICPGM LICPGM(5722DR1) OPTION(*ALL)
   ```
4. If the QITDSMGR data area exists on the i5/OS operating system, delete it using the following command:
   ```
   DLTDTAARA DTAARA(QUSRSYS/QITDSMGR)
   ```

Converting i5/OS service processor configurations to use unicast discovery

To use unicast discovery, specify either the service processor host name or the IP address in the service processor configuration properties.

IBM Director supports multicast discovery of the System x or BladeCenter service processor, but Service Processor Manager does not. When switching from IBM Director to Service Processor Manager, you must change the properties of each service processor configuration that uses multicast discovery. To use unicast discovery, specify either the service processor host name or the IP address in the service processor configuration properties. See "Changing service processor configuration properties" on page 213 for details.

Switching from Service Processor Manager to IBM Director

If you are using Service Processor Manager, and you want to switch to use IBM Director for integrated server discovery and power control, complete the following steps:

| Ensure that IBM Director Server is started. See "Verifying that Director Server is installed and running" on page 228. If IBM Director is not installed on the i5/OS operating system, see the Installing IBM Director Server on i5/OS topic collection in the IBM Systems Software Information Center. You do not need to install IBM Director Console.

| 1. Optional: If the QITDSMGR data area exists on i5/OS, delete it using the following command:

| DLTDTAARA DTAARA(QUSRSYS/QITDSMGR)

| 2. Re-synchronize each i5/OS service processor configuration to ensure that IBM Director has access to the service processor user ID and password. Use the **Validate service processor user ID and password and store in NWSCFG** option on the System i Navigator (or the *SYNC option on the INZNWSCFG command). See "Initializing a service processor" on page 213 for details.

Configuring time synchronization for integrated servers

Time synchronization for your integrated server needs to be configured both in both i5/OS and the integrated server operating systems.

To keep the time on i5/OS and the integrated server synchronized, do the following steps:

1. Select a value for synchronize date and time in the Install Windows Server (INSWNTSVR) command or the change network server description (CHGNWSD) command. Possible values include:

   *YES The system synchronizes the time between i5/OS and the integrated Windows server every 30 minutes.

| ***NO** The system synchronizes the date and time only when the integrated server is started.

| ***NONE**
       The system does not synchronize the date and time for the integrated server.

2. Ensure that the i5/OS time, date, and time zone are correct. Once these values are set they will automatically update themselves every six months for daylight savings time adjustments. The QTIMZON system value replaces the need to manually change the QUTCOFFSET system value twice a year.

   After you complete the server installation you will need to configure additional settings at the integrated server console.

   If you have problems with time synchronization, check the i5/OS system value for LOCALE to make sure it is set properly.

   For iSCSI-attached integrated Windows and Linux servers, you can use the Change Network Server Description (CHGNWSD) command, Install Windows Server (INSWNTSVR) command, or the Install Linux Server (INSLNXSVR) command to configure time synchronization. This function is not available for integrated servers running VMware ESX Server.

Configuring i5/OS TCP/IP for integrated servers

Verify that i5/OS TCP/IP is configured if you want the integrated server to use these values.

If you have already configured TCP/IP domain and TCP/IP gateway (route) values for i5/OS, you can skip this topic.

If you want to use the i5/OS TCP/IP values when you install your integrated server, you must configure your i5/OS TCP/IP before installing the Windows operating system for your integrated server.

For more information about TCP/IP, see the TCP/IP topic.

If you have System i Navigator installed, you can use it to configure your TCP/IP connections. The System i Navigator online help tells you how to configure TCP/IP. If you do not have System i Navigator installed, follow these steps:

1. On the i5/OS console, enter the command `CFGTCP` and press Enter. The `Configure TCP/IP` menu appears.
2. Select option 12 `Change TCP/IP Domain information` and press Enter. The `Change TCP/IP Domain (CHGTCPDMN)` display appears.
3. Specify the `Local domain name`.
4. In the `Domain name server` field, specify up to 3 IP addresses and press Enter.

To add a TCP/IP gateway for i5/OS, do the following steps:

1. On the i5/OS console, enter the command `CFGTCP` and press Enter. The `Configure TCP/IP` menu appears.
2. From the `Configure TCP/IP` menu, choose option 2 `Work with TCP/IP routes`. The `Work with TCP/IP Routes` display appears.
3. Type 1 in the Option field to add a TCP/IP route. The `Add TCP/IP Route` display appears.
4. Fill in the appropriate fields with the information for your gateway address.

Preparing for the integrated server operating system installation

Create the i5/OSobjects that will be used by your integrated server.

Before performing the steps below, you should already have installed the hardware, updated the firmware, configured the BladeCenter or System x model and attached all the cables. See "Installing the iSCSI target in the server running i5/OS" on page 95 and "Installing the iSCSI initiator on the integrated server hardware" on page 95.

Before starting the operating system installation, you should perform the following steps to prepare i5/OS.

Creating an NWSH object for each new System i iSCSI HBA port

The network server host adapter (NWSH) object that represents the iSCSI HBA must be started before i5/OS and your integrated server can use the HBA.

This step corresponds to Step 14 in the BladeCenter or System x iSCSI Installation Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

Use one of the following tasks to create a NWSH object for each port of the iSCSI HBA that you installed in the System i product.

Creating a network server host adapter (NWSH) object with System i Navigator:

To create a network server host adapter using System i Navigator, follow these steps:

1. Determine the i5/OS hardware resource name that was assigned to iSCSI HBA. Find the Network Server Host Adapter resource with physical location values that match the location of the newly installed iSCSI HBA. Use either of the following methods.
   a. Expand **Configuration and Service → Hardware → Communications**.
   b. Display the **Properties** of each resource with the description Network Server Host Port.
   c. On the **Physical Location** tab of the property sheet, look at the **Frame ID** and **Card position** values.
2. Expand **Integrated Server Administration**.
3. Expand **iSCSI Connections**.
4. Right-click **Network Server Host Adapters**.
5. Select **New Network Server Host Adapter**.

6. On the **General** tab:
    a. Enter the NWSH device **Name** and **Description**.
    b. Select the **Hardware resource**.
    c. Select the **Object authority**. You can use the default value **Change**.
7. On the **Local (Target) Interface** tab:
    a. Select the cable connection type. If the hardware is physically connected to an Ethernet switch, you can use the default value **Network**.
    b. Enter information to define the SCSI and LAN interface attributes for the iSCSI HBA.
8. Click **OK**.

Creating a network server host adapter object (NWSH) with the character-based interface:

Do these steps to create a Network Server Host Adapter (NWSH) object for an iSCSI HBA using the character-based interface.

1. Determine the hardware resource for the iSCSI HBA.
    a. Run the following command to display a list of the communications resources: `WRKHDWRSC *CMN`
    b. Use **option 7=Display resource detail** on each resource with the description **Network Server Host Port**.
    c. Examine the **Location:** entry to determine the frame ID and card position values.

    For more information see Work With Hardware Resources (WRKHDWRSC).
2. Type `CRTDEVNWSH` and press `F4` to display the command prompt screen. For more information, see Create Device Desc (NWSH) (CRTDEVNWSH) in the CL command reference topic collection.
3. Fill in the command parameters and press `Enter` to run the command.

Starting the NWSH for each System i iSCSI HBA port that the server will use

Start any NWSHs that will be used by the iSCSI-attached integrated server. Starting the NWSH makes the iSCSI HBA available during the operating system installation.

- If you are using System i Navigator, see "Starting a network server host adapter" on page 207.
- If you are using the i5/OS character-based interface, use the Vary Configuration (VRYCFG) command.

    For example, enter `VRYCFG CFGOBJ(`*nwshname*`) CFGTYPE(*DEV) STATUS(*ON)` where *nwshname* is the NWSH name.)

After starting the NWSH, the NWSH status should be ACTIVE.

If the NWSH does not start, see the Troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html) Web page.

Creating and initializing a service processor configuration object for the integrated server hardware

This object represents the service processor for the integrated server hardware.

This step corresponds to slide 15 in the BladeCenter or System x iSCSI installation overview animation.

If the "BladeCenter or System x service processor work sheet" on page 83 indicates that a new service processor configuration object needs to be created, use the information from the work sheet to create it now using either of the following methods. You can accept the default values for any items that are not listed in the work sheet.

A service processor network server configuration (NWSCFG subtype SRVPRC) object must be created for the service processor or Management Module of each System x or BladeCenter that is used to run an iSCSI-attached integrated server.

Notes:

1. If you are using the "iSCSI Network Planning Guide" on page 62, use the "BladeCenter or System x service processor work sheet" on page 83 to help you do the following task.
2. A service processor configuration is not needed for each blade in an IBM BladeCenter chassis. Only one service processor configuration is needed for the BladeCenter chassis.

Creating a new service processor configuration with System i Navigator:

Do these steps to create a service processor configuration object for a new integrated server.

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Service Processors**.
4. Select **New Service Processor Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Specify either a **Host name**, **Internet address**, or **Serial number** to identify the service processor on the network
   - Select the **Object authority**. You can use the default value **Change**.
6. Click **OK**.
7. Initialize the service processor configuration object. See "Initializing a service processor" on page 213.

   Important: You must initialize the new service processor configuration. This step ensures that the following situations are met.
      a. The correct service processor user ID and password are stored in the service processor configuration.
      b. The connection to the remote system service processor is physically cabled and configured.

      If you do not do this step, the i5/OS operating system will not be able to communicate with the integrated server.

Creating a new service processor configuration with the character-based interface:

Do these steps to create a new service processor configuration object for a new integrated server.

1. Type CRTNWSCFG TYPE(*SRVPRC) and press F4 to display the command prompt screen.
2. Press **Enter** once to display more parameters.
3. Fill in the command parameters and press Enter again to run the command.
4. Initialize the service processor configuration object.
   a. Type INZNWSCFG and press F4 to display the command prompt screen. For more information, see Initialize NWS Configuration (INZNWSCFG).
   b. Type the service processor configuration name.
   c. Type *SYNC for the processing option.
   d. Enter the user name and password for the service processor.
   e. Press Enter to run the command.

   Important: You must initialize the new service processor configuration. This step ensures that

a. The correct service processor user and password are stored in the service processor configuration.

b. The connection to the remote system service processor is physically cabled and configured properly.

If you do not do this step, i5/OS will not be able to communicate with the integrated server.

If you have problems, see Troubleshooting on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Creating a remote system configuration object for an integrated server

This i5/OS object contains information about the type and model and other aspects of the integrated server hardware.

Note: This step corresponds to slide 16 in the BladeCenter or System x iSCSI Installation

Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

Attention: If you need to define more than one remote interface (more than one iSCSI HBA port on the BladeCenter blade or System x model), then it is recommended that you use the System i Navigator interface to create the remote system configuration object. See the CRTNWSCFG and CHGNWSCFG Prompting Problems When defining more than one remote interface troubleshooting topic for more information.

Creating a remote system configuration object:

A remote system network server configuration (NWSCFG subtype RMTSYS) object must be created for each System x or blade system that will be used to run an iSCSI-attached integrated server.

Note: If you are using the iSCSI Network Planning Guide, you should use the "i5/OS remote system configuration object work sheet" on page 84 to help you do the following task.

To create a remote system configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Remote Systems**.
4. Select **New Remote System Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Select the **Service processor configuration**.
   - Specify the **Remote system identity**.
   - Select the **Object authority**. You can use the default value **Change**.
6. On the **Remote Interfaces** tab, enter information to define the SCSI and LAN interface attributes for the remote system.
7. Specify values on the **Boot Parameters** and **CHAP Authentication** tabs if wanted.
8. Click **OK**.

Note: The network server host adapter and the remote system configuration define IP address information for opposite sides of the iSCSI network. When connected by a simple, switched network, the following rules apply:

- The SCSI internet addresses in these two objects that are connected by a switch must be in the same subnet. For example, with IP addresses of the form a.b.x.y and 255.255.255.0 subnet masks, a.b.x must be the same value for both objects.
- The LAN internet addresses in these two objects that are connected by a switch must be in the same subnet.
- In the network server host adapter, the gateway elements can be any unassigned IP address in any subnet if you don't have a gateway in your network.
- In the remote system configuration, the gateway elements should be blank if you don't have a gateway in your network.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Creating a remote system configuration object using the character-based interface:

Do these steps to create a remote system configuration object for a new integrated server.
1. Type `CRTNWSCFG TYPE(*RMTSYS)` and press F4 to display the command prompt screen.
2. Press **Enter** once to display more parameters.
3. Fill in the command parameters and press **Enter** again to run the command.

For more information, see the Create NWS Configuration (CRTNWSCFG) command documentation.

Verifying that the initiator system is accessible and powered off or offline

Use these tasks to verify that the i5/OS operating system can contact the service processor of the System x or blade hardware and that the hardware is powered off or offline before you begin installing an iSCSI-attached integrated server.

i5/OS should be able to reach the service processor of the integrated server hardware before you begin the installing the integrated server operating system. This connection will be used to power on the integrated server hardware.

Note: A `not found` error when the remote system status is displayed might mean that i5/OS has not completed its system discovery process. If this is the case, i5/OS completes its system discovery process within a few minutes, so try displaying the remote system status again. If you continue to get a `not found` error or get some other errors, see the Troubleshooting Web page.

If the remote system is not in a Powered off (Offline) state, power it off now before continuing. If installing a blade, just the blade should be powered off, not the BladeCenter chassis.

Displaying remote system status:

Do these steps to display the status for the System x or BladeCenter hardware for iSCSI-attached integrated servers.

You can use the status to help you determine if hardware is available for use by an iSCSI-attached integrated server.
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Remote Systems**.
4. Right-click a remote system configuration from the list available.
5. Select **Status**.
6. The status of the remote system hardware is shown.
7. Click **Cancel** to close the panel.

If you want to use a CL command, see WRKNWSCFG.

Displaying remote system status with the character-based interface:

Do these steps at the i5/OS command line.
1. Enter WRKNWSCFG TYPE(*RMTSYS) at the i5/OS command line.
2. Type 8 next to **Work with status next to your remote system configuration name** and press Enter.
3. Verify that the remote system status is **Offline**.

For more information see Create NWS Configuration (CRTNWSCFG).

Creating a connection security configuration object

This object is used by the system and is required for iSCSI-attached integrated servers.

This step corresponds to slide 17 in the BladeCenter or System x iSCSI Installation Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

If the i5/OS Connection Security Configuration Object Worksheet in the iSCSI Network Planning Guide indicates that a new connection security configuration object needs to be created, use the information from the worksheet to create it now using either of the following methods. You can accept the default values for any items that are not listed in the work sheet.

Creating a connection security configuration object:

Do these steps to create a connection security configuration object for an integrated server.

Notes:

1. If you are using the "i5/OS connection security configuration object work sheet" on page 89, you should use the network planning worksheets to help you do the following task.

To create a connection security configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Connection Security**.
4. Select **New Connection Security Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Select the **Object authority**. You can use the default value **Change**.
6. Click **OK**.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Creating a connection security configuration object with the character-based interface:

Do these steps to create a connection security configuration object for a new integrated server.
1. Type CRTNWSCFG TYPE(*CNNSEC) and press F4 to display the command prompt screen.
2. Fill in the command parameters and press **Enter** to run the command.

For more information, see Create NWS Configuration (CRTNWSCFG).

Installing, configuring, and managing Windows in iSCSI-attached integrated server environments

Configure the Windows operating system to work in an iSCSI-attached integrated server environment.

Installing the Windows operating system on an integrated server

The Install Windows Server (INSWNTSVR) CL command starts installing the Windows operating system for your integrated server. Use these tasks to prepare your system to run the command and start the installation.

Windows server installation advisor

Use this advisor to select the parameters that you will use for the Install Windows Server (INSWNTSVR) CL command.

The Windows server installation advisor will generate a command that you can copy and paste to your terminal.

Installation worksheet for the Install Windows Server command

Use this worksheet to select the parameters that you will use for the Install Windows Server (INSWNTSVR) CL command when you install an iSCSI-attached integrated Windows server.

Planning for the Install Windows Server (INSWNTSVR) CL command

Before you install the Windows operating system, complete either the Windows server installation advisor or this installation worksheet.

If you need more information on the parameters, see the Install Windows Server (INSWNTSVR) topic.

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers

Field	Description and Instructions	Value
Network server description (NWSD) Required	Defines the operating characteristics and communications connections of the network server that controls the integrated Windows server. Use a name that is easy to remember. The name can have up to 8 characters. Use only the characters A - Z and 0 - 9 in the name, and use a letter for the first character. This object is created when you run the INSWNTSVR command. **Note:** When you install Windows Server 2003, the network server description name is also the computer name and TCP/IP host name of the integrated server.	Name:
Install type (INSTYPE) Required	Specify the full install type.	*FULL
Resource name (RSRCNAME) Required	Identifies the Windows server hardware. For iSCSI-attached System x and IBM BladeCenter systems, specify a resource name of *ISCSI.	*ISCSI
Windows server version (WNTVER) Required	Specifies the version of windows. Specify *WIN2003 for Windows Server 2003 or *WIN2008 for Windows Server 2008.	

Field	Description and Instructions	Value
Virtual Ethernet port (VRTETHPORT) Optional	Specifies the TCP/IP configuration for the virtual Ethernet networks used by the server. ***NONE:** Specifies that there is no virtual Ethernet port configuration. **Element 1: Port** • ***VRTETH***x***:** The network server virtual Ethernet port *x* is configured, where *x* has a value of 0 through 9. **Element 2: Windows internet address** The Windows internet address for the port in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255. **Element 3: Windows subnet mask** The subnet mask for the Windows internet address in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255. **Element 4: Associated port** The resource name that describes the port that is used to establish a connection between a Windows network server and the network. • ***NONE** An associated port resource name is not associated with the line. • **resource-name** The resource name.	**Virtual port 1** *VRTETH*x*: IP Address: Subnet mask: Associated Port (Optional): **Virtual port 2** *VRTETH*x*: IP Address: Subnet mask: Associated Port (Optional): **Virtual port 3** *VRTETH*x*: IP Address: Subnet mask: Associated Port (Optional): **Virtual port 4** *VRTETH*x*: IP Address: Subnet mask: Associated Port (Optional):
TCP/IP local domain name (TCPDMNNAME) Optional, only valid for Windows server 2003	Specifies the TCP/IP local domain name associated with the integrated server. You can specify *SYS to use the same value the i5/OS operating system uses.	Domain name:
TCP/IP name server system (TCPNAMSVR) Optional, only valid for Windows server 2003	Specifies the Internet address of the name server used by the integrated server. You can specify up to three Internet addresses, or you can specify *SYS to use the same value that i5/OS operating system uses.	Internet address for the TCP/IP name server:
To workgroup (TOWRKGRP) Optional, only Windows server 2003	Specifies the name of the Windows server workgroup in which the server participates.	Workgroup:
To domain (TODMN) Optional, only valid for Windows server 2003	Specifies the name of the Windows domain in which the server participates.	Domain name:

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers (continued)

Field	Description and Instructions	Value
Installation source and system drive sizes and auxiliary storage pool (ASP) (SVRSTGSIZE) (SVRSTGASP) (STGASPDEV) Required	Specify the size of the network server storage spaces for the installation source and system drives and in which ASP (1 - 255) you want them. An ASP device name can be specified in place of the ASP numbers 33-255 when the storage space should be created in an independent auxiliary storage pool. However, if a name is used, the ASP number field must be left as the default value of 1 or the place holder value of *N. The installation source drive (drive D) must be large enough to hold the contents of the I386 directory on the Windows server installation CD image and the IBM i5/OS Integrated Server Support code. The installation source drive (drive D) must be large enough to hold the IBM i5/OS Integrated Server Support code. For installations of Windows Server 2003, the contents of the I386 directory on the Windows server installation CD image are also copied here. The limit is 1,024 to 1,024,000 MB, depending on your resource capabilities. Consider these factors: • Your version of Windows server (Refer to Microsoft documentation for operating system requirements.) • Primary usage (print/file serving) and number of Terminal Server users. • Free space on system drive. • Application resource requirements. • Need for crash dump file. • Installed memory on server	**Installation source drive:** Size: ASP: ASPDEV: **System drive:** Size: ASP: ASPDEV:
Installation source and system drive sizes and auxiliary storage pool (ASP) (Continued)	**Notes:** 1. The INSWNTSVR command automatically sets the system drive size if a size to a minimum size that is determined based in part on factors such as the Windows version and installed memory. 2. When deciding the size of each drive, allow room for future needs such as new applications or upgrades to the Windows server product. If you specify *CALC for SVRSTGSIZE, note that i5/OS will allocate the minimum disk size necessary to install Windows. If you need additional space for applications or data you should consider manually specifying a drive size. 3. Support for independent ASPs (33 - 255) is provided through System i Navigator. For more information about working with independent ASPs, see Independent disk pools. Both the Information Center and System i Navigator refer to ASPs as disk pools. To use an independent ASP, the ASP device must be available before you run the the INSWNTSVR command.	

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers (continued)

Field	Description and Instructions	Value
License mode (LICMODE) Optional, only valid for Windows server 2003	Determines the license mode to install Microsoft Windows server. **Element 1 License mode:** ***PERSEAT** Indicates that a client license has been purchased for each computer that accesses the server. ***PERUSER** Indicates that the end user purchased a client access license for each device or user accessing the Windows Server 2003 Server. ***PERSERVER** Indicates that client licenses have been purchased for the server to allow a certain number of concurrent connections to the server. **Element 2 Client licenses:** ***NONE** Indicates that no client licenses are installed. *NONE must be specified when *PERSEAT or *PERUSER is specified. **number-client-licenses:** Specifies the number of client licenses purchased for the server being installed.	License type: Client licenses: Terminal services:
License mode (LICMODE) (Continued)	Element 3 Windows Terminal Services: ***PERDEVICE** *PERDEVICE Installs and configures Windows Server 2003 Terminal Services to require that each connected device has a valid Windows Terminal Server access license. If the client has a Terminal Server access license, it can access more than one Terminal Server. ***PERUSER** Installs and configures Windows Server 2003 Terminal Server to provide one Terminal Server access license for each active user. ***NONE** There are no Terminal Server desktop licenses for this server.	
Propagate domain user (PRPDMNUSR) Optional	Specifies if this server should be used to propagate and synchronize users to the Windows domain or active directory. ***YES** Send user updates to the Windows domain or active directory through this server. ***NO** Do not send user updates to the Windows domain or active directory through this server.	

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers (continued)

Field	Description and Instructions	Value
Disable user profile (DSBUSRPRF) Optional	Specifies whether to disable the integrated servers user profiles if the corresponding i5/OS user profiles are disabled. ***AUTO** Integrated server user profiles are disabled if corresponding i5/OS user profiles are disabled. ***NO** Integrated server user profiles are not disabled if corresponding i5/OS user profiles are disabled.	

Restricted device resources (RSTDEVRSC)
 	
Optional
	Restricts System i tape and optical devices from being used by the integrated server.
	
	*NONE
	  Restricts no tape or optical devices from being used by the integrated server.
	
	*ALL Restricts all tape and optical devices from being used by the integrated server.
	
	*ALLTAPE
	  Restricts all tape resources from being used by the integrated server.
	
	*ALLOPT
	  Restricts all optical resources from being used by the integrated server.
	
	restricted-device
	  Specify up to 10 device resources that you do not want the integrated server to use.	

Virtual Ethernet point to point (VRTPTPPORT) Optional	A local area network exists between i5/OS and Windows server. Both the i5/OS side and the Windows server side of this LAN have IP addresses and subnet masks. **Note:** By default, the INSWNTSVR command sets up these addresses automatically. These addresses are in the form of 192.168.xx.yy. If your site uses class C addresses, it is possible for duplicate IP addresses to be generated. To avoid potential conflicts, you can also specify Internet addresses that you know will be unique across your system. Use addresses in the form a.b.x.y where a.b.x is the same value for both sides of the point to point virtual Ethernet and ensure that the point to point virtual Ethernet occupies its own subnet on i5/OS. Use the Virtual PTP Ethernet port parameter under additional parameters of the INSWNTSVR command. The subnet mask is always 255.255.255.0.	i5/OS-side IP address: Windows server-side IP address:

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers (continued)

Field	Description and Instructions	Value
Storage path (STGPTH) Required	Specifies the storage path the storage spaces can use. This information consists of the Network server host adapter (NWSH) description. **Note:** You can add additional storage paths after you install your server. **name** Specify the name of an existing Network server host adapter (NWSH) description. See "Creating an NWSH object for each new System i iSCSI HBA port" on page 110.	NWSH name:
Pool identifier (POOL) Required	Specifies the shared data storage pool this integrated server should use. For most environments, you should configure the server to use a shared memory pool. See "i5/OS memory requirements" on page 60. ***BASE** The base pool is to be used by this integrated server. ***SHRPOOLnn** Specifies the shared pool to be used by this integrated server. There are sixty general-purpose shared pools, identified by special values *SHRPOOL1 to *SHRPOOL60.	Pool identifier:

Virtual Ethernet path (VRTETHPTH)
 	
Required
	Specifies the virtual Ethernet paths the Ethernet line descriptions can use. This information consists of two parts including the virtual Ethernet port and the Network server host adapter (NWSH) device description. You can enter up to five values for this parameter. You must enter at least one virtual Ethernet path which is the path to be used by the *VRTETHPTP line description name.
	Note: You can add virtual Ethernet paths after you install your server.
	
	Element 1: Port
	
	       *VRTETHPTP
	
	       The network server virtual Ethernet point to point port is configured.
	
	       *VRTETH*x* The network server virtual Ethernet port x is configured, where x has a value of 0 through 9.
	
	Element 2: Network server host adapter
	
	       name Specify the name of an existing Network server host adapter (NWSH) description. The network server host adapter name does not need to be unique for each VRTETHPTH parameter on this NWSD. This can be the same NWSH object that you specified for Storage path.
		Virtual Ethernet path:
		
		Port:
		
		NWSH name:

Table 16. Install Windows Server (INSWNTSVR) CL Command parameters for iSCSI-attached integrated servers (continued)

Field	Description and Instructions	Value
Remote system NWSCFG (RMTNWSCFG) Required	Specify the name of an existing remote system network server configuration to use with this server. For information about creating this object, see "Creating a remote system configuration object for an integrated server" on page 113.	Name:
Service processor NWSCFG (SPNWSCFG) Required	Specify the name of an existing service processor network server configuration to use with this server. For information about creating a service processor configuration object, see "Creating and initializing a service processor configuration object for the integrated server hardware" on page 111.	Name:
Connection security NWSCFG (CNNNWSCFG) Required	Specify the name of an existing connection security network server configuration to use with this server. For information about creating this object, see "Creating a connection security configuration object" on page 115.	Name:

Installing the Windows operating system

Run the Install Windows Server (INSWNTSVR) CL command to begin installing the Windows Server 2003 or 2008 operating system on your integrated server.

Starting the Windows installation at the i5/OS console:

Run the Install Windows Server (INSWNTSVR) command to create the system disk and begin installing the Windows Server operating system on the iSCSI-attached integrated server.

This step corresponds to slides 19-22 in the BladeCenter or System x iSCSI Installation Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

To install a server with the Install Windows Server (INSWNTSVR) command, you need *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority. You must have your Windows server license key available. In most cases, it is printed on the back of the installation CD jewel case.

1. Insert the installation media in the optical drive.
   - When installing Windows Server 2008, place the Windows Server 2008 DVD in the blade center media tray or System x DVD drive.

     Remember: If you are installing Windows Server 2008 on a blade in a BladeCenter system, you must also assign the BladeCenter KVM and media tray to the blade.
   - When performing an installation type of *FULL, place the installation CD in the System i optical drive (unless you plan to use an image of the installation CD).
2. Use one of the following methods to begin the installation:
   - If the Install Windows server (INSWNTSVR) command generated by the Windows server installation advisor is available:
     a. Call QCMD at the i5/OS command line to start a command entry prompt and select F11=Display Full.
     b. Paste the INSWNTSVR command generated by the Windows server installation advisor at the i5/OS command line and press Enter to run the command.

c. The installation starts and can take up to an hour. You may be prompted to enter additional information. Afterward, go to "Continuing the Windows Server 2003 installation from the integrated server console" on page 126 or "Continuing the Windows Server 2008 installation from the Windows console" on page 128.

   - Otherwise, begin the installation at the i5/OS command line by typing INSWNTSVR and pressing F4 to prompt the command. Type the values from the "Installation worksheet for the Install Windows Server command" on page 116 in each of the following fields:

3. In the Network server description field (see "Network server description" on page 41 for more information), type the server name from the "Installation worksheet for the Install Windows Server command" on page 116 and press Enter.

4. In the Install type field, type the value (*FULL or *BASIC) that you filled out in the "Installation worksheet for the Install Windows Server command" on page 116.

5. In the Resource Name field, type the information that you filled out in the "Installation worksheet for the Install Windows Server command" on page 116.

6. Choose the Windows server version you want to install; press Enter.

   Note: Windows Server 2003 or Windows Server 2008 is required for iSCSI-attached servers.

7. For Windows Server 2003, if you want to install the server from a stored image instead of the physical CD, specify the path to that image in the Windows source directory field.

8. In the Install option field, use the default *INSTALL.

9. If you want the installation to configure TCP/IP properties for any network adapters installed in the iSeries which will be controlled by the new integrated server, specify the Windows TCP/IP configuration values from the "Installation worksheet for the Install Windows Server command" on page 116. Otherwise, skip this step and use the default value *NONE.

   Note: The TCP/IP port configuration (TCPPORTCFG) parameter is not available for *WIN2008 (Windows Server 2008).

10. To install and configure an optional virtual Ethernet port, specify the Windows TCP/IP configuration values for the Virtual Ethernet port field from the "Installation worksheet for the Install Windows Server command" on page 116.

11. Type the values from the "Installation worksheet for the Install Windows Server command" on page 116 in the TCP/IP local domain name and TCP/IP name server system fields.

   Note: The TCP/IP name server system and Library parameters are not available for *WIN2008 (Windows Server 2008).

12. In the fields for the Server storage spaces, type the values from the "Installation worksheet for the Install Windows Server command" on page 116

   a. Specify values for the Install source size and System size fields or select the default *CALC to allow the system to calculate the minimum size.

      Tip: For Windows Server 2008 only, specify a minimum system drive size of 15 000 MB. Be sure to allow room for additional items, such as optional Windows features, Windows service updates, applications, page files, crash dump support, data, and future expansion.

   b. If you want to choose a different auxiliary storage pool (ASP) for the install source and system drives, specify it in the corresponding element of either the Storage space ASP or Server storage ASP device fields.

13. For Windows Server 2003, you can specify additional Windows network and licence information.

   a. Specify either a Windows workgroup or domain in the corresponding To workgroup or To domain parameters.

   b. Specify the name of the user who holds the Windows server license you are installing in the Full Name field.

    c. Specify the name of the organization that holds the Windows server license you are installing, in the `Organization` field.

> **Note:** The To workgroup (TOWRKGRP), To domain (TODMN), Full Name (FULNAM) and Organization (ORG) parameters are not available for *WIN2008 (Windows Server 2008) installations.

14. In the `Language version` field, specify `*PRIMARY` to have the IBM i5/OS Integrated Server Support use your primary language. To prevent problems with predefined names that cannot be enrolled, make sure that the integration licensed program and Windows server will be using the same language. If you need to know which languages the command supports, look at "Selecting a language for the integrated server operating system installation" on page 89.

15. In the `Propagate domain user` field, specify if this server should be used to propagate and synchronize users to the Windows domain or active directory.

16. In the `Disable user profile` field, specify one of the following values:
    - `*AUTO` Integrated server profiles are disabled if corresponding i5/OS user profiles are disabled
    - `*NO` Integrated server user profiles are not disabled if corresponding i5/OS user profiles are disabled

17. For Windows Server 2003 installations, specify values for the Windows license. In the `Windows license key` field, specify the 25 character product license key that Microsoft has provided, including the dashes. The license key is usually located on a label provided with the installation media.

> **Note:** This parameter is not available for *WIN2008 (Windows Server 2008) installations.

18. For Windows Server 2003 installations, specify the following information:
    a. In the `License type` field, specify the type of Windows server license that you purchased.
    b. If you specified `*PERSERVER` in the `License type` field, then in the `Client licenses` field, specify the number of client licenses that you purchased.
    c. Enter the `Terminal services` options to install in the `Terminal services` field.

> **Note:** These parameters are not available for *WIN2008 (Windows Server 2008) installations.

19. In the `Restricted device resources` field, type the value from the "Installation worksheet for the Install Windows Server command" on page 116.

20. In the `Storage path` field, specify the name of the Network server host adapter to use for iSCSI storage communications. For more information, see "Network server host adapters" on page 42.

21. If you configure a shared data memory pool for this integrated server to use, as described in "iSCSI virtual I/O shared data memory pool" on page 61, specify the memory pool in the `Pool identifier` field.

22. In the `Virtual Ethernet path` field, enter the name of one or more Network server host adapters to use for iSCSI LAN communications. Specify at least one value for the *VRTETHPTP port and any additional ports specified above for the `Virtual Ethernet port` field.

23. Enter names for the network server configuration objects you will use for your installation.
    a. Enter an existing network server configuration name for the following fields or select the default values for the following objects:
       - Remote system NWSCFG
       - Service processor NWSCFG
       - Connection security NWSCFG
    b. Press `Enter`.

24. If prompted, enter service processor configuration information from the "Installation worksheet for the Install Windows Server command" on page 116 in these fields, when using the defaulted `Service processor NWSCFG` name:
    - In the `Initialize service processor` field:

- Select the unicast option to use in the Enable unicast field:
    a. Enter value(s) for the Enclosure identifier field when not using unicast, specify a value for the Serial number and optional Manufacturer type and model.
    b. When using unicast, specify a value for the Service processor name field or enter an IP address in the SP internet address field.
- When using the defaulted Remote system NWSCFG name and when initializing the service processor is any value other than *NONE, specify the SP authentication values for User name and User password.
25. If prompted, enter remote system configuration information from the "Installation worksheet for the Install Windows Server command" on page 116 in these fields, when using the defaulted `Remote system NWSCFG name`:
- In the Remote system identifier field, specify one of the following:
    a. Use the serial number identified by the Enclosure identifier field of the Service processor NWSCFG.
    b. Specify a value for the Serial number and optional Manufacturer type and model for the Remote system identifier field.
- In the `Delivery method` field, enter the method used to configure the remote system.
- In the `Target CHAP authentication` field, enter the Challenge Handshake Authentication Protocol (CHAP) values used to authenticate the System x or blade initiator.
- In the `Initiator CHAP authentication` field, enter the Challenge Handshake Authentication Protocol (CHAP) values used for the remote system iSCSI initiators to authenticate the System i iSCSI target.
- In the `Boot device ID` field, specify the default value `*SINGLE`.
- When using a *DYNAMIC Delivery method, optionally specify any additional options in the `Dynamic boot options` field.
- In the `Remote interfaces` field, enter values for the interface used in the remote system.
    a. In the `SCSI interface field`, enter values for the SCSI function, including:
        1) The SCSI Adapter address
        2) The SCSI Internet address
        3) The SCSI Subnet mask
        4) **Optional:** Enter the SCSI Gateway address
        5) The iSCSI qualified name or allow the system to automatically generate the address by entering *GEN.
    b. In the LAN interface field, enter values for the LAN function, including:
        1) The LAN (TOE) Adapter address
        2) The LAN Internet address
        3) The LAN Subnet mask
        4) **Optional:** Enter the LAN Gateway address
26. Optional: Configure additional information for your integrated server.
- If you are installing Windows Server 2003, you can install a keyboard type on the integrated server other than the default. (Valid keyboard style identifiers are listed in the TXTSETUP.SIF file in the I386 directory of the Windows server installation source.)

    Note: This parameter is not available for *WIN2008 (Windows Server 2008) installations.
- Use your own IP addresses for the point to point virtual Ethernet.
- Use an NWSD configuration file. See "Network server description configuration files" on page 238.

The integrated Windows server starts to install. The second stage of the installation process is "Continuing the Windows Server 2003 installation from the integrated server console" or "Continuing the Windows Server 2008 installation from the Windows console" on page 128. The process will take approximately 1 hour, depending on your hardware configuration.

Continuing the Windows Server 2003 installation from the integrated server console:

Use the integrated server console to configure the Windows operating system license information, User ID and password, and time zone settings.

When the i5/OS phase of the installation completes, the integrated server starts. The Windows server phase of the installation begins. This phase of the installation is easy if you have completed the steps in "Starting the Windows installation at the i5/OS console" on page 122 and specified the installation attributes on the Install Windows server (INSWNTSVR) command.

To complete installation of Windows server, when not using ServerGuide™, perform these tasks:

1. In the **License Agreement** step (in Windows Server Setup window), click the **I accept this agreement** radio button. Then click **Next**.
2. If you get error messages, click **OK**, and the installation program lets you correct the situation or provide the necessary information. For examples of these error messages and how to respond, see rzahqindpdi.htm.
3. Enter and confirm the password in the **Computer Name and Administrator Password** window.
4. On the **Date/Time Settings** panel:
   a. Confirm that the i5/OS time zone is correct and matches the Time Zone system value given in Windows server installation advisor. See "Configuring time synchronization for integrated servers" on page 109.
   b. Select a setting for Daylight Saving Time.
      - If you are in an area that observes Daylight Savings Time, leave the **Automatically adjust clock** box checked.
      - If you know for sure that you do not observe Daylight Savings Time, clear the "Automatically adjust clock for daylight savings changes" check box.
5. On the Completing the Windows Setup Wizard panel, click **Finish**.
6. On the **Windows Setup** window, click the **Restart Now** button, or wait 15 seconds and the server automatically restarts.

Note: When installing a domain controller Windows server, Active Directory should be installed at this time by running the DCPROMO command. Refer to the Microsoft documentation for more information about the Active Directory installation.

See "Completing the Windows server 2003 installation."

Completing the Windows server 2003 installation:

Verify that the Windows Server 2003 operating system is correctly installed on the iSCSI-attached integrated server.

Perform a few final tasks after installing Windows Server 2003 on the integrated server to verify that it is correctly installed and ready.

1. Install updates to Microsoft Windows and run Windows Update.
   a. Install the latest supported Microsoft service pack. Refer to the Microsoft Service packs page for the latest supported service pack list on the System i integration with BladeCenter and system x Web site .

b. Run Windows Update to install the latest Windows security hot fixes From the Windows server console, run Windows Update or visit (http://windowsupdate.microsoft.com) and install the latest security hot fixes.

c. Install the Microsoft hot fix for the storport.sys driver. In addition to any other Microsoft hot fixes that are available for your server, you should install the Microsoft hot fix for the storport.sys driver. Follow the instructions on the Microsoft Knowledge Base Article 90381 An updated

   Storport storage driver is available for Windows Server 2003 ![icon] to download and install this Microsoft hot fix.

2. If you are running Windows on a System x model 336 or 236 product, see the BladeCenter and

   System x models supported with iSCSI ![icon] Web page for information about a driver that eliminates slot restrictions for the iSCSI HBA.

3. Disable the **NetBIOS over TCP/IP** protocol on the following Ethernet adapters: all QLogic Ethernet adapters, the point-to-point virtual Ethernet adapter and any additional virtual Ethernet adapters configured on the Windows server. If this protocol is enabled on the previously mentioned adapters, intermittent delays and hangs of iSCSI-attached Windows servers might occur. For more information,

   see Software Knowledge Base article 460560441 ![icon] .

4. If you want the integrated Windows server to automatically vary on when you start TCP/IP, see "Starting an integrated server when i5/OS TCP/IP starts" on page 191.

5. If you want the server to have a name that is different than the NWSD name (for example, a name that is longer than 8 characters), you can change the computer name from the Windows console. See the Windows documentation for more information.

6. You can create additional disks for applications and data, rather than storing these items on the system drive. See "Adding disks to integrated servers" on page 230 for more information.

7. You can define additional virtual Ethernet LANs for your server so that it can connect to other servers in the same partition or other partitions. See "Configuring and managing virtual Ethernet and external networks" on page 131 for more information.

8. You might want to enroll some of your i5/OS users to the Windows server or domain. See "Administering integrated Windows server users from i5/OS" on page 138 for more information.

9. You can prevent the optical drive from changing drive letters whenever you link a user storage space to the server. Use **Disk Management** to assign the integrated server optical drive letter. (For example, you could make it drive X.)

10. You can customize your servers by creating your own NWSD configuration file. See "Network server description configuration files" on page 238.

11. If your server is installed with Windows Server 2003 and has Active Directory installed (for example, it is a domain controller), see "Enabling QNTC access to Windows Server 2003 with Active Directory" on page 148.

12. If you want to set up time synchronization for your integrated server, do the following steps:

    a. Configure i5/OS for time synchronization. See "Configuring time synchronization for integrated servers" on page 109.

    b. At the Windows console, click **Control Panel** → **Date/Time**, select the **Time Zone** tab and select your time zone from the drop-down list.

    c. Select the **Automatically adjust clock for daylight savings changes** check-box. Then click OK.

13. Verify that the Microsoft Windows operating system is reporting all of the installed memory. If your system has 4GB or more of memory installed but not all of it is being reported by Windows, see When 4 GB or more of memory is installed, why does Windows report less memory than is actually

    installed? ![icon]

14. Scale the iSCSI network.

The basic installation process addresses iSCSI attached servers that use one target (System i) HBA and up to two initiator System x or blade) iSCSI HBAs. After the server is installed, you can configure additional target or initiator iSCSI HBA ports if needed.

- Configure multipath I/O for the integrated server storage. See "Multipath I/O for iSCSI-attached integrated servers running Windows or VMware ESX Server" on page 21
- Refer to the Scaling your iSCSI network chapter in the Implementing Integrated Windows Server through iSCSI to System i5 (www.redbooks.ibm.com/abstracts/sg247230.html) Redbooks publication for more information.

Continuing the Windows Server 2008 installation from the Windows console:

Do these steps to continue the Windows Server 2008 installation on an iSCSI-attached integrated server.

You should complete the steps in "Starting the Windows installation at the i5/OS console" on page 122 before starting this task.

Follow the prompts from the Windows operating system to complete the installation. Be prepared to:
- Select language, time zone and keyboard settings.
- Enter a product key for activation.
- Select the type of the Windows Server operating system to install. For a list of the supported versions for your BladeCenter or System x model, see the Operating systems tested on iSCSI-attached servers table on the BladeCenter and System x models supported with iSCSI Web page.

  Tip: Both full and core installations are supported.
- Accept Microsoft license terms.
- Select installation type.
- Specify that the Windows Server 2008 operating system will be installed on Disk 0.
  The Windows operating system will automatically format and partition the unallocated space for the system disk.
- If you are installing Windows Server 2008 on a System x platform with a QLogic PCIe initiator iSCSI adapter (PN 39Y6146 or PN 42C1770), complete the following steps:
  1. Select **Custom (Advanced)** when you see this message: `Which type of installation do you want?`
  2. Select **Load driver**.
  3. At the **Load Driver** screen, insert the iSCSI driver media that you created and click **OK**.
  4. Click **Next** to continue with the installation.

The Windows operating system will proceed with the installation and might restart as necessary in order to complete the installation.

Be prepared to change the Administrator user password. After you change the password, the operating system will prompt you to begin the initial configuration tasks.

Completing the Windows Server 2008 installation from the Windows console:

Do these steps to complete the Windows Server 2008 installation on an iSCSI-attached integrated server.

Disable the **NetBIOS over TCP/IP** protocol on the following Ethernet adapters: all QLogic Ethernet adapters, the point-to-point virtual Ethernet adapter and any additional virtual Ethernet adapters configured on the Windows server. If this protocol is enabled on the previously mentioned adapters, intermittent delays and hangs of iSCSI-attached Windows servers might occur. For more information, see

Software Knowledge Base article 460560441 .

Completing the Windows Server 2008 full installation from the Windows console:

If you are performing a full installation, complete these steps.

1. Sign in to the Windows operating system as the Administrator user.
2. Go to the Server Manager.
3. Ensure that the installation drive is available to the integrated server operating system.
   a. Select **Storage** → **Disk Management**.
   b. Locate the partition that has no drive letter. This partition will appear as **Disk 1**.
   c. Right-click this partition and select **Online**. The Windows operating system will assign a letter to the partition.

      Note: The drive letter will depend on how many media devices are available to the server.
   d. Note the letter that is assigned. This drive is the installation drive.
4. Run the **ibmsetup.exe** program to finish configuring the integrated server.

   The ibmsetup.exe program is located in the root directory of the installation drive. For example, if the installation drive is D:, run the command `D:\ibmsetup.exe` at the Windows console.
5. If your integrated server hardware requires additional drivers, install them now. See the Windows or System x or BladeCenter documentation.

Completing the Windows Server 2008 core installation from the Windows console:

If you are performing a core installation, use these commands in the following order to mount the installation drive and to run the ibmsetup.exe program.

1. C:\>diskpart
2. DISKPART> select disk 1
3. DISKPART> online disk
4. DISKPART> attribute disk clear readonly
5. DISKPART> exit
6. C:\>e:
7. E:\>IBMSETUP

Tip: IBMSETUP is typically on the E: drive, but not in all situations.

Configuring and Managing Windows

Learn how to configure the Windows operating system to work in your integrated server environment.

Installing updates to the Integrated Server Support software running on Microsoft Windows

IBM i5/OS Integrated Server Support includes components that run on i5/OS and the Windows operating system.

Use PTFs to update the i5/OS software. Use one of these tasks to copy the updates to the integrated Windows server.

   Related concepts
   "Software updates for integrated servers" on page 51
   There are several types of software updates for iSCSI-attached integrated servers.

Updating the integration software level: integrated Windows server console:

Do these steps to copy updates from the i5/OS operating system to the integrated server.

Before beginning the installation, end any applications that are running and make sure that no users are logged on to the integrated server. If you fail to do this, you risk data loss because the integrated server may require a restart after completing the installation.

1. Click **Start** → **Programs** → **IBM iSeries** → **IBM iSeries Integrated Server Support**.
2. Click the integrated server's name, then **Software Level**.
3. The software level of the i5/OS integration software and of the Windows integration software is shown. Click **Synchronize** to bring the Windows integration software to the same level as the i5/OS integration software.
4. If the installation is performed successfully a confirmation message appears.

Note: If you log on as an administrator to the integrated Windows server console and there is a software level mismatch, you will automatically be asked to synchronize the software.

Updating the integration software: System i Navigator:

Do these steps to update the integrated server support software on the integrated server.

1. In System i Navigator, click **Integrated Server Administration** → **Servers**.
2. Right click the integrated server you want to synchronize and select **Synchronize iSeries Integration Software**. (If the i5/OS server you are accessing is not a V5R3 or later server, you will be presented with a list of earlier options, allowing you to install and uninstall service packs individually, or to perform a release update only.)
3. Click **Synchronize** to confirm the action.
4. You will receive a message indicating the synchronization is in progress followed by a completion message indicating that a reboot is about to take place. You will not be asked whether to reboot now or later.

Determining the software levels for the integration software:

View which levels of software are installed on i5/OS and the integrated server.

1. In System i Navigator, click **Integrated Server Administration** → **Servers**.
2. Right click the integrated server you are interested in and select **Properties**.
3. click the **Software** tab. The software levels will be displayed there.

Updating the integration software: remote command:

You can use the lvlsync command to update the integration software that is installed on the Windows server. This command can be used as part of a program that runs regularly.

Entering the command `lvlsync` at an integrated Windows server console command prompt will cause the integrated server to synchronize. The principle utility of this command-line program is that it allows you to synchronize an integrated server by remotely submitting a command. This functionality would be useful if you, for example, wanted to write a CL program to periodically synchronize your integrated servers. To learn more about remotely submitted commands, see "Guidelines for submitting remote commands to an integrated Windows server" on page 136.

Here is a simple procedure to remotely synchronize an integrated server by remotely submitting the `lvlsync` command from the i5/OS console.

1. At the i5/OS character-based interface, type `SBMNWSCMD` and press **F4**.
2. Enter `lvlsync` in the **Command** field and press **Tab**.
3. Enter the NWSD name of your integrated server in the **Server** field and press enter.

The lvlsync program allowed optional parameters in the past. These parameters no longer function, although their presence in the command will not affect its functionality.

Lvlsync returns the following error codes:

lvlsync error codes

Error Code	Error
0	No errors
01	Must be an administrator to run lvlsync
02	Release level on integrated Windows server higher than on i5/OS
03	Service pack level on integrated server higher than on i5/OS
04	Cannot install release from i5/OS - language files not on i5/OS
05	Syntax not valid
06	Cannot access service pack information on i5/OS
07	Cannot map network drive
08	Cannot access service pack information in registry
09	Cannot open qvnacfg.txt file
10	No service pack installed on i5/OS
11	NWSD not found
13	NWSD not active
20	No service pack available on i5/OS
21	Cannot start InstallShield application
31	Unexpected error while starting lvlsync
44	Unexpected error during lvlsync

Note: The error message NTA0218 is a diagnostic (*DIAG) message for syntax, authorization, and NWSD not found errors.

Managing and configuring networking for integrated Windows servers

Use these tasks to create and manage virtual Ethernet and external networks for iSCSI-attached integrated Windows servers.

Configuring and managing virtual Ethernet and external networks:

Use these tasks to configure and manage the Ethernet networks for integrated Windows servers.

> **Related concepts**
>
> "Virtual Ethernet networks for integrated Windows servers" on page 30
> Integrated servers can use a virtual Ethernet network that is configured on a System i product to communicate with the hosting i5/OS partition, another partition, or other integrated servers.

Configuring IP address, gateway and MTU values for integrated servers:

Learn which console to use and how to configure networking values for integrated Windows servers.

The IP address, gateway, and maximum transmission unit (MTU) values for virtual and physical network adapters in the hosted system are managed from the Windows operating system, except for the following cases.

- The IP address and subnet mask for a new virtual Ethernet line description may optionally be assigned by the i5/OS Install Windows Server (INSWNTSVR) command. After the server is installed these values may only be changed from within the Windows operating system.

- The IP address and subnet mask may be assigned when a virtual Ethernet line is added to an existing server. After the line description is added, these values can only be changed from within the Windows operating system.
- Virtual Ethernet point to point IP address changes should be configured in both the Windows operating system and i5/OS. For more information, go to the Troubleshooting page on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html) and search for `Point to point virtual Ethernet IP address conflicts`.
- The IP address and gateway values for the Windows side of an iSCSI network are always configured and changed from the i5/OS remote system configuration. For more information, see "Changing remote system configuration properties" on page 210.
- The IP address, subnet mask, gateway, and MTU values for IXS external LAN adapters may optionally be set in the i5/OS Install Windows Server (INSWNTSVR) command. After the server is installed these values may only be changed from within the Windows operating system.

  Related concepts

  "Virtual Ethernet networks for integrated Windows servers" on page 30
  Integrated servers can use a virtual Ethernet network that is configured on a System i product to communicate with the hosting i5/OS partition, another partition, or other integrated servers.

Configuring virtual Ethernet networks between integrated Windows servers:

Do these steps to configure a virtual Ethernet network between integrated servers that are configured in the same logical partition.

If you are installing a new integrated server, you can use the Install Windows Server (INSWNTSVR) command to automatically configure virtual Ethernet networks.

1. Configure a virtual Ethernet port and line description for the integrated server.
   a. Expand **Integrated Server Administration** → **Servers**.
   b. Right-click the integrated server and select **Properties**.
   c. On the server properties panel, click the **Virtual Ethernet** tab.
   d. click the **Add...** button to add a new virtual Ethernet port.
   e. On the virtual Ethernet properties panel, specify the values for the new virtual Ethernet port
      1) Select the virtual Ethernet port number.
      2) Type the IP address that the integrated server will use.
      3) Type the subnet mask that the integrated server will use.
      4) You can leave the default line description name or change it to something else. The default line description name is the NWSD name followed by a v followed by the port number. For example, if adding port 3 to an NWSD named *Mynwsd*, then the default line description name is *Mynwsdv3*.
      5) Leave the associated port set to **None**.
      6) Leave the maximum frame size set to the default **8996**.
      7) If the server is an iSCSI attached server, select the network server host adapter corresponding to the iSCSI HBA that you want i5/OS to use for this virtual Ethernet configuration to reach the hosted system.
      8) Click **OK** to add the new port to the **Virtual Ethernet** tab on the server properties panel.
   f. On the server properties panel, click **OK** to save the changes. This will update the NWSD and create a line description for the new virtual Ethernet port.
   g. If you want this integrated server to be connected to more than one virtual Ethernet network, repeat all of the above steps to create a virtual Ethernet port and a line description for each network, using different virtual Ethernet port numbers.
2. Repeat Step 1 for each integrated server that you want to connect to the network. Use the same virtual Ethernet port for each server.

3. Restart the integrated servers. A virtual Ethernet adapter device driver will be automatically installed and set to the Windows TCP/IP address that has been specified for it in the NWSD. However, an IP address entered at the integrated server console overrides the values that are set in the NWSD.

4. Test to see that the virtual Ethernet network is functioning, for example by pinging from one server to the IP addresses you specified for the other servers.

   Related concepts

   "Virtual Ethernet networks for integrated Windows servers" on page 30
   Integrated servers can use a virtual Ethernet network that is configured on a System i product to communicate with the hosting i5/OS partition, another partition, or other integrated servers.

Configuring inter-partition virtual Ethernet networks for integrated servers:

If you want an integrated server to communicate with other logical partitions, or with integrated servers controlled by other i5/OS partitions, you need to configure one or more inter-partition networks.

   Related concepts

   "Virtual Ethernet networks for integrated Windows servers" on page 30
   Integrated servers can use a virtual Ethernet network that is configured on a System i product to communicate with the hosting i5/OS partition, another partition, or other integrated servers.

Configuring inter-partition networks with the Hardware Management Console:

If you want an integrated server to communicate with other logical partitions, or with integrated servers controlled by other i5/OS partitions, you need to configure one or more inter-partition networks. Inter-partition connections exist between partitions or integrated servers using the same VLAN ID. Participating integrated servers do not support VLAN IDs directly. Instead, each participating integrated server needs an Ethernet line description that associates a virtual Ethernet port value with a virtual adapter having a VLAN ID. The configuration procedure consists of the following steps:

1. Use the Hardware Management Console (HMC) to create a virtual Ethernet adapter for each partition and each integrated server that will participate in the inter-partition network. See Partitioning on systems with POWER5 or POWER6 processors and Configuring a virtual Ethernet adapter using version 6 or earlier of the HMC for more information. For each virtual adapter that will connect an integrated server or i5/OS partition to the inter-partition network, specify a consistent Port virtual LAN ID and uncheck **IEEE 802.1Q compatible adapter**.

2. Configure a virtual Ethernet port and line description for the port the server will use if one does not exist. You can use ports 0 through 9. See step 1 of the "Configuring virtual Ethernet networks between integrated Windows servers" on page 132 topic. Select an associated port name (Cmnxx) for the appropriate 268C resource.

3. Continue with step 2 of the "Configuring virtual Ethernet networks between integrated Windows servers" on page 132 topic (in all i5/OS partitions that control a participating integrated server), and step 3 of "Configuring virtual Ethernet networks between integrated Windows servers" on page 132.

4. For a partition to fully participate, you will need to appropriately configure the protocol(s) within the partition. In each i5/OS partition, create an Ethernet line description on the appropriate dedicated 268C port resource. Configure an appropriate unique IP address in each partition that will participate in TCP/IP communications.

5. Test to see if the inter-partition network is functioning. For example, ping between connected integrated servers and partitions.

Managing point to point virtual Ethernet networks for integrated Windows servers:

Each integrated Windows server has a point to point virtual Ethernet network connection with i5/OS, which allows i5/OS to control the integrated server.

These connections are automatically configured during installation. You can view and manage these connections from the i5/OS operating system or the integrated Windows server console.

Viewing point-to-point virtual Ethernet connections from i5/OS:

Point to point Ethernet connections in i5/OS are composed of a line description and an entry in an integrated server's NWSD.

1. To view the line description issue the command WRKCFGSTS *NWS from the i5/OS character-based interface.
2. Find the cascade of entries corresponding to your integrated server. One of the entries in the Line Description column will have the same name as your NWSD and end with the characters PP. Enter 8 to its left and press enter.
3. Now you are in the Work with Line Descriptions menu. Enter a 5 to the left of your line description and press enter to display its information.
4. Press **F3** until you return to the base menu.
5. Now issue the command CFGTCP and select option 1, **Work with TCP/IP interfaces**.
6. One entry in the Line Description column should have the same name as your NWSD and end with the letters PP.
7. Option 5 will display the TCP/IP Interface information, while options 9 and 10 will allow you to enable and disable it. Note the internet address. It will be used later.
8. Now we will take a quick look at the entry in the integrated server's NWSD. Issue the command WRKNWSD. Find your integrated server's NWSD and enter 5 to display it. Press enter to page through the NWSD attributes.
9. One of the screens will be titled **Attached lines** and will display Port number *VRTETHPTP and the name of the line description that the network is using.
10. Back in the **Work with Network Server Descriptions** menu you can use option 2 to change this information.

Viewing point to point virtual Ethernet connections from the integrated Windows server console:
1. At the console of your integrated server, click **Start** → **Settings** → **Control Panel**.
2. Select **Network and Dial-up Connections**.
3. Double-click **virtual Ethernet point to point**. A dialog box will appear.
4. Click **Properties**
5. Double-click **Internet Protocol (TCP/IP)** in the next dialog box.
6. In this final dialog box you should see the IP address associated with the integrated server side of the point to point virtual Ethernet connection. It should be the i5/OS IP address augmented by one so as to be even instead of odd.
7. Close all of the windows that you opened, click **Start** → **Run**, and enter the command cmd. Press enter. This will start an instance of the Windows command prompt.
8. At the C:\> command prompt which appears, enter the command ping followed by the i5/OS IP address that you used in the last step. For example ping 192.168.3.1. The command should return Reply from ..... The ping command sends a packet of data to a certain internet address and times how long it takes to make a round trip.
9. Optional: Return to the i5/OS character-based interface and enter the command call qcmd. (This will increase the display space so that you can see the results of your commands.) Use the i5/OS command to ping the integrated server. For example, enter ping '192.168.3.2'.

Administering integrated Windows Servers

Use these tasks to administer the Windows operating system.

Viewing integrated server messages

View i5/OS message logs for integrated servers.

The **monitor job log** is a key source of information when troubleshooting integrated server problems. It contains messages that vary from normal processing events to detailed error messages. The monitor job always runs in the QSYSWRK subsystem with the same name as the integrated server.

To find the job log in System i Navigator

1. Click **Work Management** → **Active Jobs**.
2. One of the jobs listed under the QSYSWRK section will have the same name as your integrated server. Right-click it and select **Job log**.
3. The integrated server job log window opens. Double-click a message ID to see details.

To find the job log in the character-based interface

1. At an i5/OS command line enter WRKACTJOB SBS(QSYSWRK).
2. One of the jobs listed will have the same name as your integrated server. Select option 5 (Work with job).
3. Type 10 and press Enter to display the job log.
4. Press F10 to see the detailed messages.

There are other relevant job logs that you may want to check as well. The IBM Redbooks publication

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 , includes information about integrated server event logs in i5/OS and at the Windows console.

Running integrated Windows server commands remotely

You can use i5/OS™ to remotely submit integrated server batch commands. Windows server commands that can run in batch mode without user interaction will work.

Before submitting a remote command verify that the following is true:

- The server is an Integrated Windows Server on this i5/OS and is active.
- Your user profile is enrolled to the integrated Windows server or domain, or you sign-on with the QSECOFR profile.
- You have authority to run SBMNWSCMD, which requires *JOBCTL special authority. You must also have at least *USE authority to the QSYS/SBMNWSCMD *CMD object.
- If the user profile *LCLPWDMGT value is *YES, then the system value, QRETSVRSEC, must be set to 1 and the user password must be changed or the user have signed-on after QRETSVRSEC was changed.
- If the user profile *LCLPWDMGT value is *NO, then network authentication (Kerberos) is used. The user must access the System i operation through Kerberos enabled applications (like System i Navigator single sign-on). See "Guidelines for submitting remote commands to an integrated Windows server" on page 136 for more information.
- Thei5/OS user profile password, and Windows password must be equivalent. The easiest way to keep them consistent is to use User and Group enrollment.

To run integrated server commands from System i Navigator

1. In System i Navigator, select **Integrated Server Administration** → **Servers**.
2. Right-click the server on which to run the batch command and select **Run command**.
3. On the **Run Command** panel, type the Windows command to run (such as dir \).

   Tip: You can select the command from a list of 10 commands that you have run previously on the server.
4. Click **Run** to run the command.

Note: A command using the Run Command panel uses *PRIMARY as the authentication domain. For alternative domains use SBMNWSCMD.

To run integrated Windows server commands from the character-based interface

1. Type `CALL QCMD` and press Enter.
2. Type `SBMNWSCMD` and press F4.
3. Type the command you want to run on the remote server. Page down.
4. Enter the NWSD of the server you want to run the command on and press enter.
5. The i5/OS account which you are using should be enrolled to the integrated server in order to be granted authentication to run the remote command. The Authentication domain field allows you to specify where to attempt to authenticate your user ID.
6. The output returned from the command will be displayed on the console. Press F10 to see all messages.

Guidelines for submitting remote commands to an integrated Windows server:

The environment, user, and interface must be configured to send remote commands to an integrated Windows server.

Note: Many of the Submit Network Server Command (SBMNWSCMD) CL command parameters listed in this section are not available when running Windows commands from using System i Navigator. If you need to use a parameter that System i Navigator does not support, then you must use Submit Network Server Command (SBMNWSCMD) directly.

- The requested command is run under the Windows console command "cmd.exe." SBMNWSCMD will not return control to its caller until the command has finished running on Windows and the cmd.exe program terminates.
- The authentication domain field of SBMNWSCMD indicates the Windows domain where your user ID is to be authenticated. The default, *PRIMARY, logs on to the primary domain of the server, if the server is a domain member. *LOCAL logs on to the server itself. The name of a trusted domain may also be specified.
- The QSECOFR user profile is handled differently than all other user profiles. User authentication is not performed on Windows when SBMNWSCMD is run by the QSECOFR profile. The requested Windows command is run under the Windows Local System Account. The Local System Account is used even if the QSECOFR profile is enrolled. The Local System Account does not have a password and lacks network access rights.
- Do not use the "/u" parameter with the Windows "cmd" command.
- SBMNWSCMD has limited support of Kerberos v5 authentication. Kerberos will only be used when the LCLPWDMGT user profile attribute is *NO. See "SBMNWSCMD and file level backup support for Kerberos V5 and EIM" on page 137.
- The Remote Command service and SBMNWSCMD are able to distinguish between ASCII multi-byte and unicode output data and convert them as appropriate.
- You can combine integrated Windows server commands into a single command string by using features of the Windows "cmd.exe" command interpreter. For example, on the SBMNWSCMD command line, you can enter `net statistics workstation && net statistics server` to collect statistics. However, commands that you combine in a single SBMNWSCMD request should not return mixed data (for example, a combination of ASCII and Unicode data), or data in mixed codesets. If the commands return different types of data, SBMNWSCMD may end abnormally with a message which indicates "a problem occurred in the data output conversion." In that case, run the commands separately.
- Do not use characters that are not normally available from the integrated server keyboard. In rare cases, an EBCDIC character in the active jobs coded character set may not have an equivalent in the active code page on Windows. Each different Windows application will give different conversion results.
- The Submit Network Server Command does not completely initialize your logon environment. The user's environment variables are set, but may not be completely equal to those provided by an

interactive logon. Thus, environmental variables that an interactive logon normally sets to user-specific values may not exist or may be set to system default values. Any scripts or applications that rely on user-specific environmental variables may not operate correctly.

- If the home directory for your user ID on the integrated server is mounted on the local server, the Submit Network Server Command sets the current directory to your home directory. Otherwise, it tries to use /home/default or the local system drive.
- If the Load User Profile (LODUSRPRF) keyword is *YES, and if a user profile exists, SBMNWSCMD will attempt to load your Windows profile. You can then use commands that use or alter profile dependencies. However, there is no indication of profile load failures, beyond event log messages that may be produced by Windows. A windows profile can only be active in one Windows Logon session.
- You can use SBMNWSCMD to run integrated server applications as long as they do not require user intervention. The commands run in a background window, not on the integrated server console. If an application requests user intervention, such as popping up a message window, then SBMNWSCMD will hang, waiting for the command to complete - but no intervention is possible. If you end SBMNWSCMD on i5/OS, it will attempt to end the hung Windows command. The background command stops whether GUI or console based.
- You can also run commands that require a **yes** or **no** reply to proceed. You do this by using input pipe syntax to provide the response. For example, `echo y|format f: /fs:ntfs` will let the format proceed after the **Proceed with Format** question raised by the format command. Note that the ″y″ and the pipe symbol ″|″ do not have a space between them. However, not all Windows batch commands support the piping of input (for example, the ″net″ command). Attempts to pass a default response may not be possible.
- You can prevent SBMNWSCMD from logging the command. If the command string contains sensitive data, such as passwords, that you do not want logged in error messages, do the following steps:
  1. Specify `*NOLOGCMD` as the command string.
  2. When the `Command (not logged)` field appears, enter the command to run in this field.

  Note, however, that the *NOLOGCMD option does not affect data that the command returns. If the command returns sensitive data, you can use the command standard output (CMDSTDOUT) parameter to store the output in a secure location, such as an integrated file system file.
- You can direct standard output from the command to your job log (*JOBLOG), to a spool file (*PRINT), or to an integrated file system (IFS) object. Standard error data always goes to the job log.

  When you specify *PRINT, the Work with Spool File (WRKSPLF) display shows SBMNWSCMD in the User Data field for the spooled file. If you select option 8 to display the attributes, the names of the specified integrated server and Windows command appear in the user-defined data field.

  When you specify an integrated file system object, the path name must already exist. If the integrated file system object name does not exist, SBMNWSCMD creates it.
- In the `Convert standard output` field, you can specify (*YES) to convert output from the Windows code set to the coded character set identifier (CCSID) of the i5/OS job.

  New IFS files will be created with the job CCSID. Output directed to an existing IFS object is converted to the IFS object CCSID. Output directed to a new member of an existing file in the `/QSYS.LIB` file system is converted to the existing file CCSID.
- If Convert standard output is (*NO), the Windows standard output will be written to the IFS object, or spool file, with CCSID conversion.

SBMNWSCMD and file level backup support for Kerberos V5 and EIM:

You can use Kerberos V5 for some types of remote commands and backup.

File level backup operations to an integrated Windows server utilize the System i NetClient and Submit Network Server Command (SBMNWSCMD) functions. In i5/OS V5R3 or later, these functions provide limited Kerberos v5 support (also known as System i Network Authentication).

Keep these guidelines in mind if you want to use network authentication with file level backup for your integrated Windows server..

1. In order to enable System i to use Kerberos authentication, you must configure these things on the System i model:
   - System i Navigator Security option
   - Network authentication service
   - Enterprise Identity Mapping (EIM)
   - Network authentication service planning work sheets

2. i5/OS NetServer should be configured to use Password/Kerberos v5 authentication and i5/OS NetServer must be active.

3. The Kerberos KDC must be a Windows Active Directory domain controller (Windows 2000 Server or Windows Server 2003). For more information, see "Enabling QNTC access to Windows Server 2003 with Active Directory" on page 148.

4. Kerberos authentication will only be used when the i5/OS job's user profile has the LCLPWDMGT attribute set to *N0. When LCLPWDMGT is set to *YES, then password authentication will always be used.

5. User Enrollment supports using EIM to map a Windows user name to a different i5/OS profile name. Thus, user enrollment can look for an EIM registry which is named for the Windows Active Directory domain name, or for a EIM registry which is named for the integrated server name as appropriate. User enrollment will use the EIM mapping regardless of whether Kerberos authentication can be used. However, SBMNWSCMD and NetClient will **only** use an EIM mapped name when Kerberos authentication is used. So, user enrollment may create a local windows user with a different name than the i5/OS profile as specified by the EIM mapping. But, SBMNWSCMD and NetClient will only use the different windows name when Kerberos authentication is performed (When LCLPWDMGT = *NO). Otherwise, they attempt to authenticate with a Windows name equal to the i5/OS profile name.

6. For SBMNWSCMD submitted windows commands to be able to connect to other network servers when Kerberos authentication is used, the target windows server must be *trusted for delegation*. In Windows 2000, this is enabled by default for domain controllers. However, it is disabled by default for domain member servers. It may be enabled via the Administration Tool: **Active Directory User and Computers** on a domain controller. Within this tool, click **Computers** and select the correct computer. Then click **Computer properties –> General**. Then check **Trust computer for delegation**.

Administering integrated Windows server users from i5/OS

Use these tasks to manage integrated Windows server users from the i5/OS operating system

One of the main advantages of using integrated Windows server is synchronized, simplified user administration. Existing i5/OS user profiles and groups of profiles can be enrolled to integrated Windows servers, meaning that those users can log onto Windows server with the same user ID and password pair that they use to sign on to i5/OS. If they change their i5/OS password, their Windows password changes as well.

Enrolling a single i5/OS user to an integrated Windows server: System i Navigator

To enroll an i5/OS user to an integrated Windows server, follow these steps.

Create an i5/OS user profile for the user if one does not already exist. You can find information about creating i5/OS user profiles in the Security topic collection.

To enroll a single user to the integrated Windows server, follow these steps:

1. Expand **Integrated Server Administration** → **Servers** or **Integrated Server Administration** → **Domains**.

2. Right-click an available Windows domain or server from the list and select **Enroll Users**.

   Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.

3. Select to enter the user name or choose the user name from the list.

4. Optional: If you want to use a user template as a basis for user settings, specify a Windows user to use as a template when creating the user on Windows. Remember that if you change the user template after you enroll a user, the changes will not affect the user.

5. Click **Enroll**.

If you have problems enrolling users, see Troubleshooting on the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Configuring the QAS400NT user for user enrollment on integrated Windows servers

You need to set up the QAS400NT user in order to successfully enroll an i5/OS user or group profile on a domain or local server in these situations.

- You are enrolling on a domain through a member server.
- You are enrolling on a local server using a template which specifies a home directory path
- You are enrolling on a domain through an i5/OS partition which contains both domain controllers and member servers on the same domain.

You do not need to set up the QAS400NT user in order to successfully enroll an i5/OS user or group profile on a domain or local server in the following cases:

- You are enrolling on a domain through an i5/OS partition which contains a domain controller but no member servers on the same domain.
- You are enrolling on a local server (or locally on a member server) using a template which does not specify a home directory path.

If you need to set up the QAS400NT user, follow these steps:

1. Create the QAS400NT user profile on i5/OS with User class *USER. Take note of the password because you need it in the next step. Make sure that the password complies with the rules for Windows passwords if you are enrolling on a domain.

2. Create the QAS400NT user account on the Windows console of the integrated Windows server you are enrolling through. Note that the i5/OS user profile password and Windows user account password must be the same for the QAS400NT user.

   a. Setting up QAS400NT on a domain controller

      On the domain controller of the domain you are setting up enrollment for, create the QAS400NT user account as follows:

      1) From the integrated server console

         a)
            - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
            - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.

         b) Select **System Tools –> Local Users and Groups**.

      2) Right-click the **Users** folder (or the folder that the user belongs to), and select **New** → **User**...

      3) Enter the following settings:

         ```
         Full name: qas400nt
         User logon name: qas400nt
         ```

      4) Click Next. Enter the following settings:

         ```
         Password: (the same password as you used for QAS400NT on i5/OS)
         Deselect: User must change password at next logon
         Select: User cannot change password
         Select: Password never expires
         ```

      5) Click Next, then Finish

6) Right click the QAS400NT user icon and select Properties.

7) Click the **Member Of** tab and then Add.

8) Enter Domain Admins in the box and click OK, then OK again. This gives the QAS400NT user account sufficient rights to create users.

b. Setting up QAS400NT on a local server

On the local server (or member server if you are enrolling locally) you are setting up enrollment for, create the QAS400NT user account as follows:

1) From the integrated server console
   - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
   - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.

2) Right-click the **Users** folder, and select **New User....**

3) Enter the following settings:

```
User name: qas400nt
Full name: qas400nt
Password: (the same password as you used for QAS400NT on i5/OS)
Deselect: User must change password at next logon
Select: User cannot change password
Select: Password never expires
```

4) Click Create, then Close.

5) Right click the QAS400NT user icon and select Properties.

6) Click the Member Of tab and then Add.

7) Enter Administrators in the box and click OK, then OK again. This gives the QAS400NT user account rights to the User Administration Service.

3. Enroll the i5/OS QAS400NT user profile on the domain or local server using System i Navigator or the CHGNWSUSRA command. Do not try to use a template when enrolling QAS400NT.

4. Use System i Navigator or the WRKNWSENR command to confirm that QAS400NT has been successfully enrolled. You may now enroll i5/OS user profiles through domain controllers or member servers on the domain.

Notes:

- You may change the QAS400NT password from i5/OS since it is now an enrolled user.

- If there are multiple integrated servers that belong to different domains on a single i5/OS partition, you must set up QAS400NT for each domain. All QAS400NT user accounts must have the same password as the i5/OS user profile. Alternatively, consider using Active Directory or trust relationships between domains, and enroll users on only a single domain.

- If you have multiple i5/OS partitions and multiple integrated servers, QAS400NT passwords on different i5/OS partitions can be different as long as each domain does not contain integrated servers on more than one i5/OS partition. The rule is, all i5/OS QAS400NT user profiles and corresponding Windows user accounts must have the same password for a single domain.

- Be sure not to delete the QAS400NT user profile on i5/OS, or let the password expire. To minimize the risk of the QAS400NT password expiring on one of multiple i5/OS partitions on the same Windows domain, it is recommended that you allow only one i5/OS partition to propagate changes to the QAS400NT user profile.

- If you have multiple i5/OS partitions, each with an integrated Windows server on the same domain, failing to keep the QAS400NT password synchronized across all i5/OS partitions can cause enrollment problems. To minimize this problem, it is recommended that you limit propagation of changes to the QAS400NT password to just one i5/OS partition, but still allow other partitions to keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only.

Enrolling i5/OS groups to integrated Windows servers: System i Navigator

To enroll i5/OS groups to integrated Windows servers, follow these steps.

You can find information about creating i5/OS user and group profiles in the Security topic collection.

To enroll an i5/OS group and its members to the integrated Windows server, follow these steps:

1. Expand **Integrated Server Administration** → **Servers or Domains**.
2. Right-click an available Windows domain or server from the list and select **Enroll Groups**.

   Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.
3. Enter a group name or select an unenrolled group from the list.
4. Optional: To use a template to create new users, specify a Windows user to use as a template when creating users in the group on Windows. If you change the user template after you enroll a user, the changes do not affect the user.
5. Select **Global** if the group is being enrolled in a domain and the group should be visible to the domain. Otherwise, select **Local** . Windows server local groups can contain users and Windows server global groups, while Windows server global groups can contain only users. See the Windows online help for more information about group types.
6. Click **Enroll**.

If you have problems enrolling groups, see Troubleshooting on the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Enrolling i5/OS users to an integrated Windows server using the character-based interface

Use the Change Network Server User Attributes (CHGNWSUSRA) command to enroll an i5/OS user to an integrated Windows server.

1. At the i5/OS character-based interface, type CHGNWSUSRA and press **F4**.
2. In the **User profile** field, type the name of the i5/OS user profile you want to enroll to the Windows environment.
3. Press **enter** twice. More fields should appear.
4. **Page down** and enter those Windows domains and Windows local servers you want to enroll the user to.
5. Press **enter** to accept the changes.

Table 17. CL commands for user enrollment

WRKUSRPRF	Work with i5/OS user profiles.
WRKNWSENR	Work with i5/OS user profiles enrolled to the Windows environment.
CHGNSWUSRA	Enroll i5/OS users to the Windows environment.

Creating user enrollment templates for integrated Windows servers

Follow these steps to create user enrollment templates.

A user enrollment template is a tool to help you enroll users from i5/OS to the Windows environment more efficiently. You do not have to manually configure many new users with identical settings.

You can make a user template a member of any Windows server group, whether you enrolled that group from i5/OS or not. You can enroll users with a template that is a member of a group that was not enrolled from i5/OS. If you do this you can only remove users from the group by using the User Manager program on Windows server.

If you are creating a template that will be used to enroll administrators, you may want to make the template a member of the Windows server group *Administrators*. Likewise, if you want to protect Windows users from accidental deletion from i5/OS, enroll the template in the *AS400_Permanent_Users* (or OS400_Permanent_Users) group.

Follow these steps to create a Windows template.

Related concepts

"User enrollment templates for integrated Windows servers" on page 49
You can use templates to simplify the enrollment of new users to integrated Windows server.

Creating user profiles for a Windows 2000 Server or Windows Server 2003 domain:

Do these steps at the integrated server console.

1. Click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Click the domain name.
3. Right-click **Users**, then select **New** → **User**.
4. In the **Username** and **Logon name** fields, enter a distinctive name for the template, such as *stduser* or *admtemp*. Click **Next**.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **User cannot change password**, **Password never expires**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access the integrated server.
6. Do not enter a password for a template account.
7. Click **Finish**.
8. To set up group memberships, double-click the template name in the list of domain users and groups that appear in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

Creating user profiles on Windows 2000 Server or Windows Server 2003 server:

Do these steps at the integrated server console.

1. Open the Local Users and Groups window.
   - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
   - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
2. Select **System Tools** → **Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. In the **User name** field, enter a distinctive name for the template, such as *stduser* or *admtemp*.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **Password never expires**, **User cannot change password**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access Windows server.
6. Click **Create**, then **Close**.
7. Click **Users** or refresh to show the new user template.
8. To set up group memberships, double-click the template name in the list of domain users and groups that appears in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

Specifying a home directory in a user template

Follow these steps to specify a home director in a user template.

To allow integrated Windows servers to manage users in the most portable way possible, a home directory can be set up for each user to store user-specific information generated by applications. To minimize the amount of work that must be done, specify home directories in the template accounts so that each new profile created by the enrollment process has a home directory created for it automatically. To provide scalability, it is important not to lock home directories to a particular disk drive. Use the Universal Naming Convention (UNC) names to give portability.

To customize your template profiles to include a home directory, follow these steps from the integrated Windows server console:

1. Create the home directory folder on the appropriate server, and share it.
2. In a domain, click **Start** → **Programs** → **Administrative Tools** → **Active** → **Directory Users and Computers** from the Windows console. On a local server, click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
3. Double-click the template (model user) to display its properties.
4. Click the Profile tab.
5. In the Home folder segment, click **Connect**. Select a drive letter (such as Z:). Move to the **To:** dialog, and enter the directory path of the home directory using a UNC name, for example: \\systemiWin\homedirs\%username%. In this example, **systemiWin** is the name of the server where the home directory folder resides, and **homedirs** is the name of the home directory folder. If you use the variable *%username%*, instead of the logon or user name, Windows server automatically substitutes the user's name in place of the variable name when each new Windows server account is created. It also creates a home directory for the user.

Changing the LCLPWDMGT user profile attribute

Use these steps to change the Local Password Management (LCLPWDMGT) user profile attribute.

1. Type CHGUSRPRF and the user profile name you want to change.
2. Press F4 to prompt.
3. Press **F9** to view all attributes and **F11** to view their abbreviations.
4. Find the attribute LCLPWDMGT and set it to *YES or *NO.
5. Press enter.

Configuring Enterprise Identity Mapping for integrated Windows servers

Use this information to configure a user account to use EIM.

What is EIM?

Enterprise Identity Mapping (EIM) is a way to consolidate a user's various UserIDs and passwords together under a single account. Using it, a user can log on just once to a system, and then EIM will work together with other services behind the scenes to authenticate the user to all of his accounts.

This is called a single sign-on environment. Authentication still takes place whenever users attempt to access a new system; however, they will not be prompted for passwords. EIM reduces the need for users to keep track of and manage multiple user names and passwords to access other systems in the network. Once a user is authenticated to the network, the user can access services and applications across the enterprise without the need for multiple passwords to these different systems.

The EIMASSOC user profile attribute

EIMASSOC is a user profile attribute specifically designed to aid in configuring EIM. At the i5/OS command prompt type CHGUSRPRF and the user profile name and then press F4 to prompt. Then page down to the very bottom and you will see a section labled EIM association. Here is a summary of what the fields mean:

- **Element 1: EIM identifier** This is the UserID that EIM uses to identify you. Think of it as your Master ID under which all your other user IDs will be stored. If you specify *USRPRF the system will use your i5/OS user profile name as the EIM identifier. Alternatively, you can specify any valid character-string. If you enter *DLT in this field and press enter, you will be presented with a list of changed options for deleting EIM associations.
- **Element 2: Association type** This value specifies how the i5/OS user profile that you are editing will be associated with the EIM identifier. The values of *TARGET, *TGTSRC, or *ALL will allow auto-creation or deletion of i5/OS target and Windows source associations.
- **Element 3: Association action** The special values are:
  - *REPLACE The Windows source associations will be removed from all EIM identifiers that have an association for this user profile. For the enrolled user, a new Windows source association will be added to the specified EIM identifier.
  - *ADD For the enrolled user, a Windows source association will be added.
  - *REMOVE The Windows source association will be removed.
- **Element 4: Create EIM identifier** This value specifies whether the EIM identifier should be created if it does not already exist. The special values allowed are, *NOCRTEIMID, an EIM identifier will not be created, or, *CRTEIMID, an EIM identifier will be created if it does not exist.

Automatic and Manual EIM associations

In a typical EIM configured environment, which uses single sign-on, i5/OS target associations and Windows source associations are typically defined. With integrated Windows server user administration, the system administrator may decide to define enrolled Windows users to have EIM associations automatically defined. For instance, if an enrolled Windows user has EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) specified, i5/OS will automatically create an i5/OS target and a Windows source association. The EIMASSOC information is not stored in the user profile. Also, this information is not saved or restored with the user profile. And, if the i5/OS system is not configured for EIM, then no association processing is done and the EIMASSOC information is ignored.

If i5/OS is configured to use EIM and EIMASSOC processing is defined for the enrolled user, integrated Windows server user administration will auto create or delete Windows source associations for the user in the Windows EIM registry. For a user enrolled locally to the Windows environment, the Windows EIM registry name is the fully qualified, local Domain Name System (DNS) name. The Windows EIM registry type is defined to be Windows 2000. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be Kerberos - case ignore. If EIMASSOC is defined for a user, and i5/OS is configured to use EIM, and the Windows EIM registry doesn't exist, integrated Windows server user administration will create the Windows EIM registry.

Use EIM associations to allow different Windows user profile names

EIM provides a mechanism to associate user profiles in a directory system. EIM allows for an EIM identifier to have an i5/OS user profile target association defined and a Windows user profile source association to be defined. It is possible for a user administrator to define a Windows source association using a different Windows user profile name than the i5/OS target association user profile name. Integrated Windows user administration will use the defined EIM Windows source association Windows user profile, if it exists, for Windows user enrollment. The i5/OS target association needs to be defined. Using the EIM identifier, the Windows source association needs to be defined by the administrator. The Windows source association needs to be defined for the same EIM identifier in the correct Windows EIM registry name and type. For a user enrolled locally to Windows, the Windows EIM registry name is the fully qualified, local domain name server (DNS) name. The Windows EIM registry type is defined to be EIM_REGTYPE_WIN2K. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be EIM_REGTYPE_KERBEROS_IG.

Ending user enrollment to an integrated Windows server

To end the enrollment of a user to Windows domains and servers, do these steps at the Windows console.

To end the enrollment of a user to Windows domains and servers, follow these steps on the integrated Windows server console:

1. Expand **Integrated Server Administration —> Servers or Domains**.
2. Expand the domain or server that contains the user that you want to unenroll.
3. Select **Enrolled Users**.
4. Right-click the user that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** on the confirmation window.

Effects of ending user enrollment to the integrated Windows server

When you end user enrollment from the Windows environment, you also remove the user from the list of enrolled Windows server users, as well as from the Windows server group AS400_Users (or OS400_Users). Unless the user is a member of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users), you also delete the user from the Windows environment.

You cannot delete users who are members of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users) from Windows server by either ending enrollment or deleting them from i5/OS. However, ending enrollment does remove the user from the list of enrolled Windows server users and from the Windows server group AS400_Users (OS400_Users).

You can keep users on the Windows environment after you have ended their enrollment on i5/OS. This practice is not recommended, since it makes it possible to add these users to groups on i5/OS and change passwords on i5/OS without these updates ever appearing in the Windows environment. These discrepancies can make it difficult to keep track of users on either system.

You can end user enrollment in a number of ways. Actions that end user enrollment include the following:
* Intentionally ending enrollment for the user.
* Deleting the i5/OS user profile.
* Ending enrollment for all i5/OS groups to which the user belongs.
* Removing the user from an enrolled i5/OS group when the user does not belong to any other enrolled groups.

Ending group enrollment to an integrated Windows server

To end the enrollment of a group to Windows environment domains and servers, follow these steps.

When you end enrollment of a group to the integrated Windows server, all users whose enrollment is limited to that group also have their enrollment ended. If the group has only members that were enrolled through it, the group is deleted from the integrated Windows server.

However, if the group has any members that were added from the Windows operating system rather than enrolled from i5/OS, the group is not deleted. The only members that the group can still have are nonenrolled users.

To end the enrollment of a group to Windows domains and servers, follow these steps in System i Navigator:

1. Expand **Integrated Server Administration › Servers or Domains**.
2. Expand the domain or server that contains the group that you want to unenroll.
3. Select **Enrolled Groups**.

4. Right-click the group that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** in the confirmation window.

Preventing enrollment and propagation to an integrated Windows server

Use these tasks to prevent users from being enrolled or propagated to an integrated Windows server.

There are several reasons why you might want to prevent i5/OS user profile propagation to a particular integrated server:

- If there are multiple integrated servers that belong to the same domain, and they are all on the same i5/OS partition, user profile enrollment will, by default, go through all of the integrated servers in that partition. To reduce network traffic you can turn off enrollment to all integrated servers on the domain except one. This single integrated server would normally be the domain controller, if it is in the partition.
- If there are multiple integrated servers that belong to the same domain, but they are all on different i5/OS partitions, there is a risk of the QAS400NT passwords getting out of synchronization and causing problems with user profile enrollment. By preventing propagation of the QAS400NT user profiles from all i5/OS partitions except one, you can reduce the risk of enrollment problems. Notice that the other i5/OS partitions keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only.

There are two methods to prevent i5/OS user profile propagation to a particular integrated server:

- Use the Propagate Domain User (PRPDMNUSR) parameter. See below for a description of how to do this.
- Create data areas with the Create data area (CRTDTAARA) command. See below for a description of how to do this.

Notes:

- Do not turn enrollment off for all of the integrated servers on the domain. Otherwise all your users may go to update pending (*UPDPND) status, and no further propagation takes place.
- You may want to leave two integrated servers enabled for user enrollment so that you can still make changes if one of the servers is down.

Using the PRPDMNUSR parameter to prevent enrollment to a domain through a specific integrated server:

The Propagate domain user (PRPDMNUSR) parameter of the Change network server description (CHGNWSD) command can be used to prevent user enrollment to a domain through a specific integrated server.

You can also set this parameter when installing an integrated server using the Install Windows Server (INSWNTSVR) command. This option may be useful in the case where there is a single i5/OS partition which controls multiple integrated Windows servers that belong to the same domain, because it can turn off enrollment for all integrated servers except one.

To use the PRPDMNUSR parameter to prevent user enrollment, do these steps.

1. Using the Work with Network Server Description (WRKNWSD) command, select the integrated server you wish to stop enrollment on. (You do not need to vary off the server.)
2. Enter the command: `CHGNWSD NWSD(nwsdname) PRPDMNUSR(*NO)`

Using the CRTDTAARA command to prevent enrollment of QAS400NT to a specific integrated server:

The Create Data Area (CRTDTAARA) command can be used to prevent enrollment of the QAS400NT user profile only, for the specified integrated server. The propagation of other user profiles is not affected.

This option may be useful in the case where there are multiple integrated servers that belong to the same domain, but they are all on different i5/OS partitions. You want to enroll user profiles from these different i5/OS partitions, but not have multiple QAS400NT user profiles propagating passwords to the domain. Follow these steps:

1. Choose one i5/OS partition that you wish to use for enrollment of QAS400NT on the domain. Ensure that QAS400NT is enrolled on this i5/OS partition.
2. If QAS400NT is enrolled on other i5/OS partitions follow these steps:
   a. On the domain controller, add the QAS400NT user account to the OS400_Permanent_Users group to ensure that it is not deleted.
   b. On the i5/OS partitions where you want to prevent enrollment of QAS400NT, delete the QAS400NT user profile.
3. On the i5/OS partitions where you want to prevent enrollment of QAS400NT, create a data area with this command: CRTDTAARA DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE(*NOPROP) where **nwsdname** is the name of the network server description for the integrated server, and ***NOPROP** is the keyword that signals that QAS400NT user profile parameters (including the password) are not propagated from this i5/OS partition.
4. Create and enroll the QAS400NT user profile on each of the i5/OS partitions you created the data area on. Notice that you still need to keep the QAS400NT password current (not expired) on all these i5/OS partitions for enrollment of user profiles (other than QAS400NT) to occur. Because the QAS400NT password is not propagated, it does not matter what the password is, as long as it is not expired.

Backing up and recovering integrated Windows servers

You can back up your server from the integrated Windows server console or i5/OS. Learn about the methods available to you.

You can use either i5/OS or Windows server utilities or a combination of both to manage backups. When you are planning your backup strategy, refer to the Backup and recovery topic, as well as Microsoft documentation.

To back up an integrated server on i5/OS, you have these basic options:
* Do a full system backup on your i5/OS. See the topic Backing up your system.
* Back up the network server description (NWSD) and the disk drives that are associated with the integrated server on i5/OS. See "Backing up the NWSD and other objects associated with integrated servers" on page 194.
* Back up individual integrated server files by using the i5/OS SAV and RST commands and i5/OS NetServer or a backup utility. See "Backing up individual integrated Windows server files and directories" on page 148.

Your recovery options depend on how you backed up your system, as well as what you need to recover.
* If you need to recover your entire system, see the Backup and recovery topic collection.
* If you need to restore a network server description and its associated i5/OS disk drives, refer to "Restoring integrated server NWSDs" on page 201.
* To restore integrated server data (files, directories, shares, and the Windows registry) that you backed up with the Save (SAV) command, see "Restoring integrated Windows server files" on page 153.
* If you used a program such as the Windows backup utility or tar to save your file, use that program to restore the files.

Enabling QNTC access to Windows Server 2003 with Active Directory

i5/OS uses the QNTC file system to access your integrated server disks for administrative functions such as user administration and updating the integration code. You must enable Kerberos to allow authentication to Windows Active Domain servers.

QNTC, SBMNWSCMD, and File Level Backup can use Kerberos to authenticate to Windows Active Domain member servers.

You may need to install an update Windows Server 2003 on your Microsoft Active Directory controller servers in order to use Kerberos. This update is available in Service Pack 1 or Microsoft hot fix KB833708. For additional information, including information about installing the service pack or the hot fix, search for "KB833708" or "Windows Server 2003 service pack" on the Microsoft Web site .

After you install the hot fix or service pack 1, you must also update the Windows Server 2003 registry. Do the following steps:

 1. Click **Start**>**Run**
 2. Type regedit in the **Open** box.
 3. Click **OK**.
 4. Select the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc** registry subkey.
 5. Right-click **Kdc**.
 6. Select **New** .
 7. Click **DWORD Value**.
 8. Enter KdcUseRequestedEtypesForTickets as the New Value.
 9. Right-click **KdcUseRequestedEtypesForTickets**.
 10. Select **Modify**.
 11. Set the **KdcUseRequestedEtypesForTickets** registry value to 1.
 12. Click **OK**.
 13. Quit Registry Editor.
 14. To activate the change, restart the Key Distribution Center service or reboot the server.

  Related information

   i5/OS NetClient file system (QNTC)

Backing up individual integrated Windows server files and directories

The Integrated Server Support option allows you to save integrated server data (files, directories, shares, and the Windows registry) to tape, optical or disk (*SAVF) along with other i5/OS™ data and restore the data on an individual basis.

IBM i5/OS Integrated Server Support allows you to save integrated server data (files, directories, shares, and the Windows registry) to tape, optical or disk (*SAVF) along with other i5/OS data and restore the data on an individual basis. However, you should not use this approach as your primary backup procedure. You should still periodically save your entire system and the NWSD associated with your Windows server for disaster recovery. Then you can choose to do daily backups of only the integrated server files that have changed. See "Backing up the NWSD and other objects associated with integrated servers" on page 194.

You can also use a utility such as the Backup program that comes with Windows (see "Using the Windows Backup utility with integrated servers" on page 154). For more information about options for backup and recovery of your integrated Windows server files, see Backup for Windows servers on the System i integration with BladeCenter and System x Web site.

  Related information

➡ Backing up your system

File-level backup restrictions for integrated Windows servers:

File-level backup for integrated Windows servers has some limitations and requirements for the environment.

Limitations

- This support is not available to stand-alone Windows servers because the code comes packaged with IBM i5/OS Integrated Server Support.
- This method does not back up files that are part of the IBM i5/OS Integrated Server Support code.
- You cannot stop users from signing on and accessing data on the server while the Save (SAV) or Restore (RST) command is running. IBM i5/OS Integrated Server Support can save a file that is in use as long as it can read the file. Consequently, you should back up integrated server files when you expect few users to be accessing the system. A note telling users to avoid accessing the server would be a good precaution.
- Windows Server 2003 provides function with its Volume Shadow copy Service (VSS). This allows applications that are backup aware the ability to save files while they are still in use when using file-level backup
- The QSECOFR user profile should not be used to perform a file-level backup. Even if enrolled to the integrated server, QSECOFR will not be used to back up the files. The Windows Local System Account will be used instead. It may not have the necessary authority to back up all of the requested files.
- If the user profile *LCLPWDMGT value is *YES, then the system value, QRETSVRSEC, must be set to 1 and the user password must be changed or the user have signed-on after QRETSVRSEC was changed.
- If the user profile *LCLPWDMGT value is *NO, then network authentication (kerberos) is used. The user must access the i5/OS operation through an EIM enabled application (like System i Navigator single-signon). See "SBMNWSCMD and file level backup support for Kerberos V5 and EIM" on page 137 for more information.

Requirements

- The integrated server must be active and have a working TCP/IP point to point virtual Ethernet connection with the i5/OS operating system. You must back up your integrated server files either before putting the system into restricted state to back up the rest of the i5/OS files or after completing restricted state operations.
- This procedure requires that you have the same user ID and password on the integrated server and the i5/OS operating system.
- Your integrated server user account must be a member of the Administrators group.
- File-level backup uses the QNTC file system (NetClient) to build the list of files to be saved. QNTC uses i5/OS NetServer to locate servers in the domain. You need to have the i5/OS NetServer in the same domain (see "Verifying that i5/OS NetServer and the integrated Windows server are in same domain" on page 152) as the integrated server from which you are going to save files.
- Be careful about trying to restore all files on all drives that you previously saved through the QNTC file system. Certain Windows system files (for example, files in the Recycle Bin) can cause unexpected results after you restore them.
- On Windows 2000 Server or Windows Server 2003, you need to give special consideration to System File Protection when you are backing up and recovering Windows system files. Refer to Microsoft documentation.

Installing and configuring i5/OS NetServer:

i5/OS NetServer is used for file-level back up and some administration tasks. Use these steps to install i5/OS NetServer.

To install updates to the i5/OS integrated server support software on the Windows operating system, you must be signed on with a Windows account that corresponds to an i5/OS user profile with the same password, or you must have a guest i5/OS NetServer user profile configured.

If you plan to use i5/OS NetServer only to perform maintenance tasks, you can set it up without System i Navigator. In that case, you can use the quickstart method found in the Getting started with i5/OS NetServer topic. If you want the full capabilities of i5/OS NetServer, you need System i Navigator, which requires setting up System i Access (see "System i Access and integrated servers" on page 50) on a PC that you use for administration.

Once you have set up i5/OS NetServer, you need to set up a Windows user with access to i5/OS NetServer or you can set up an i5/OS NetServer guest user profile.

Creating a Windows user with authorities to access i5/OS NetServer:

Before you can apply code fixes and system upgrades to the Integrated Server Support software that runs on the integrated Windows server, you must be signed on with a Windows account that has the authorities that are required to access i5/OS NetServer.

The Integrated Server Support code that runs on the Windows server is stored in the i5/OS Integrated File System (IFS) and is downloaded to the Windows server with i5/OS NetServer.

You can use one of the following methods to use this account.
- Sign onto Windows with an account that has a corresponding i5/OS user profile with the same password. This Windows account must also be a member of **Windows Administrators** group. You can enroll the user to Windows after the server has been installed. See "Enrolling a single i5/OS user to an integrated Windows server: System i Navigator" on page 138.
- If you prefer not to create a user profile, you can also use a guest user profile that is configured for i5/OS NetServer.

You must have *SECADM special authority to perform this task.

If you have System i Navigator on your system, you can use the graphical interface to set up a guest user profile for i5/OS NetServer with no special authorities and no password.

If you do not have System i Navigator, follow these steps to set up a guest user profile for i5/OS NetServer:
1. On i5/OS, create a user profile with no special authorities and no password:

    CRTUSRPRF USRPRF(*username*) PASSWORD(*NONE) SPCAUT(*NONE)

    Note: See the Security topic collection for information about user profiles.
2. Enter the following command, where *username* is the name of the user profile that you created:

    CALL QZLSCHSG PARM(*username* X'00000000')
3. To stop i5/OS NetServer, enter the following command:

    ENDTCPSVR SERVER(*NETSVR)
4. To restart i5/OS NetServer, enter the following command:

    STRTCPSVR SERVER(*NETSVR)

Configuring integrated Windows servers for file-level backup:

Do these steps to configure file-level backup for integrated servers.
1. Ensure that the person who is saving and restoring files has the same password on i5/OS and the integrated server. The easiest method is found at "Enrolling a single i5/OS user to an integrated

Windows server: System i Navigator" on page 138. Also ensure that the user is a member of the Administrators group. Refer to "Creating user enrollment templates for integrated Windows servers" on page 141.

2. Create shares for each drive or volume that you want to save when you request to save all the files on a Windows server. IBM i5/OS Integrated Server Support accesses the file system and translates these shares into path-names. See "Creating shares on integrated Windows servers."

3. Add members to the QAZLCSAVL file in QUSRSYS that lists the share names that you want to be able to save. See "Adding members to the QAZLCSAVL file."

4. Ensure that i5/OS NetServer is in the same domain as the integrated server for which you want to save files. See "Verifying that i5/OS NetServer and the integrated Windows server are in same domain" on page 152.

5. Ensure that the person performing the saves or restores has *ALLOBJ authority which gives the user full access to the programs and devices required for the save or restore process. If *ALLOBJ authority cannot be provided, the user must have at least *USE authority on object QNTAP/QVNASBM so the backup or restore request can be communicated to the integrated Windows server.

Creating shares on integrated Windows servers:

Create a file share for each file or directory that you want to save at the integrated server console. i5/OS will use this share to back up the Windows files.

To create shares on integrated Windows servers, do this from the integrated server console:

1. Open the **My Computer** icon to open **Windows Explorer**.
2. Right-click the drive or volume that you want.
3. From the pop-up menu, select **Sharing**.
4. Click **Share this folder**. Provide a **Share Name** (characters in the share name must be in the more restrictive code page 500 character set). The default share name is the same as the last part of the directory name. Share names can be no longer than 12 characters and can include embedded blanks.
5. You can choose unlimited access or limit the number of users who can access the share at one time. You can also use the **Permissions** button to set up the level at which you want to share (No Access, Read, Change, or Full Control).
6. Click on **Apply** to create the share.

Adding members to the QAZLCSAVL file:

To enable file-level backup and recovery from i5/OS, add a member for each integrated server to the QAZLCSAVL file in QUSRSYS.

For the member name, use the NWSD name of the server (*nwsdname*).

To add a member, do this:

1. On the i5/OS command line, use the Add Physical File Member (ADDPFM) command to add a file member. Type
   ```
   ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nwsdname)
    TEXT('description')  EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE).
   ```
2. In the file member that you just created, list all the shares that you want to be able to save. List each share name that you defined for the server on a separate line. The maximum length that the Windows share name can be is 12 characters. Share names can have embedded blanks. For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as shares on WINSVR1, your member name WINSVR1 would look like this:
   ```
   QUSRSYS/QAZLCSAVL
   WINSVR1
   0001.00  cshare
   ```

```
0002.00  dshare
0003.00  eshare
0004.00  fshare
0005.00  gshare
0006.00  my share
```

> **Note:** If you specify multiple share names that point to the same integrated server directory, i5/OS saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not include multiple shares that include the same directory or data.

Verifying that i5/OS NetServer and the integrated Windows server are in same domain:

To save integrated server files for file-level backup, i5/OS NetServer must be configured \in the same domain as the files you want to save.

1. Check the domain for your integrated server:
   a. In System i Navigator, select **Integrated Server Administration** → **Servers**.
   b. Find your integrated server in the list in the right pane; then look in the Domain column to find the domain for that server.
2. Check the domain for i5/OS NetServer:
   a. In System i Navigator, select **Network** → **Servers** → **TCP/IP**.
   b. Find i5/OS NetServer in the list of TCP/IP servers.
   c. Right-click i5/OS NetServer, and pick **Properties** (or double-click **i5/OS NetServer**, then select **File**, then **Properties**). The domain name for i5/OS NetServer appears under the **General** information file tab.
3. If i5/OS NetServer is not in the same domain as the integrated server, change the domain for i5/OS NetServer:
   a. Click the **Next Start** button.
   b. In the **Domain name** field, type the name of the Windows server domain.
   c. Stop and start i5/OS NetServer (right-click **i5/OS NetServer** and pick **Stop**, then **Start**.)

Saving integrated server files:

Use the Save (SAV) CL command to save your files.

After you finish the necessary preliminaries (see "Configuring integrated Windows servers for file-level backup" on page 150), you are ready to back up integrated server files on i5/OS. To be able to restore a directory or file by share name, you must specify that file or share name specifically on the SAV command.

Note: To avoid duplicating data, be careful specifying what you want to save on the SAV command. If you specify multiple share names that point to the same directory on the integrated server, i5/OS saves the data multiple times.

To specify what you want i5/OS to save, do this:

1. Ensure that the integrated server is active (described in "Starting and stopping integrated servers" on page 190). Also ensure that the QSYSWRK subsystem, QSERVER, and TCP/IP are active (you can do this by using the Work with Active Jobs (WRKACTJOB) command).
2. On the i5/OS command line, type SAV and press F4.
3. In the Device field, specify the device on which you want i5/OS to save the data. For example, 'QSYS.LIB/TAP01.DEVD' saves the data to tape.
4. In the Object field, specify what you want i5/OS to save in the form '/QNTC/*servername*/sharename' You can use wildcard characters. Refer to "Examples: Saving parts of integrated servers" on page 153 for how to specify particular parts of the integrated server.

5. Use the `Directory subtree` field to specify whether you want to save subtrees under a directory. The default is to save all directories.
6. To specify that you want to save changes since the last save, specify *LASTSAVE in the `Change period` field. You can also specify a specific range of dates and times.
7. Press Enter to save the shares that you specified.

Examples: Saving parts of integrated servers:

These examples show how to use the save (SAV) or restore (RST) commands for specific parts of an integrated server.

Here are examples for server *server1*, where *server1* is the name of the integrated server.

To save or restore this:	Specify this:
All integrated server objects.	OBJ('/QNTC/*') SUBTREE(*ALL)
All objects for *server1*.	OBJ('/QNTC/server1/*') SUBTREE(*ALL)
All objects for *server1* that changed since you last saved the files.	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
All objects for *server1* that changed during a certain period (in this case between 10/19/99 and 10/25/99).	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
All directories, files, and shares to which a particular share (for example, 'fshare') refers. i5/OS does not save and restore the directory over which the share is built.	OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)
Only files to which the specified share (for example, 'fshare') refers that match the specified pattern (pay*). i5/OS does not save directories nor shares.	OBJ('/QNTC/server1/fshare/pay*')
Only directories and shares (no objects) for 'fshare' and its immediate children.	OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)
Directories, shares, and files for 'terry' and its subtrees (not directory 'terry').	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
Only the specific file 'myfile.exe'.	OBJ('/QNTC/server1/gdrive/myfile.exe')
The registry for an integrated Windows server	OBJ('/QNTC/server1/$REGISTRY')

Restoring integrated Windows server files:

Use the Restore (RST) command to restore individual files for your integrated server.

IBM i5/OS Integrated Server Support supports file-level backup and recovery of your files. You can recover a particular file from your i5/OS backup without restoring the entire disk drive. Before using this method, however, consider the amount of data you need to restore. For large amounts of data, restoring an entire disk drive object is much faster than restoring all the individual files in the disk drive. To restore a smaller amount of data, this method works great.

You should restore the directory first, then files, then the registry, then reboot for new registry entries to take effect. To restore files that you saved by this method, use the RST command:
1. Ensure that the integrated Windows server and TCP/IP are running.

2. On the i5/OS command line, type RST and press F4.
3. In the `Device` field, specify the device on which the data is available. (For example, `'QSYS.LIB/TAP01.DEVD'` restores the data from tape.)
4. In the `Object` field, specify what you want i5/OS to restore in the form '/QNTC/*servername*/ sharename'

   You can use wildcard characters. Refer to "Examples: Saving parts of integrated servers" on page 153 for how to specify particular parts of an integrated Windows server. Avoid restoring Windows system files by this method because the restored files may behave unpredictably.
5. In the `Name` field, specify the path name of the object to restore.
6. You can use the `Include or omit` field to include or omit objects with the pattern that you specify in the `Name` portion of the `Object` parameter.
7. In the `New object name` field, leave the object name the same or specify a new path name. The new path name must be referenced by a share name that exists on the integrated Windows server.

   Note: When you save a directory that has shares defined over it, i5/OS saves the share information with the directory. If you specify a new object name when you restore the directory, i5/OS does not re-create these shares.
8. Use the `Directory subtree` field to specify whether you want to restore subtrees under a directory. The default is to restore all directories.
9. To specify that you want to restore files that were saved during a particular period, specify starting and ending dates and times in the `Change period` field.
10. Provide any other information that you want i5/OS to use to restore the files and press Enter.
11. When the files are restored, reboot the integrated server for new registry entries to take effect.

Using the Windows Backup utility with integrated servers

You can use the Windows Backup utility and a System i tape drive to do backups from the integrated Windows server.

You can use the Windows backup utility on Windows Server 2003 or Windows Server 2008 to save data to CD, DVDs or the virtual disks for the integrated server.

Integrated servers running Windows Server 2003 can also use tape or shared System i tape devices with the Windows backup utility. See "Using System i tape devices with integrated Windows servers" on page 157.

To start the Backup utility:
1. On the integrated server console, click **Start**
2. Select **Accessories** → **System Tools** → **Backup**.

For information about backup or recovery by using LAN-connected mass storage devices, refer to your Windows server documentation from Microsoft.

Using i5/OS to back up disks for active integrated Windows servers

Use the FREEZE.BAT and THAW.BAT scripts to configure backup for active Windows servers.

The disks that you create for integrated Windows servers are stored in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command.

The i5/OS operating system saves the changes that are made to the storage space during a save operation. This information is stored in a temporary file that can be up to 25% of the total size of the storage space. This default setting should work for most configurations.

Use the freeze and thaw scripts if you receive a message that too much space is being used by the process that tracks changes. You can also use the scripts if you know that applications on the Linux server will make frequent read and write requests to the storage space during the backup.

- The FREEZE.BAT script runs when i5/OS starts to back up a storage space. Use this script to stop applications that might fill the temporary storage space.
- The THAW.BAT script runs when i5/OS finishes backing up a storage space. Use this script to start any applications that you stopped with the FREEZE.BAT script.

Do the following steps to customize storage space backup.

1. Run these scripts when you start and finish backing up the storage space. You can modify them for your environment.
   a. %SYSTEMROOT%\AS400WSV\ADMIN\FREEZE.BAT
   b. %SYSTEMROOT%\AS400WSV\ADMIN\THAW.BAT
2. Edit the scripts.
3. Use the save (SAV) and restore (RST) commands to save the storage space. For more information about using the SAV and RST cmmands, see "Backing up predefined disks for integrated servers" on page 195.

Sharing devices between i5/OS and integrated Windows servers

Use these tasks to configure an integrated Windows server to use i5/OS tape and optical devices.

Related concepts

"Virtual and optical devices that are shared between i5/OS and integrated servers" on page 21
Integrated Windows and Linux servers can use tested System i tape and optical devices.

"Tested System i tape and optical devices iSCSI-attached integrated servers" on page 61
See the System i integration with BladeCenter and System x Web page for information about tape and optical devices that have been tested with iSCSI-attached integrated Windows and Linux servers. iSCSI-attached VMware servers do not support System i tape or optical devices.

Finding device descriptions and hardware resource names for System i devices

Do these steps to find device description and hardware resource names for System i devices.

You can have multiple integrated servers of the same type installed on your System i product. Use CL commands to see details about the resources and identify the hardware that is associated with a resource name.

1. If you are not already at the `Display Communication Resources` display, type `DSPHDWRSC *CMN`; then press Enter.
2. Type a 7 in the `Opt` field to the left of the resource name for a `File server IOA`. The `Display Resource Detail` display appears. For iSCSI-attached servers, locate the `locate the Network Server Host Port`. This is the resource to be used when creating an NWSH object. The NWSH object name is used when installing the NWSD.
3. Find the `Card Position` under the `Physical Location` heading.
4. Locate the labels on the slots of your System i product. One slot should be labeled with the same number or combination of letters and numbers shown in the `Card Position` field. This slot contains the integrated server hardware to which the resource name refers.

Using System i tape and optical devices with integrated Windows servers

Configure your iSCSI-attached integrated Windows server to use System i optical or tape devices.

Windows server can use an System i optical drive just as it does a local optical drive. The System i optical drive appears as a normal local optical drive in the **My Computer** folder on Windows server.

Locking an optical device:

If you have logical partitions on your System i product, the optical drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions and the optical drive must be allocated (locked) to a NWSD to be used.

To lock an optical drive, follow the steps below:

1. Click **Start**, then **Programs,** then **IBM i5/OS,** then **IBM i5/OS Integrated Server Support.**
2. Expand **IBM i5/OS Integrated Server Support**.
3. Expand the Network server description name.
4. Select **iSeries Devices**.
5. Select the device name.
6. Right-click and select **All Tasks, Lock Device.**

If you have any problems using the System i optical drive from an integrated Windows server, see Troubleshooting .

Transferring control of an optical drive from i5/OS to an integrated server:

The optical drive must be varied on before you can allocate it to an integrated Windows server. If the optical drive is not varied on, follow these steps to vary it on:

1. Vary on the optical device.
   a. At the i5/OS command line, type WRKCFGSTS *DEV *OPT and press Enter.
   b. In the Opt column next to the correct optical device, typically OPT01, type 1 to vary on the optical drive.
   c. Press Enter and the optical drive varies on.
2. Lock the optical device.
   a. Click **Start**, then **Programs,** then **IBM i5/OS,** then **IBM i5/OS Integrated Server Support**.
   b. Expand **IBM i5/OS Integrated Server Support**.
   c. Expand the network server description name.
   d. Select **System i Devices**.
   e. Select the device name.
   f. Right-click and select **All Tasks, Lock Device.**

Note: If the integrated server fails before unlocking an optical device, the optical device may be unavailable to i5/OS or other integrated servers. You will need to vary off the optical device using WRKCFGSTS *DEV *OPT and vary it back on to free the lock.

Transferring control of an optical device from an integrated server to i5/OS:

To use the optical drive from i5/OS, you must first unlock it from the integrated server. To unlock the optical drive from the integrated server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of the System i optical drive from an integrated server to i5/OS, follow these steps:

1. Click **Start,** then **Programs,** then **IBM iSeries,** then **IBM i5/OS Integrated Server Support**.
2. Expand **IBM i5/OS Integrated Server Support**.
3. Expand the network server description name.
4. Select **System i Devices**.
5. Select the device that you want to unlock.
6. Right-click and select **All Tasks,** then **Unlock Device**.

Restricting i5/OS tape and optical devices from integrated servers

You can prevent an integrated server from using a particular tape or optical device by specifying the tape or optical device as a restricted resource in the server's NWSD.

Restricting System i tape and optical devices with System i Navigator:

Do these steps to make System i devices inaccessible to an integrated server.

1. Expand **Integrated Server Administration** → **Servers**.
2. Right-click the server and select **Properties**.
3. Select the **System** tab.
4. Click **Advanced**.
5. Go tot he **Restricted Devices** tab and select the devices you want to restrict.
6. Click **OK**.

Restricting System i tape and optical devices using the character-based interface:

Do these steps at the i5/OS command line to use CL commands to make System i devices inaccessible to an integrated server.

1. Shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. Type WRKNWSD and press **Enter**. The Work with Network Server Descriptions display appears.
3. Type 2 in the Opt column next to the NWSD that you want to change. Press **Enter**. The Change Network Server Desc display appears.
4. Scroll down to the Restricted device resources parameter (RSTDEVRSC) and list the devices that are not to be made available. To specify more than two resources, type a + in the + for more values field and press **Enter**.
5. After you have entered your resources press **Enter**. Here is an example:

   CHGNWSD NWSD(nwsd-name) RSTDDEVRSC(OPT01 TAP02).
6. Start the server. See "Starting and stopping integrated servers" on page 190.

Using System i tape devices with integrated Windows servers

Do these steps to configure an integrated Windows server to use System i tape or optical devices.

System i tape drives can perform significantly faster than drives you normally attach to a PC server, and you can allocate them to integrated servers, therefore providing a faster tape access method than

available to PC servers. See Backup for Windows servers .

Because multiple integrated servers in the same System i product can all access the same tape drive (although not at the same time), you need to allocate only one tape drive for multiple integrated servers.

Notes:

1. Although you can dedicate tape drives to the integrated server and to i5/OS, both systems cannot simultaneously use the same tape drive. The two operating systems require different tape formats. You cannot use the same tape on an integrated server and on i5/OS without reformatting it.
2. If you have logical partitions on your System i model, the tape drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions.

To use an System i tape drive from an integrated server you must do these tasks.

Installing tape device drivers on Windows:

Download and install Windows device drivers for tape or optical devices.

For information about supported tape device drivers, see Supported tape devices for Windows servers

 .

No special actions are required to install the drivers. The instructions provided by the driver provider should be sufficient. Using the new tape drivers, the tape drives look identical to drives available for System x hardware. The devices are still listed by type-model number in the device locking/unlocking utility.

After the tape device has been locked once and the server has rebooted, there may appear to be an extra instance of the device in the Removable Storage Manager, and some backup applications. This behavior is normal. It may be safe to delete these extra instances. Consult your documentation. For the latest

information see Tape driver migration on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/windows/tape_driver_migration.html).

Formatting a System i tape for use with an integrated Windows server:

Use the Initialize tape (INZTAP) command to format a System i tape drive to work with your integrated Windows servers.

To format a tape, do the following steps:
1. Insert a tape in the System i tape drive.
2. At the i5/OS command line, enter INZTAP DEV(*tap01*) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED) CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC), where *tap01* is the name of your tape drive.
3. Press Enter.

Allocating a System i tape device to an integrated Windows server:

Do these steps to allocate a System i tape device to an integrated Windows server.

Note: Some tape devices report in under more than one device description. Tape libraries (3590, 3570, and so forth) report in as devices (TAPxx) as well as tape libraries (TAPMLBxx), where xx is a number. i5/OS Integrated Server Support does not support tape libraries. Therefore, if your device has a tape library description, you must vary off both the tape device and the tape library device before locking the device on the integrated server.

To transfer control of the System i tape device to an integrated server, follow these steps:
1. Vary off the tape drive on i5/OS.
   - To do this from System i Navigator
     a. Click **Configuration and Service** → **Hardware** → **Tape Devices**.
     b. Click **Stand-Alone Devices** or **Tape Libraries**.
     c. Right-click a device or library and select **Make Unavailable**.
   - To do this from the i5/OS character based interface
     a. At the i5/OS command line, type WRKCFGSTS *DEV *TAP, and press the Enter key. The Work with Configuration Status display appears.

        Note: WRKCFGSTS *DEV *TAPMLB will display a list of the tape library devices.
     b. In the Opt column next to the device name of your tape drive, type 2 to vary off the tape drive.
     c. Press Enter. The tape drive varies off.
2. Lock the tape device on an integrated server:
   a. From its Windows console, click **Start** → **Programs** → **IBM iSeries** → **IBM i5/OS Integrated Server Support**.

b. Expand **IBM i5/OS Integrated Server Support**.

c. Expand the network server description name.

d. Select **System i Devices**.

e. Select the tape object that you want to lock.

f. Right-click and select **All Tasks, Lock Device.**

If you need other information about the tape device to enable an application to recognize it, see "Identifying System i tape devices to Windows applications." If you have problems, see Troubleshooting on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Transferring control of a tape device from an integrated Windows server to the i5/OS operating system:

To use a tape drive currently locked on an integrated server from i5/OS, you must first unlock it from the integrated server and vary it on from i5/OS.

To unlock the tape drive from Windows server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of a System i tape drive from an integrated Windows server to i5/OS, follow these steps:

1. Unlock the tape device from the integrated Windows server console.

   a. Click **Start,** then **Programs,** then **IBM System i,** then **IBM i5/OS Integrated Server Support**

   b. Expand **IBM i5/OS Integrated Server Support**

   c. Expand the network server description name.

   d. Select **System i Devices**.

   e. Select the tape object that you want to lock.

   f. Select **Action,** then **All Tasks,** then **Unlock Device**.

2. Make the device available to i5/OS from the i5/OS console.

   From System i Navigator:

   a. Click **Configuration and Service** → **Hardware** → **Tape Devices**.

   b. Click **Stand-Alone Devices** or **Tape Libraries**.

   c. Right-click a device or library and select **Make Available**.

   From the i5/OS command line interface:

   a. Type WRKCFGSTS *DEV *TAP, and press Enter. The Work with Configuration Status display appears.

   b. In the Opt column next to the tape drive device name (for example, TAP01), type 1 to vary on the tape drive.

   c. Press Enter. The tape drive varies on.

   d. Change the tape to one formatted for i5/OS.

Identifying System i tape devices to Windows applications:

Do these steps to identify a System i tape device to Windows applications.

Windows applications do not refer to tape devices by device description or hardware resource name as i5/OS does. Instead they show tape devices in one of three ways:

- Manufacture-feature-model number
- Device map
- Port-bus-target id-lun

If you need these values, do this:

1. On the integrated Windows server console, click **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
2. Click on **System Tools**.
3. Click on **Device Manager**.
4. Double-Click on **Tape Devices**.
5. Right-Click on a tape device.
6. Select **Properties**.
7. The properties box has two tabs, one marked **General** and one marked **Driver**. The **General** tab shows the name of the device and the Bus Number, Target ID and LUN.

If all the tape devices on your System i product are of different types, this information is enough to distinguish between them in Windows applications. If you have multiple tape devices of the same manufacture-feature-model number, you must experiment to determine which tape drive is which.

Transferring System i tape and optical devices between integrated Windows servers

System i tape and optical devices can only be used by one integrated server at a time. Do these steps to transfer System i tape and optical devices between integrated servers.

To transfer control of tape and optical drives from one server to another, you must unlock it on one server and lock it on the other.

Note: If you have logical partitions on your System i product, the tape and optical drive is allocated to a single partition and cannot be shared by integrated servers that are in other partitions.

To transfer control of an System i tape or optical drive between integrated servers, follow these steps:

On the integrated server console that has control of the drive:

1. Click **Start** → **Programs** → **IBM System i** → **IBM i5/OS Integrated Server Support**
2. Expand **IBM i5/OS Integrated Server Support**
3. Expand the network server description name.
4. Select **System i Devices**
5. Select the device that you want to unlock.
6. Select **Action,** then **All Tasks,** then **Unlock Device**

On the integrated server console that you want to give control, lock the tape or optical drive.

1. Click **Start**, then **Programs**, then **IBM System i**, then **IBM i5/OS Integrated Server Support**
2. Expand **IBM i5/OS Integrated Server Support**
3. Expand the **Network Server Description** name
4. Select **System i Devices**
5. Select the device that you want to lock.
6. Select **Action,** then **All Tasks,** then **Lock Device**.

Printing from integrated Windows servers to System i printers

Do these steps to configure an integrated Windows server to print to a System i printer.

To send a print job to i5/OS, you must set up the i5/OS printer for TCP/IP printing. You must also set up the integrated server to use that printer through the LPD/LPR protocol. Your integrated server must also have the **Microsoft TCP/IP Printing** Network Service installed. See the Windows documentation for more information about TCP/IP Printing.

To set up an integrated server to print to System i printers, perform these tasks:

1. Set up the i5/OS printer for TCP/IP printing. For more information, see TCP/IP Setup topic collection.
2. Set up the integrated server to print to i5/OS printers:
    a. From the **Start** menu on Windows 2000 Server or Windows Server 2003, click **Settings**, then **Printers**. The **Printers** window appears.
    b. Double-click the **Add Printer** icon. The **Add Printer Wizard** starts.
    c. Click the **Network Printer** button.
    d. On the **Locate your Printer** panel, type the printer name or click **Next** to browse for the printer.

Uninstalling integrated Windows servers

Use the Delete Windows Server (DLTWNTSVR) command to uninstall integrated Windows servers.

You can use the Delete Windows Server (DLTWNTSVR) command to uninstall Windows server from integrated server hardware. Prior to running the Delete Windows Server command, shut down your integrated Windows server from i5/OS.

The Delete Windows Server (DLTWNTSVR) command deletes the specified Windows network server description and associated objects that were created by the Install Windows server (INSWNTSVR) command. These objects include the network server description, line descriptions, TCP/IP interfaces, and system created network server storage spaces. The network server must be varied off before this command is issued.

If you remove all your Windows and Linux servers from i5/OS and plan not to install any more, you can delete IBM i5/OS Integrated Server Support to free up the storage the product uses.

If the DLTWNTSVR command cannot be used (for example if the server's NWSD object no longer exists but some of the associated objects need to be cleaned up) you can manually delete the server and the associated objects using the following tasks:

Unlinking integrated server disks

Do these steps to unlink an integrated server disk from the Network Server Description (NWSD) object. When you unlink a disk, you make it inaccessible to the integrated server.

Restrictions:

1. For integrated Windows servers, see "Storage space linking for integrated servers" on page 20 for information about when disks can be dynamically unlinked.
2. For servers running VMware ESX Server, you can not unlink a disk from an active server (dynamic unlinking).
3. You can unlink a disk from a Linux server either when the server is shut down or when it is active (dynamic unlinking). Unlinking a dynamic storage from a running server is only possible at i5/OS V5R3 or later. Verify that the following things are true before you unlink the disk or the dynamic unlink will fail.
    - No users are using the Linux disk to be unlinked.
    - The disk was dynamically linked to the server
    - The disk is not part of an active logical volume group.

        Be careful about unlinking storage spaces from Linux servers that have an entry in /etc/fstab. If you unlink a drive from an integrated Windows server (other than the system or installation drives), Windows tolerates the missing drive and boots up normally, assuming that there are no application errors. Linux, however, detects the missing drive and halts the boot sequence. In this case, you need to sign on as root and go into maintenance mode to remove the file system entry for the drive you

unlinked before the server can continue the boot process. If you relink the storage space, you need to add back the file system entry you previously deleted.

Unlinking integrated server disks with System i navigator:

To unlink a Linux disk using System i Navigator, complete the following steps:

1. If you do not want to dynamically unlink the disk, shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. If you are dynamically unlinking a disk for an integrated Linux server, use the umount command at the integrated server console to unmount the disk.
3. Expand **Integrated Server Administration** → **All Virtual Disks** or expand **Integrated Server Administration** → **Servers** → *servername* → **Linked Virtual Disks**, where *servername* is the name of the server that the disk is linked to.
4. Optional: **Optional:** To change the sequence of the disks, click **Compress link sequence**.
5. Right-click the disk you want to unlink.
6. Select **Remove link** to open the Remove Link from Server window. The disk name and description that you specified when you created the storage space are displayed.
7. Click **Remove** to unlink the disk.

Unlinking disks with the character-based interface:

To unlink integrated server disks using CL commands, do the following steps.

1. If you do not want to dynamically unlink the disk, shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. If you are dynamically unlinking a disk for an integrated Linux server, use the umount command at the integrated server console to unmount the disk.
3. Type in WRKNWSSTG. Press **Enter**. The Work with Network Server Storage Spaces display appears. Type 11 in the Opt column next to the storage space that you want to unlink. Press **Enter**. The Remove Server Storage Link display appears.
4. Optional: Enter RMVNWSSTGL on the command line. Press **Enter**. The Remove Server Storage Link display appears.
   a. For **Network server storage space** enter the storage space name.
   b. For **Network server description** enter the NWSD that corresponds to the integrated server.
   c. You might need to press **F9** to see the **Renumber link** parameter. It is recommended that you take the default of *YES for this parameter unless you plan to relink the disk at a later time.
5. Press **Enter**. You see a message at the bottom of the display confirming that the storage space was unlinked successfully from the NWSD.

Deleting integrated server disks

Use these tasks to delete an integrated server disk with System i Navigator or CL commands.

Before you can delete an integrated server disk, you must unlink it from the integrated server. See "Unlinking integrated server disks" on page 161.

Deleting integrated server disks using System i Navigator:

Do the following steps to delete a virtual disk for an integrated server.

1. For integrated VMware servers, stop the server. See "Starting and stopping integrated servers" on page 190.
2. Unlink the disk from the server. See .
3. Expand **Integrated Server Administration** → **All Virtual Disks**.

4. Right-click the disk that you want to delete and select **Delete** or click the appropriate icon on the System i Navigator toolbar.

   To delete multiple disks simultaneously, hold down the control key (Ctrl) and click each of the disks you want to delete. Then right-click one of the selected drives and click **Delete**.
5. Click **Delete** on the confirmation panel.

Deleting integrated server disks with the character-based interface:

Do these steps to delete a network server storage space (known as a virtual disk).

You can use either the Delete network server storage space (DLTNWSSTG) command or Work with network server storage space (WRKNWSSTG) command to delete a virtual disk. Use these steps to delete a disk with the WRKNWSSTG command.

1. For integrated VMware servers, stop the server. See "Starting and stopping integrated servers" on page 190.
2. Unlink the disk from the server. See "Unlinking integrated server disks" on page 161.
3. Type WRKNWSSTG. Press **Enter**. The Work with Network Server Storage Spaces display appears.
4. Type 4 in the Opt column next to the storage space that you want to delete.
5. Press **Enter**. The system displays a message confirming that the storage space was deleted successfully.

Deleting device descriptions associated with integrated servers

Use the Work with Device Desscriptions (WRKDEVD) command to delete device descriptions associated with an integrated server.

To delete all of the device descriptions for an integrated server, follow these steps:

1. On i5/OS, type the command WRKDEVD and press Enter.
2. Page down until you see the device description that you want to delete.

   Note: The name of the device description starts with the first five characters of the NWSD name, followed by 'TCP' and a two-digit number. For example, if the NWSD name is MYSERVER, the device name might be MYSERTCP01.
3. Place a 4 in the Opt field to the left of the device description and press Enter. Repeat this step for any other device descriptions that are associated with the NWSD.

Note: There may be many devices on a system. Use the WRKDEVD MYSERTCP* or WRKDEVD *NET commands to get the complete list of network devices that need to be deleted.

Deleting controller descriptions associated with integrated Windows servers

Use the Work with Controller Descriptions (WRKCTLD) command to delete controller descriptions associated with integrated Windows servers.

To delete all of the controller descriptions for an integrated server, follow these steps:

1. On i5/OS, type the command WRKCTLD and press Enter.
2. Page down until you see the controller description that you want to delete.

   Note: The name of the controller description starts with the first five characters of the NWSD name, followed by 'NET' and a two-digit number. For example, if the NWSD name is MYSERVER, the controller name might be MYSERNET01.
3. Place a 4 in the Opt field to the left of the controller description and press Enter. Repeat this step for any other controller descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the WRKCTLD MYSER* command, where MYSER is the first 5 characters of the NWSD name.

> **Attention:** If you use this method, verify that you wish to delete all of the NWSDs on your system that begin with these 5 characters.

Deleting TCP/IP interfaces associated with an integrated Windows server

Delete the TCP/IP address that are associated with the Network Server Description (NWSD) for an integrated Windows server.

To delete TCP/IP interfaces that are associated with an integrated server, follow these steps:

1. On the i5/OS console, enter the CFGTCP command.
2. Choose option 1. Work with TCP/IP interfaces from the Configure TCP/IP menu.
3. Type a 4 in the Opt field next to the TCP/IP interface you want to remove, then press Enter.

   You can identify the TCP/IP interfaces that are associated with the network server description (NWSD) by looking at the name of the attached line description. This name consists of the NWSD name, followed by a number.
4. Repeat step 3 for each TCP/IP interface that is associated with the NWSD.

Deleting line descriptions for integrated Windows servers

Use the Work with Line Description (WRKLIND) command to delete line descriptions for integrated Windows server.

To delete all of an integrated server's line descriptions, follow these steps:

1. On i5/OS, type the command WRKLIND and press Enter.
2. Page down until you see the line description that you want to delete.

   Note: The name of the line description should be the name of the network server description (NWSD) followed by 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 or V9. This depends on the port number to which you attached it.
3. Place a 4 in the Opt field to the left of the line description and press Enter. Repeat this step for any other line descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the WRKLIND nwsdname* command, where nwsdname is the name of the associated network server description.

Deleting network server configurations for an iSCSI-attached integrated server

Use the Work with Network Server Configuration (WRKNWSCFG) command to delete Network Server Configuration (NWSCFG) objects for an integrated server.

To delete network server configurations that are associated with an integrated server, follow these steps:

1. On the i5/OS console, enter the WRKNWSCFG command.
2. Locate network server configurations associated with the NWSD. Typically they are identified generically as nwsdname*
3. Type a 4 in the **Opt** field next to the network server configurations you want to remove.
4. Press **Enter**.

Deleting the NWSD for an integrated Windows server

Delete Network Server Descriptions (NWSDs) for integrated Windows servers.

Before you delete a network server description (NWSD), you need to unlink its disk drives (see "Unlinking integrated server disks" on page 161) and delete storage spaces that are associated with that NWSD (see "Deleting integrated server disks" on page 162). Then you can delete the NWSD.

1. To unlink the storage space for the system drive for NWSDs created at V4R5 and later, on the i5/OS command line, type RMVNWSSTGL NWSSTG(nwsdname1) NWSD(nwsdname). Press Enter.

2. To unlink the storage space for the install source drive, type `RMVNWSSTGL NWSSTG(nwsdname2)` `NWSD(nwsdname)` and press Enter.

3. Any user defined storage spaces that have been linked to the NWSD can also be removed at this time using the command as often as needed `RMVNWSSTGL NWSSTG(nwsstgname) NWSD(nwsdname)` and press Enter.

4. To delete the network server storage space object for the system drive, type the command `DLTNWSSTG` `NWSSTG(nwsdname1)` and press Enter.

5. To delete the network server storage space object for the install source drive, type `DLTNWSSTG` `NWSSTG(nwsdname2)` and press Enter.

6. Remove any additional storage spaces that are no longer needed by typing the `DLTNWSSTG` `NWSSTG(nwsstgname)` command and pressing Enter.

To delete an integrated server's network server description (NWSD), follow these steps:

1. On i5/OS, type the command `WRKNWSD` and press Enter.

2. Type 8 in the `Opt` field to the left of the Network Server; press Enter. The Work with Configuration Status display appears.

3. If the status of the NWSD is not varied off, type 2 in the `Opt` field to the left of the Network Server; press Enter. Otherwise, go to the next step.

4. Press F3 to return to the previous dialog.

5. Enter a 4 in the `Opt` field to the left of the Network Server and press Enter.

6. On the `Confirm Delete of Network Server Descriptions` display, press Enter.

Note: If you are deleting an NWSD that was created before V4R5, see Delete an integrated Windows server's NWSD in the V5R3 iSeries Information Center.

Uninstalling IBM i5/OS Integrated Server Support

If you remove all integrated Windows and non-partition Linux® servers from your iSeries and do not plan to reinstall others, you may also want to remove IBM i5/OS Integrated Server Support, Option 29 from i5/OS. Removing the program frees the storage space it occupied on i5/OS.

Installing, configuring, and managing VMware ESX Server in iSCSI-attached integrated server environments

Use these tasks to install and configure an integrated server that runs the VMware ESX Server operating system.

Before installing VMware ESX server, see the VMware ESX on integrated servers (www.ibm.com/systems/i/bladecenter/vmware/) Web page for updates and limitations.

VMware ESX Server might also be referenced as 'ESX server' or 'ESX'.

Installing VMware ESX Server

Use these tasks to install and configure VMware ESX Server 3 on an iSCSI-attached integrated server. The ESX Server editions supported are Standard or Enterprise.

Starting the VMware ESX Server installation from the i5/OS console

Run the Install Linux Server (INSLNXSVR) command to start installing VMware ESX Server on an iSCSI-attached integrated server.

This step corresponds to slides 19-22 in the BladeCenter or System x iSCSI Installation Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

Complete the steps through *Prepare for operating system installation* from the "iSCSI-attached integrated server installation road map" on page 52 before you start this task.

1. Make sure that you connect the external Ethernet connection to the network before you begin installing VMware ESX Server so that the installation program can configure this connection.

2. Run the Install Linux Server (INSLNXSVR) command at the i5/OS console. For information about the parameters, see the Install Linux Server (INSLNXSVR) topic.

   When you install VMware ESX Server on an integrated server, two storage spaces are created by the INSLNXSVR command. These correspond to the first two drives. The first drive is the system drive (/dev/sda) where the ESX Server will be installed. The second drive is the install drive (/dev/sdb) which contains integrated server utilities to be installed. This drive is not for general use and is needed for integrated server function. For more information, see "Predefined disks and naming conventions for integrated servers running VMware ESX server" on page 19.

   Here is a sample command that uses the iSCSI configuration objects that you created in "Preparing for the integrated server operating system installation" on page 110:

   ```
   INSLNXSVR NWSD(MYESX) LNXSVRDST(*ESX3) RSTDDEVRSC(*ALL) STGPTH(MYNWSH) VRTETHPTH((*VRTETHPTP MYNWSH)) RMTNWSCFG(MYRM) SPNWSCFG(MYSP) CNNNWSCFG(MYCN)
   ```

3. The INSLNXSVR command prompts to place the ESX media in the BladeCenter or System x server before varying on the server.

   - For a blade, place ESX in the media tray and assign the BladeCenter KVM and media tray to the blade on which you want to install the VMware ESX Server, and then respond with a **G** to continue.

   - For a System x server, the server is not initially powered on, so that you can insert the installation media. Respond with a **G** to continue and insert the media when the server is performing the power on self test (POST). If the media are not available by the time POST completes and a boot source is not found, ensure that the installation media is inserted and then restart the server by pressing CTRL-ALT-DEL on the integrated server console.

Continuing the installation at the VMware ESX console

Do these steps to complete the VMware ESX installation on an iSCSI-attached integrated server.

1. Follow the steps listed in the Installing VMware ESX Server Software chapter in the Installation and Upgrade Guide for VMware Infrastructure 3 available on the VMware Infrastructure 3 Documentation

    (www.vmware.com/support/pubs/vi_pubs.html) Web page.

2. You can use the default values for most options during the installation. You must specify the following options on these screens:

Option	Description
Partitioning Options	• You must install ESX on /dev/sda which will be listed as **SCSI Disk sda IBM VDASD** *xxxx* where the *xxxx* is the name of the system drive. • You must not modify the partition on /dev/sdb otherwise your server will fail to boot after installation. This is the install drive which is intended only for integrated server functionality.
Advanced Options	You must select the **From a drive (install on the MBR of the drive)'** option in the ESX Boot Specification box.

Running the post install utility

Run the post install utility, ibmsetup.sh, to complete the required configuration tasks for an iSCSI-attached integrated server.

This step is not an optional step. This step ensures that the ESX server will shut down when the Network Server Description (NWSD) is varied off.

Note: When ESX server is shutdown by varying off the NWSD, it does not attempt to shutdown any virtual machines that the ESX server is hosting. You must manually shutdown the virtual machines before shutting down the ESX server to ensure a clean shutdown.

1. At the VMware ESX Server console, press ALT-F1 and sign on as root.
2. Enter the following command:

   `mkdir /mnt/ibmlsv`

3. Enter the following command:

   `mount /dev/sdb1 /mnt/ibmlsv`

4. Enter the following command:

   `/mnt/ibmlsv/install/ibmsetup.sh` *address* where *address* is the IP or hostname of your System i product.

Updating the integration software for VMware ESX Server

The integrated server software for VMware ESX Server has some components that run on i5/OS and others that run on the ESX server.

The ESX server components are installed when you complete the server installation.

The i5/OS-based software can be maintained by using the normal PTF process. The integration software installed on the ESX server requires you to

1. Apply the 5761-LSV PTF on your System i product.
2. Running the ixsupdt command from the ESX Server console.

Do the following steps to update the integration software that is installed on the integrated server.

1. Apply the i5/OS PTFs.
2. At the VMware ESX Server console, press ALT-F1 and log on as the root user.

   The syntax is `ibmlsvupdt userid [`*address*`]`

   where *userid* is an i5/OS user profile and *address* is the IP address or host name of the hosting i5/OS partition. The ibmlsvupdt command allows you to change the IP address or host name listed as the managing i5/OS partition for your server.

3. The ibmlsvupdt command will prompt for the i5/OS user's password. Type in the password and press Enter.

Managing integrated servers running VMware ESX Server

Use these tasks to manage iSCSI attached integrated servers running VMware ESX Server.

See "Managing and configuring iSCSI-attached integrated server environments" on page 190 for management tasks such as starting and stopping integrated servers, configuring the iSCSI network, and backup and recovery.

You need a knowledge of VMware Infrastructure 3 to configure your environment. See the VMware

Infrastructure 3 Documentation (www.vmware.com/support/pubs/vi_pubs.html) Web site.

Configuring multipath I/O for integrated servers running VMware ESX server

A hosted system can use redundant iSCSI data paths to access virtual disks hosted by i5/OS.

You can establish additional iSCSI data paths by defining a multipath group of two or more iSCSI targets and then specifying that a given virtual disk must be accessed using a group, rather than a single iSCSI target. With this configuration, the data on the virtual disk can be accessed using any of the iSCSI targets in the group.

The integrated server running ESX Server can have a maximum configuration of two iSCSI initiators and four iSCSI targets. For a general description of a multiple initiator or an iSCSI target configuration, see "Multipath I/O for iSCSI-attached integrated servers running Windows or VMware ESX Server" on page 21.

To configure a multiple iSCSI initiator or target configuration for an integrated server running ESX Server, you need to do some configuration tasks on i5/OS other configuration tasks from the VMware Virtual Infrastructure Client. Complete the following steps after the initial installation, and any time that you add additional iSCSI ports to the topology.

1. Do the following steps on i5/OS.

   a. Create a multipath group and link storage spaces to the multipath group. See "Configuring integrated servers for multipath input/output (I/O)" on page 193.

   b. Record all information for the iSCSI initiators that exist in the remote system configuration for the integrated server. You need to know the MAC address, IP address, and iSCSI qualified name of each initiator for a later step. You can display this information for iSCSI initiators from the remote system configuration object. From System i Navigator:

      1) Expand **Integrated Server Administration** → **iSCSI Connections** → **Remote systems**.

      2) Right-click a remote system configuration from the list available.

      3) Select **Properties**.

      4) Click the **Network Interfaces** tab.

      5) Record the MAC address, IP address, and iSCSI qualified name for each iSCSI initiator port.

      6) Click **Cancel** and close the properties panel.

   c. Start the integrated server. See "Starting and stopping integrated servers" on page 190.

2. From a client workstation, start the Virtual Infrastructure Client interface. You can connect to the Virtual Center Server or directly to the ESX server. If connecting to the Virtual Center Server, select the ESX server that you want to work with.

   a. Click the **Configuration** tab.

   b. Click **Storage Adapters**.

   c. A list of iSCSI initiator ports appears under QLA4022. One of the initiator ports is configured during the boot process. You need to configure other initiator ports to match the information in the remote system configuration. Do the following steps for each port that appears under QLA4022:

      1) Select the initiator port and click **Properties**, which is located below and to the right of QLA4022.

      2) On the General tab, note the MAC address and find the same MAC address in the remote system configuration.

      3) Click **Configure**.

      4) Enter the initiator iSCSI qualified name (IQN) from the remote system configuration, if not already configured. The initiator IQNs assigned by i5/OS are identical except for the last character, which is a 0, 1, 2, or 3.

      5) Enter the initiator IP address information, if not already configured. Even though a gateway is not supported, the VMware interface requires one to be configured. Make the gateway address the same as the IP address. This signifies that there is no gateway.

6) If changes were made, click **OK**. Otherwise, click **Cancel**.

7) Select the **Dynamic Discovery** tab. Click **Add** and enter the IP address of a NWSH that is part of the multipath group in i5/OS. Repeat the previous step until the IP address of every NWSH in the multipath group has been added.

8) Click **OK**.

d. Under Recent Tasks near the bottom of the window, check the status associated with previous steps. When the status is **Completed**, click **Rescan**, which is located in upper right corner Storage Adapters view. In the Rescan dialogue, click **OK**. When the rescan completes, you should see more LUN information in the Storage Adapters view.

Uninstalling integrated Linux or VMware ESX servers

Use the Delete Linux Server (DLTLNXSVR) CL command to delete integrated Linux or VMware ESX servers and the associated i5/OS objects.

You can use the Delete Linux Server (DLTLNXSVR) on i5/OS V5R4 or later to delete integrated Linux and VMware servers and the associated i5/OS objects, including:

- Network server description (NWSD) and associated line descriptions
- Point-to-Point Virtual Ethernet LAN line descriptions
- TCP/IP interfaces bound to Virtual Ethernet LAN line descriptions
- Predefined storage spaces (virtual disks) linked to the NWSD

You cannot delete an integrated server using System i Navigator. This command is available through CL commands only.

To run the delete command, enter:

```
DLTLNXSVR NWSD(nwsd-name)
```

If you no longer want to run integrated VMWare ESX, Linux, or Windows servers on the System i product, you can also delete the i5/OS Integrated Server Support option (5761-SS1 option 29) and the IBM Extended Integrated Server Support (5761-LSV) licensed program.

To remove the integrated server support software, run these commands at the i5/OS console:

```
DLTLICPGM LICPGM(5761SS1) OPTION(29)
DLTLICPGM LICPGM(5761LSV)
```

Installing, configuring, and managing Linux for iSCSI-attached integrated server environments

Install the Linux operating system and configure it for an integrated server environment.

There are the following limitations to running Linux on an iSCSI attached integrated server:

- Only a 1 initiator to 1 target iSCSI HBA configuration is supported.
- There is no virtual Ethernet support.
- iSCSI-attached Linux servers cannot use shared storage.

See the Linux on integrated servers (www.ibm.com/systems/i/bladecenter/linux/) Web site for the latest information about running Linux on integrated servers.

Installing the Linux operating system

Use Install Linux Server (INSLNXSVR) command to install Linux on the integrated server and complete the basic operating system configuration.

Starting the Linux installation at the i5/OS console

Run the Install Linux Server (INSLNXSVR) command to create the virtual disks and beginning installing Linux for an iSCSI-attached integrated server.

The Install Linux Server (INSLNXSVR) command initiates the installation of the Linux server operating system on an integrated server. INSLNXSVR also copies the integrated server support code on the installation drive which will be installed during the post installation steps.

This step corresponds to slides 19-22 in the BladeCenter or System x iSCSI Installation Overview animation on the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/index.html) Web page.

Linux server installation occurs in two steps. During the first step, the INSLNXSVR command creates all necessary objects to manage the server. This includes a network server description, message queue, line descriptions, storage spaces and TCP/IP interfaces. The network storage configuration objects for remote system, service processor and connection security are created by default unless the pre-existing objects are specified.

During the second step of the Linux server installation, the integrated server is varied on to start the Linux server installation.

Further Linux server installation is performed using the file server console and the normal Linux server installation process.

When INSLNXSVR completes normally, the Linux server is left in a varied on state.

Restrictions:

1. You must have input/output system configuration (*IOSYSCFG), all object (*ALLOBJ) and job control (*JOBCTL) special authorities to run this command.
2. The integrated server hardware must be varied off when you run the INSLNXSVR command.
3. The integrated server hardware will be varied off and varied back on during the second step of the installation as Linux server installs and requires the server to reboot.

Notes:

1. Any errors that occur during the first step of configuring the file server will result in the failure of this command.
2. After this command is run, if you need to manage the different resources created, use the following commands:
   - To check out the status of the Linux server, use the Work with Configuration Status command; WRKCFGSTS CFGTYPE(*NWS).
   - To manage the server just installed, use the Work with Network Server Descriptions command; WRKNWSD NWSD(network-server-name).
   - To manage the line descriptions created by this command, use the Work with Line Descriptions command; WRKLIND LIND(nwsdname*). The line descriptions are named using the network server name (NWSD parameter) specified on the INSLNXSVR command.
   - To manage the TCP/IP interfaces created by this command, use the Work with TCP/IP Network Status (NETSTAT) command, option 1. Another option is to use the Configure TCP/IP (CFGTCP) command, option 1.

- To manage the network server configurations just created by this command, use the Work with NWS Configuration command; WRKNWSCFG NWSCFG(nwsdname*). The network server configurations are named using the network server name (NWSD parameter) specified on the INSLNXSVR command.

If the installation fails at an early stage, all i5/OS objects that have been created are removed. However, if the installation fails after being transferred to the Linux console, the i5/OS objects remain. This is because you might be able to correct the error and recover the installation. In this case, restart the server and the installation code will try to resume from the point of failure. If you are unable to recover, or you decide to restart the installation from scratch, you can delete the Linux server instance using the Delete Linux Server (DLTLNXSVR) command.

Do these steps to run the INSLNXSVR command and start the installing the Linux operating system.

1. Complete the steps through *Prepare for operating system installation* from the "iSCSI-attached integrated server installation road map" on page 52.
2. Verify that the blade or System x hardware is turned off.
3. Make sure that you connect the external Ethernet connection to the network before you begin installing Linux so that the Linux installation program can configure this connection.
4. Verify that no other NWSD is varied on for the hardware resource you want to install on by running the CL command, and typing WRKCFGSTS *NWS. Display each NWSD that is varied on and confirm that it is not using the resource you intend to use.
5. Sign on to an i5/OS character-based session with a profile that has the following authorities: *IOSYSCFG, *ALLOBJ, and *JOBCTL or *SECADM.
6. Change the QSYSOPR message queue to something other than *BREAK so that the installation is not interrupted. For example, type the CL command CHGMSGQ MSGQ(QSYSOPR) DLVRY(*NOTIFY).
7. On the i5/OS command line type **INSLNXSVR** and press **F4**.

   This will display the parameters for the command. Below is a brief description of the required parameters. All other parameters are filled in with default values which can be modified as you prefer. For more details on the parameters, see "Install Linux Server (INSLNXSVR) command parameter descriptions" on page 174 and "Examples: Running the Install Linux Server (INSLNXSVR) command" on page 174.

   a. Enter information the following parameters:

   Network Server Description

   > Choose any name of up to eight characters that is meaningful to you. This does not have to be identical to the Linux server's host name. It is used to track the i5/OS objects associated with the integrated server. This name is used as the prefix for the system and installation drives, and the Point-to-Point Virtual Ethernet line description.

   Linux server distribution

   > See Linux on integrated servers (www.ibm.com/systems/i/bladecenter/linux/) for a list of distributions that have been tested on iSCSI-attached integrated servers.

   > Tested distributions include:

   > ***SLES10**
   > > SUSE Enterprise Linux Server 10 for AMD64 and Intel EM64T

   > ***RHEL5**
   > > Red Hat Enterprise Linux 5 for x86-64

   b. You might want to change the default values for the following optional parameters:

   Server storage space sizes
   > **Install source size:** The default value is calculated based on the space required to hold

the integrated server files. For details on sizes see "Predefined disks and naming conventions for integrated Linux servers" on page 19.

System size: The default value is calculated based on the space required to hold the Linux installation files. For information about disk sizes "Predefined disks and naming conventions for integrated Linux servers" on page 19.

Restricted device resources

You can use this parameter to list System i tape and optical devices that you do not want to make available to the Linux server as virtual devices.

You can optionally restrict which tape and optical drives can be allocated to integrated Linux servers in the hosting i5/OS partition. You might want to do this in order to reserve certain drives for use by i5/OS only. Tape and optical drives that are not to be made available to integrated Linux servers can only be specified after installation has been completed.

For iSCSI-attached solutions, you must restrict any tape or optical device that is not available, such as:

- External devices that are not powered on
- Any device that has been physically removed but still has a device description

If you do not restrict these devices, other devices (including disk, optical, and tape devices) might fail to report on your Linux server.

c. Enter information for the following parameters:

Storage Path

This parameter specifies the storage path the storage spaces can use. The **Network server host adapter** field must have the name of the existing network server host adapter device.

Virtual Ethernet Path

This parameter has two fields that describe the virtual Ethernet point to point connection. The **Port** field is filled in with *VRTETHPTP by default. The **Network server host adapter** field must have the name of the existing network server host adapter device.

Note: Virtual Ethernet is not supported on Linux but the INSLNXSVR command requires the VRTETHPTH parameter. When varying on the NWSD, the line description for the virtual Ethernet connection will remain in a vary on pending status.

Pool identifier

This parameter specifies the shared data pool this integrated server should use to process virtual disk I/O requests.

d. Use one of the following methods to enter information for the network server configuration (NWSCFG) objects that i5/OS will use to manage the remote system.

- The iSCSI install readme first Web page instructs you to create the network server configuration (NWSCFG) objects for **remote system**, **service processor**, and **connection security** prior to executing the INSLNXSVR command. You need to specify the names of these objects with the following parameters:

   Remote system NWSCFG

   Specifies the remote system network server configuration to use with this server.

   Service processor NWSCFG

   Specifies the service processor network server configuration to use with this server.

   Connection security NWSCFG

Specifies the connection security network server configuration to use with this server.

IP security rule

You must specify *NONE. The IP security rule parameter is not currently supported.

- If you do not specify values for the remote system, service processor, and connection security network server configuration (NWSCFG) objects, the INSLNXSVR command will create them for you. It is recommended that you verify your network connections by creating these objects before running the command.

If you have not already created these objects, enter information for the following parameters:

Enable unicast

This value should be ***YES**. This will enable the unicast packet distribution method for transmission of packets to the specified service processor host name or internet address.

Service processor name or SP internet address

You must specify the either the internet host name or address of the service processor for the remote system.

Initialize service processor

Specifies how the remote system's service processor is secured. This value should be *SYNC since a new service processor object will be created and needs to be synchronized with the remote system's service processor.

SP authentication

Specifies the service processor user ID and password. You must specify the user ID and password since the Initialize service processor parameter will be set to the value *SYNC .

Remote system identifier

Specifies the identifying serial number, type, and model of the remote system. You must specify these values for a blade system. You can use the default value of *EID for a System x product.

Remote interfaces

This parameter is used to identify and configure the remote system's SCSI and LAN interfaces. Both the SCSI and LAN have fields for **Adapter address**, **Internet address**, **Subnet mask** , **Gateway address**. The SCSI interface requires a value for **iSCSI qualified name**.

If you configure the iSCSI initiator to use dynamic addressing on boot (as recommended) and the install command has use the default setting of *DYNAMIC for the **Delivery** parameter, these values are provided to the iSCSI HBA during the boot process. If you use the default value of *GEN the Install Linux Server (INSLNXSVR) command will automatically generate a value if it is not specified. This default is designed to work with dynamic boot option.

When the iSCSI initiator is configured for manual addressing on boot and the install command has the **Delivery** parameter set to *MANUAL, these values must match what you have configured on the iSCSI HBA. In this case, you must specify a value other than *GEN in the iSCSI qualified name field.

8. Press **Enter**. When the command runs, the following things occur:
   - The NWSD is created.
   - The system storage space is created. This might take a few minutes depending on the size.

- The installation storage space is created.
- Files are copied to the installation drive.

9. The INSLNXSVR command prompts you to place the Linux distribution installation media in the BladeCenter or System x product prior to varying on the server. For a BladeCenter, place the Linux distribution installation media in the media tray and select the blade that will be installed then respond with "G" to continue. For a System x product, the server will not initially be powered on so that the installation media can be inserted. Respond with "G" to continue and insert the media while the server is performing the power on self test (POST). If the media are not available by the time POST completes and a boot source is not found, ensure that the installation media is inserted then reboot the server by pressing CTRL-ALT-DEL on the integrated server console.

   For example, a SLES 10 installation on an iSCSI-attached BladeCenter or System x product would prompt:

   ```
   Please insert *SLES10 install media into &1 local optical device (C G).
   ```

10. You will be prompted to input the installation media in the BladeCenter System x product would prompt: optical drive.

11. The configuration files are updated and then the installation is transferred to the Linux server's console. When this happens you see the following message at the bottom of the i5/OS command line session from which you ran the INSLNXSVR command:

    ```
    Network server install completed for <network server name>.
    ```

    The server boots after the i5/OS portion of the installation has completed. The Linux installation wizard is displayed on the server's console. You must now complete the installation from the Linux console.

Install Linux Server (INSLNXSVR) command parameter descriptions:

This topic lists information abut the Install Linux Server (INSLNXSVR) parameters.

For information about parameters for the Install Linux Server command, see the Install Linux Server (INSLNXSVR) topic in the Programming topic collection.

Note: The INSLNXSVR command only supports installations on iSCSI-attached servers.

Examples: Running the Install Linux Server (INSLNXSVR) command:

You can customize the parameters that you use for the Install Linux Server (INSLNXSVR) command depending on the configuration of your integrated server. Use these examples to help you select the parameters that you will use.

Installing SLES10 on an iSCSI-attached System x solution using existing configuration objects

Fewer parameters are required for the INSLNXSVR command when you create the i5/OS configuration objects in advance. This example uses an existing remote system, connection security, and service processor network server configuration (NWSCFG) objects. The iSCSI initiator is configured for DHCP boot.

```
INSLNXSVR NWSD(MYSLES10) LNXSVRDST(*SLES10) STGPTH(MYNWSH) VRTETHPTH((*VRTETHPTP MYNWSH))
RMTNWSCFG(MYRM) SPNWSCFG(MYSP) CNNNWSCFG(MYCN)
```

Installing SLES10 on an iSCSI-attached integrated server using the INSLNXSVR command to create configuration objects

You can use the Install Linux Server (INSLNXSVR) command to create the configuration objects for your integrated server.

In this example, the INSLNXSVR command generates the remote system, service processor, and connection security network server configuration (NWSCFG) objects that are required for a blade system.

```
INSLNXSVR NWSD(MYBLADE) LNXSVRDST(*SLES10) STGPTH(MYNWSH) VRTETHPTH((*VRTETHPTP MYNWSH))
SPINTNETA('X.X.X.X') SPAUT(MYUSER (MYPASSWORD)) RMTSYSID(SERAILNO TYPEMDL) CHAPAUT(*NONE)
RMTIFC((MACMACMACMAC 'X.X.X.X' 'M.M.M.M') (MACMACMACMAC 'X.X.X.X' 'M.M.M.M'))
```

Continuing the installation from the Linux console

Complete the operating system installation and update the integration code to ensure that your integrated server functions correctly.

Attention: The Linux distributors may require special instructions for the installation on supported BladeCenter and System x models. You must follow these special instructions. Any special instructions can be found by checking the hardware certification list as described below.

- For Red Hat: http://hardware.redhat.com ![icon] On this page you will see a **Quick Search** text field. Input your System x or BladeCenter model and click **Search**. You will see the associated Red Hat Enterprise Linux version listed. Click on your specific model to see details on the certification summary and details.

  In the details under Platform, **i386** means 32-bit, and **x86_64** means 64-bit version of the operating system. The 64-bit version is the only version supported.Your model should be listed. Click on the bulletin number to see information about configurations and installation requirements.

- For SUSE: http://developer.novell.com/yessearch/Search.jsp ![icon] On this page input the following and click **Search**.

  Keywords: Input your BladeCenter or System x model

  Company: IBM

  Product: SUSE Linux Enterprise Server 10 for AMD64 & Intel EM64T

  Note: The 64-bit version is the only version supported.

Completing a SLES 10 installation:

Do these steps to complete the required configuration tasks for SuSE Enterprise Linux Server 10 for AMD64 & Intel EM64T on an iSCSI-attached integrated server

Complete the steps in "Starting the Linux installation at the i5/OS console" on page 170 before you begin this task.

1. Do these steps when the System x or blade system boots from the SUSE Linux Enterprise Server 10 disc 1 located in the System x or blade CD-ROM drive.
   a. Select **Installation**.

      Important: If you do not make any selections within the 20 seconds, the default option to Boot from Hard Disk will be used. Because there is no operating system on the hard disk yet, the message "Failed to start from Harddisk" will be displayed. Press **OK** and then select **Installation**.
   b. Press **Enter**.
2. When the YaST installation wizard starts and the License agreement is displayed, click **I Agree** to accept the terms and continue with the installation.
3. The YaST installation wizard will display the phases of install on the right part of the screen. Specific settings are required for the **Base Installation - Installation Settings** phase and the **Configuration - Online** update phase. Settings in all other phases can be answered as you prefer. For more

information about installing SLES with YaST, you can reference the *SUSE Linux Enterprise Server Installation and Administration* manual, which you will find on the SUSE Linux Enterprise Server 10 disc 1 under /doc/en/manual.pdf.

Attention: If you see a message indicating that no hard drives were found, it might be due to an error in the iSCSI initiator settings or Remote system configuration NWSCFG object.

If you see this message, click **Abort**, then **Abort Installation**, and then select **Exit/Reboot**. Your system will reboot and will start the installation over again. Make sure you follow the steps in Step 1. For more information about installation problems, see Troubleshooting on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

4. During the **Base Installation - Installation Settings** phase, you can accept the default settings. To change the settings click on the Expert tab then either click on the category heading or click **Change...** and select the category from the list. Here is a list of the restrictions for each category:

Option	Description
Partitioning	If you choose to modify the partition setup, you must not modify the FAT partition on /dev/sdb1. Otherwise the server will not boot.
Booting	The Bootloader Type must be **GRUB** with a **Location** on /dev/sda (MBR).
Software	You must verify that the gettext package is being installed. To check this, do the following steps. 1. Click **Software**. 2. On the Software Selection and System Tasks screen, click on the **Details...** button. 3. Click the **Filter** drop down list and select **Package Groups**. This will show the RPM packages for the installation. 4. Select **Development Tools**. 5. In the list of tools in the upper-right panel, check **gettext**. 6. Click **Accept**.

5. After you have finished customizing the settings click **Accept**, then **Yes, install** when the warning message appears. The installation will prompt you for additional SLES10 discs if needed. When the installation is done copying data it will start the Configuration phase of the install.

6. During the **Configuration - Network** phase of the install, you will see a screen labeled **Test Internet Connection**.

Attention: You **must** select **No, Skip this test**. If you do not select **No, Skip this test**, a SLES update will be performed at this time which can cause unrecoverable damage to your server. A SLES update should only be done after the server has completed the install and you have completed the steps as described in "Continuing the installation from the Linux console" on page 175.

7. Continue on with the rest of the configuration phases of installation.

8. When the configuration phases are complete, you will be prompted to sign on to the server. You must follow the instructions described in "Running the post install utility" on page 177.

Completing a RHEL5 installation:

Do these steps to complete the installation of Red Hat Enterprise Linux 5 for x86_64 server on an iSCSI-attached integrated server.

Complete the steps in "Starting the Linux installation at the i5/OS console" on page 170 before beginning this task.

1. The Red Hat installation will prompt you for graphical or text based install. You can choose either method.
2. During the install interview, it is ok to use the defaults for most values. You must select the following values for **When partitioning disks**:
   - You must install RHEL 5 on /dev/sda.
   - You must not modify the partition on /dev/sdb otherwise your server will fail to boot after installation.
3. After the installation interview, the system will reboot and you will need to complete the configuration phase. During this phase on the Set up Software Update panel choose **No I prefer to register at a later time**.
4. After completing the installation steps for RHEL5 server, you must follow the instructions described in "Running the post install utility."

Running the post install utility

Run the post install utility, ibmsetup.sh, to complete the required configuration tasks for an iSCSI-attached integrated server.

Attention: This step is not an optional step. This step ensures that the server will:
- Shut down cleanly
- Prepare for Linux distribution updates
- Lock and unlock virtual tape and optical devices
- Exchange administrative information with the hosting i5/OS partition

To run the ibmsetup.sh script, complete the following steps:

1. Verify that the integrated hardware is connected to the hosting i5/OS partition using an external LAN connection.
2. Sign in to the Linux server as root.
3. Open a shell prompt. Right click on the desktop and select Open Terminal.
4. Enter the following command:

   `mkdir /mnt/ibmlsv`
5. Enter the following command:

   `mount /dev/sdb1 /mnt/ibmlsv`
6. Enter the following command:

   `mnt/ibmlsv/install/ibmsetup.sh address`

   (where *address* is the IP or host name of your System i product).

Maintaining the Linux integration code

Use the ibmlsvupdt script to install the latest integration code on your integrated server.

The Linux integration software has some components that run on i5/OS, and others that run on Linux. The Linux components are installed when you create the Linux server. The i5/OS-based code can be maintained using the normal PTF process.

The integration code installed on the Linux server requires:

1. Applying the 5761-LSV PTF on your System i product.
2. Running the ibmlsvupdt command from the Linux server console.

To run the `ibmlsvupdt` command, complete the following steps:

1. Sign in to Linux as either the root user or a user with root authority, and start a terminal session.
2. At the command prompt enter the `ibmupdt` command and press **Enter**. The syntax is:

   `ibmlsvupdt <userid> [<address>]`

   Where *userid* is an i5/OS user profile and *address* is the IP address or host name of the hosting i5/OS partition. The ibmupdt command allows you to change the IP address or host name listed as the managing System i partition for you integrated server.

   Linux integration support needs this data in order to set up a connection to exchange administrative information with i5/OS. It is important that you specify a valid IP address, or host name that is registered in the local DNS.
3. The ibmlsvupdt command will prompt for the i5/OS user's password. Type in the password and press **Enter**.

Managing integrated Linux servers

Use these tasks to connect to an integrated Linux server and perform basic management tasks such as starting or stopping the server.

See "Managing and configuring iSCSI-attached integrated server environments" on page 190 for management tasks such as starting and stopping integrated servers, configuring the iSCSI network, and backup and recovery.

Backing up and recovering integrated Linux servers

Use these tasks to back up and recover integrated Linux servers.

Linux backup and recovery overview

This topic discusses Linux backup and recovery.

Linux-centric backup is inherently file oriented in nature because Linux backup utilities operate at a file level. It is very difficult to back up an entire Linux drive as a single entity using Linux backup utilities. The only way to save a complete copy of a disk volume using Linux is to buy a third-party imaging product. These products require special skills to use, and are not supported for use with integrated Linux servers.

It should be noted that when we discuss Linux file-level backup and the applications that can be used to perform this task, we are really talking about Linux flat files, that is, non-database files. In i5/OS, we usually do not draw such a distinction because we use the same backup tools to save both database and non-database files. In Linux, however, you would usually back up database files using a backup application that is specific to the installed database. Therefore, when we discuss file-level backup in this section it is in the context of flat, or non-database, files.

There are other differences between an i5/OS and Linux backup. When performing an i5/OS backup, we usually put the partition to restricted state and save objects direct to tape. While the data can be compressed, the objects are written sequentially on the tape and not saved to a single container (archive in Linux terms). When backing up to tape, this is the most logical and efficient way to perform a save. In the Linux world, however, a backup usually means saving files to a single archive file on disk. The archive file can then either be copied to another Linux server in the network for safekeeping, or dumped to tape.

When we discuss backup we usually assume that we are backing up to tape. However, we can also back up to disk. Backing up to disk is usually an intermediate step before saving to tape in a staged backup. Ultimately we must back up to tape, or to disk on another system to guard against a complete loss of the primary system. While backup to tape is fairly straightforward, there are applications and techniques that can also be used to save data to disk on remote systems so that files can be quickly recovered in the event of a data loss.

Although Linux documentation might talk about "disaster recovery" backup, we need to draw a distinction between the disaster recovery backup capability provided by i5/OS for an integrated Linux server, and disaster recovery in the context of a Linux backup application. From the Linux point of view, a disaster recovery backup is a backup of all files on a disk volume or volumes versus backing up selected files. However, Linux backup applications still save at a file level, and you can still restore individual files from a Linux "disaster recovery" backup. In contrast, an i5/OS storage space backup saves a complete image of a Linux drive as a single entity, and you cannot directly restore individual files from it. You can restore the storage space to a new name and link it to the same server, then copy the needed files from it. However, i5/OS storage space backup is very fast, and can provide additional functions not readily available with a Linux "disaster recovery" backup, such as the ability to quickly restore a complete copy of the system drive. In the context of this information, we regard all Linux backup operations as file-level backups.

Note: When using a Linux backup application you can use either a native System i tape drive or a standalone Linux server-attached tape drive to save and restore Linux files. Both i5/OS and Linux cannot use a System i tape drive concurrently; it must be allocated or "locked" to one operating system or the other.

Note that the tape drive must be varied off in the hosting i5/OS partition. Tape devices show up under the /dev directory, for example, /dev/st0 or /dev/st1.

Using a Linux application to perform file-level backups can be difficult to incorporate into an unattended backup from the i5/OS side. This is because Linux cannot share a tape cartridge formatted for use by i5/OS.

Note: Tape libraries and automatic cartridge loaders (ACLs) on the supported devices list are not supported in random access mode. However, they are supported in manual or sequential access mode.

There are some good reasons why you might want to use an System i tape drive in preference to a device attached directly to the System x or blade system. System i tape drives tend to be very fast, reliable, robust and high capacity; and it can be possible to consolidate a number of tape drives in your organization down to one or two System i devices. If you have multiple integrated Linux servers in the same i5/OS partition, they can all access the same tape drive (although not at the same time). Therefore, you might only need one System i tape drive to back up all your Linux servers.

You can find more information about Linux backup strategies and automating the backup process, along with general information about backup and restore, at the following Web site:

http://www.backupcentral.com/

Linux recovery options
This topic discusses different Linux recovery options.

In the case where an integrated Linux server fails to start, there are options that allow you to boot from external media and potentially recover the server. These Linux recovery functions include:
- Rescue diskette
- Recovery mode CD-ROM

The Rescue diskette and Recovery mode CD-ROM functions are intended to provide you with a means of recovering a Linux server that fails to start. While it can be possible to use either of these techniques to recover an integrated Linux server, they are designed for standalone servers.

If you are unable to recover a failed standalone Linux server then your only other alternative is to rebuild it. In the case of an integrated Linux server, you should rarely, if ever, need to either use the Linux

recovery options or rebuild the server because you can save a complete image of the server using i5/OS storage space backup. In this case, all you need to do to recover a failed server is to restore a previously saved copy of the server's drives (storage spaces) and then restart it. Note that you might need to also restore volatile files from your file-level backup to make sure that the data is up-to-date.

You can effectively use these techniques to eliminate the need for the Rescue diskette and Recovery mode CD-ROM options that are available to recover a standalone Linux server.

Note: The ability to quickly and easily recover a failed Linux server is one of the major benefits of the Linux integration support.

Choosing a tape drive for use by your Linux backup application

This topic discusses the different tape drives to be used for a Linux backup.

Linux backup applications can either save to an System i tape drive or a tape drive directly controlled by a Linux server somewhere in the network.
- Backing up to a native System i tape drive

  System i tape drives can be accessed by backup applications running on the integrated Linux server.

  Because a System i tape drive appears to an integrated Linux server as a directly connected tape drive, you can also save remote integrated or non-integrated Linux servers to the System i tape drive across the network using a utility such as rsync. In other words, the System i tape drive behaves exactly as if it were a native Linux tape drive.
- Backing up to a native Linux tape drive

  If you have a Linux-based backup infrastructure already in place, it is likely that you have tape drives attached to standalone Linux servers in the network. Therefore, you can save files to a tape drive attached to an integrated Linux server in the same way as you would save files on any other standalone Linux server in the network.

Restricting System i tape drives that can be used by Linux

This topic discusses how to restrict Linux to specific tape drives.

You can optionally restrict which tape and optical drives can be allocated to integrated Linux servers in the hosting i5/OS partition. You might want to do this in order to reserve certain drives for use by i5/OS only. Tape and optical drives that are not to be made available to integrated Linux servers can only be specified after installation has been completed.

For iSCSI-attached solutions, you must restrict any tape or optical device that is not available, such as:
- External devices that are not powered on
- Any device that has been physically removed but still has a device description

If you do not restrict these devices, other devices (including disk, optical, and tape devices) might fail to report on your Linux server.

To restrict devices, complete the following steps:
1. Shut down the integrated Linux server.
2. On an i5/OS command line, enter the Change Network Server Description (CHGNWSD) command and press **F4**.
3. Scroll down to the Restrict device resources (RSTDEVRSC) parameter and list the devices not to be made available. Press **Enter**.
4. Restart the server.

Configuring a System i tape drive for use by Linux

This topic describes the tasks you need to perform to set up a System i tape drive for use by an integrated Linux server.

The System i platform supports a wide range of tape drives. If you have multiple tape drives on your System i product, each one can be allocated separately to either i5/OS or Linux.

A number of System i tape drives have been tested for use with integrated Linux servers, but some models cannot be used. The latest information about which tape devices have been tested for use can be found at the Tested tape devices for iSCSI attached Linux servers ![icon] (www.ibm.com/systems/i/bladecenter/linux/iscsi_tape_support.html) Web site.

To allocate a native System i tape drive for use by an integrated Linux server, the System i tape drive must be logically detached (varied off) from i5/OS. Then it must be logically attached (locked) to the integrated Linux server so that Linux thinks it has a physical tape drive directly attached. When this has been done, the integrated Linux server can use the System i tape drive as if it were a directly attached tape drive.

To enable an System i tape drive for use by Linux backup utilities and applications, complete these tasks.

Related concepts

"Virtual and optical devices that are shared between i5/OS and integrated servers" on page 21
Integrated Windows and Linux servers can use tested System i tape and optical devices.

"Tested System i tape and optical devices iSCSI-attached integrated servers" on page 61
See the System i integration with BladeCenter and System x Web page for information about tape and optical devices that have been tested with iSCSI-attached integrated Windows and Linux servers. iSCSI-attached VMware servers do not support System i tape or optical devices.

Formatting tape media for use by Linux:

This topic discusses how to format tape media.

The tape media formats used by i5/OS and Linux are mutually exclusive; i5/OS uses labels, Linux requires a non-labelled tape. Therefore i5/OS and Linux servers cannot share the same tape media.

Note: All new tapes must be initially formatted using the Initialize Tape (INZTAP) CL command. After the tape has been formatted using INZTAP, additional formatting can be done by Linux, if required.

From an i5/OS command line, enter the Initialize Tape (INZTAP) CL command:

```
INZTAP DEV(TAP01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED) CHECK(*NO) DENSITY(*DEVTYPE) CODE(*EBCDIC)
```

TAP01 is the name of the tape device. Yours might be different.

DENSITY(*DEVTYPE) gives the best performance; however, if you receive an error with this setting when trying to initialize the tape cartridge, try using DENSITY(*CTGTYPE). If you still receive an error, the tape cartridge is incompatible with your tape drive.

This command produces a non-labelled tape that can be used by Linux backup applications. Note that if tapes are used that are not of the default density for the drive (consult your drive's documentation), you need to reset the tape density after the System i partition has been restarted.

To reset the tape density after an System i partition has been restarted, complete the following steps:
1. Put a spare tape in the drive. Note that the next step erases all the data on the tape.
2. Issue the following command:

```
INZTAP DEV(tape-device-name) CHECK(*NO) Density(*CTGTYPE).
```

3. You can now switch the blank tape with the tape that you want to use for Linux backups. Backup applications should now work normally. Failure to initialize a blank tape of the correct density can have unanticipated results. If you regularly switch tape densities you might need to repeat the above steps more often than just after an IPL.

Transferring control of a tape drive from i5/OS to Linux:

This topic discusses how to transfer control of a tape drive from i5/OS to Linux.

Before you use an System i tape drive for a Linux backup application, you must make it unavailable from the i5/OS side using System i Navigator or a CL command, and then lock it on the Linux side through a Linux terminal session.

Note that some tape devices report in under more than one device description. Tape libraries (3570, 358x, 3590, and so on) report in as tape libraries (TAPMLBxx) as well as tape devices (TAPxx), where xx is a sequence number. The Linux integration support software does not support the tape library function. Therefore, if your device has a tape library description, both the tape and tape library devices must be made unavailable (varied off) before locking the device on the Linux server. Note that, although tape libraries are not supported as libraries in Linux, you can use them in sequential mode if the drive supports it.

If you have multiple integrated Linux servers being hosted by the same i5/OS partition, only one server at a time can use a particular System i tape drive. If you have multiple logical partitions on your System i product, a tape drive that is owned by one partition cannot be shared by integrated Linux servers that are being hosted by other partitions. Note, however, that it might be possible to logically switch tape drives between i5/OS partitions, depending on the hardware configuration of the System i product.

To transfer control of a tape drive from an i5/OS partition to an integrated Linux server, you must have i5/OS Administrator or Backup Operator authority.

To transfer control of an System i tape drive from i5/OS to Linux, choose one of the two following methods:

Transferring control of a tape drive with iSeries Navigator:

To transfer control of a System i tape drive with System i Navigator, complete the following steps:
1. From a System i Navigator window, expand the i5/OS partition you are working with.
2. Click **Configuration and Service** → **Expand** → **Hardware** → **Tape Devices**.
3. Click **Stand-Alone Devices** and then right-click the tape device you want to transfer control of to Linux. Select **Make Unavailable**.
4. If the tape device is also a tape library, click **Tape Libraries** and then right-click the tape library you want to transfer control of to Linux. Select **Make Unavailable**.
5. To lock the tape device to Linux, start a Linux terminal session and log in as root.
6. At the command prompt enter the ibmlsvdev command and press **Enter**. The syntax is:
   `ibmlsvdev [-list] | [[-lock | -unlock] device name]`
   For example, to list the tape and optical drives accessible by Linux enter the following command:
   `ibmlsvdev -list`
7. To lock TAP02 to Linux you would enter the following command:
   `ibmlsvdev -lock TAP02`

   Note: In Linux, commands are case sensitive. Make sure you use the same case as in our examples, for example, use TAP02 not tap02.

You could also use the Linux name. `ibmlsvdev -lock /dev/st1` for a rewindable tape device, or `ibmlsvdev -lock /dev/nst1` for a non-rewindable tape device. The ibmlsvdev -list command shows the status of TAP02 as LOCKED.

Note that you do not need to mount the tape device because Linux does not see it as a block device. You only need to mount block devices.

8. Insert a tape cartridge that has been formatted for Linux.

Transferring control of a tape drive with CL commands:

To transfer control of a System i tape drive with CL commands, complete the following steps:

1. On the i5/OS command line, use this command to vary off the tape device:

   `WRKCFGSTS *DEV *TAP`

2. On the Work with Configuration Status display, find the tape device you want to transfer control of to Linux. Type 2 next to the device and press **Enter**.

3. If the tape device is also configured as a tape library, enter the following command:

   `WRKCFGSTS *DEV *TAPMLB`

4. On the Work with Configuration Status display, find the tape library corresponding to the tape device you want to transfer control of to Linux. Type 2 next to the tape library and press **Enter**.

5. To lock the tape device to Linux, start a Linux terminal session and log in as root.

6. At the command prompt enter the ibmlsvdev command and press **Enter**. The syntax is:

   `ibmlsvdev [-list] | [[-lock | -unlock] device name]`

   For example, to list the tape and optical drives accessible by Linux enter the following command:

   `ibmlsvdev -list`

7. To lock TAP02 to Linux you would enter the following command:

   `ibmlsvdev -lock TAP02`

   Note: In Linux, commands are case sensitive. Make sure you use the same case as in our examples, for example, use TAP02 not tap02.

   You could also use the Linux name. `ibmlsvdev -lock /dev/st1` for a rewindable tape device, or `ibmlsvdev -lock /dev/nst1` for a non-rewindable tape device. The ibmlsvdev -list command shows the status of TAP02 as LOCKED.

   Note that you do not need to mount the tape device because Linux does not see it as a block device. You only need to mount block devices.

8. Insert a tape cartridge that has been formatted for Linux.

After the tape drive has been logically switched to the integrated Linux server, you can use it in the same way as you would use a tape drive directly attached to a standalone Linux server. Using a Linux backup application, you can now direct your Linux backups to the System i tape drive.

Transferring control of a tape drive from Linux to i5/OS:

This topic discusses how to transfer control of a tape drive from Linux to i5/OS.

To hand control of the tape drive back to i5/OS, unlock it on the Linux side and then make it available on the i5/OS side. This procedure is simply the reverse of the process you used to pass control of the tape drive to Linux.

Note that if you shut down the integrated Linux server, or the Linux server fails before you unlock the tape drive, it unlocks automatically. However, it is still in an unavailable state in i5/OS.

To transfer control of a tape drive from Linux to i5/OS, use one of the following methods:

Transfer control of a tape drive with Linux commands:

To transfer control of an System i tape drive back to i5/OS from Linux with Linux commands, complete the following steps:

1. To unlock the tape drive from Linux, start a Linux terminal session and log in as root.
2. At the command prompt enter the ibmlsvdev command and press **Enter**. The syntax is:

   ```
   ibmlsvdev [-list] | [[-lock | -unlock] device name]
   ```

   To unlock TAP02 from Linux you would enter the following command:

   ```
   ibmlsvdev -unlock TAP02
   ```

   You can also use the Linux name:

   ```
   ibmlsvdev -unlock /dev/st1
   ```

   Note: In Linux, commands are case sensitive. Make sure you use the same case as in our examples, for example, use TAP02 not tap02.

Transfer control of a tape drive with iSeries Navigator:

To transfer control of a System i tape drive back to i5/OS with System i Navigator, complete the following steps:

1. From a System i Navigator window, expand the i5/OS partition you are working with.
2. Click **Configuration and Service → Hardware → Tape Devices**.
3. Click **Stand-Alone Devices** and then right-click the tape device you want to transfer control of to i5/OS. Select **Make Available**.
4. If the tape device is also a tape library, click **Tape Libraries** and then right-click the tape library you want to transfer control of to i5/OS. Select **Make Available**.

Transfer control of a tape drive with CL commands:

To transfer control of an System i tape drive back to i5/OS with CL commands, complete the following steps:

1. On an i5/OS command line, use the following command to vary on the tape device:

   ```
   WRKCFGSTS *DEV *TAP
   ```

2. On the Work with Configuration Status display, find the tape device you want to transfer control of to i5/OS. Type 1 next to the device and press **Enter**.
3. If the tape device is also configured as a tape library, enter the following command:

   ```
   WRKCFGSTS *DEV *TAPMLB
   ```

4. On the Work with Configuration Status display, find the tape library you want to transfer control of to i5/OS. Type 1 next to the library and press **Enter**.

You can now use the tape drive from i5/OS.

Backing up files using Linux utilities and applications

This topic discusses backup and recovery using Linux utilities.

At the time of writing, not all the applications listed here had been tested for use with System i tape drives. However, even though a particular Linux backup application has not been tested for use with System i tape drives, this does not mean that the application will not work. You need to test your backup application to determine if it is compatible with the tape drive installed on your iSeries server.

When performing a backup you should close any operation that is using files on the Linux file system or the directory you intend to back up. Though native Linux backup utilities do back up files that are in use, we recommend that you close all open files and the operations using them so as to preserve the latest file updates and avoid any data corruption.

If the file system is network file system (NFS) then file locking occurs when the file residing on NFS is in use by an operation. Creating a tar or cpio backup archive can fail if you try to include such files. Commercial applications like IBM Tivoli® Storage Manager (TSM), ARCserve, Veritas, or Legato provide better facilities for backing up data as they provide open file agents. Even so, it would be safe practice to stop the operation that is locking the file over NFS before backing it up.

Determining the tape device block size

Before you begin your backup using a Linux utility or application, you need to determine the block size of the tape device you are using. To do this you run the mt command, for example:

```
mt -f /dev/st1 status
```

Replace /dev/st1 with the device name of your tape drive.

Setting the tape device block size

The ibmlsvdev command will attempt to set the block size to 32768 bytes when the device is locked. If the ibmlsvdev command is unable to set the block size, you can use the mt command to set it after the media is inserted.

For example, you can run the following command at the Linux console:

```
mt -f /dev/st0 setblk 32768
```

Replace *idev/st0* with the device name of your tape drive. Do not use a block size larger than 65,536 bytes.

Using i5/OS to back up disks for integrated Linux servers

Do these steps to back up integrated Linux server disks from the i5/OS operating system.

Backing up storage spaces for an active integrated Linux server:

Use the Save (SAV) command to back up storage spaces for active integrated Linux servers.

Use of this feature requires the IBM Extended Integrated Server Support for i5/OS licensed program (5761-LSV).

The virtual disks that you create for your integrated servers are in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command..

Note: You can use the same steps for backing up predefined disks (the system disk and the installation disk) and user defined disks.

The i5/OS operating system saves the changes that are made to the storage space during a save operation. This information is stored in a temporary file that can be up to 25% of the total size of the storage space. This default setting should work for most configurations. For information about customizing the backup process, see "Customizing storage space backup for an active integrated Linux server" on page 186.

To save disks from i5/OS, do these steps.
1. Ensure that the auxiliary storage pool (ASP) that contains the disk is varied on.
2. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.

3. Select one of the following options.

Option	Description
Save a disk for an active Linux or Windows server.	See "Using i5/OS to back up disks for active integrated Windows servers" on page 154 or "Customizing storage space backup for an active integrated Linux server."
Shut down the integrated server to prevent users from updating files during the backup.	See "Starting and stopping integrated servers" on page 190.

4. On the i5/OS command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device . For example, specify /QSYS.LIB/TAP01.DEVD in the *Device* field.
6. If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device.

   For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.
7. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc', where stgspc is the name of the network server storage space.

   For example, if the NWSD for the integrated server is named *testserver*, you can save the system and install disks by saving these network server storage spaces:
   - /QFPNWSSTG/*testserver*1
   - /QFPNWSSTG/*testserver*2
8. If you are saving a disk for an active server, specify the following values:
   a. Specify *YES for the **Save active** parameter. This option allows the storage space to be saved while it is still being used the system.
   b. Specify *NWSSTG for the **Save active option** parameter. This option allows network server storage spaces in directory '/QFPNWSSTG' to be saved when they are active.
9. Specify values for any other parameters that you want and press Enter to save the storage space.
10. If you stopped the integrated server, restart it now. See "Starting and stopping integrated servers" on page 190.

Customizing storage space backup for an active integrated Linux server:

Use the freeze and thaw scripts to configure storage space backup for an active integrated Linux server.

The default settings should work for most environments. Use the freeze and thaw scripts if you receive a message that too much space is being used by the process that tracks changes. You can also use the scripts if you know that applications on the Linux server will make frequent read and write requests to the storage space during the backup.
- The ibmlsvfreeze.sh script runs when i5/OS starts to back up a storage space. Use this script to stop applications that might fill the temporary storage space.
- The ibmlsvthaw.sh script runs when i5/OS finishes backing up a storage space. Use this script to start any applications that you stopped with the ibmlsvfreeze.sh script.

Do the following steps to customize storage space backup for a Linux server.
1. Copy the freeze and thaw scripts to the /etc/ibmlsv directory and rename them. You can use the following commands at the Linux console.
   a. cp /mnt/ibmlsv/service/ibmlsvfr.sh /etc/ibmlsv/ibmlsvfreeze.sh
   b. cp /mnt/ibmlsv/service/ibmlsvth.sh /etc/ibmlsv/ibmlsvthaw.sh
2. Edit the scripts. See your Linux documentation for more information about editing shell scripts.
3. Use the save (SAV) and restore (RST) commands to save the storage space.

Backing up and recovering individual integrated Linux server files and directories:

Use these tasks to back up individual integrated Linux server files and directories.

The IBM Extended Integrated Server Support licensed product provides support for file-level backup on Linux servers. You can use the i5/OS save (SAV) and restore (RST) commands to save files to System i tape, disk, or optical devices.

File-level backup for Linux has the following restrictions:
- The maximum size of file that can be saved or restored is 4GB.
- Hard-linked files will be restored as separate copies, not as linked files.
- The files saved must reside in the ext2, ext3, ext4, JFS/JFS2, ReiserFS, or XFS file system.
- Files in the /dev, /sys, /proc and /swap file systems cannot be backed up or restored.
- Files must be saved from and restored to the same operating system. For example, a file saved from a Linux server cannot be restored to a Windows server.

Configuring integrated Linux servers for file level backup:

Do these steps to configure integrated Linux servers for file-level backup.

Use of this feature requires the IBM Extended Integrated Server Support for i5/OS licensed program (5761-LSV).

1. Install the IBM Extended Integrated Server Support for i5/OS licensed program.
2. Use the ping utility to verify that i5/OS can contact the Linux server host name or IP address. The host name of the Linux server is typically the same as the NWSD name. See Ping for information about using the ping utility.
   a. If the Linux host name is the same as the NWSD name and the Linux host name can be resolved using DNS, then take no action.
   b. If there is no DNS entry for the NWSD name, then add the NWSD name to DNS or use the Add TCP/IP Host Table Entry (ADDTCPHTE) command to add the IP address of the Linux server to the System i host table. See Add TCP/IP Host Table Entry (ADDTCPHTE).
3. Create an account on the Linux server for file-level backup.

   The i5/OS operating system will use this user to sign into the server. This user must have access to the files that you want to save. The user ID and password must match the i5/OS user and password that will be used for backing up files. If the user ID and password do not match, the system will not find the files on the Linux server.
4. Create a Samba password for the Linux user. See the Samba documentation for more information about how to create a Samba password.

   For example, enter `smbpasswd -a` *userid* where *userid* is the name of the Linux user.
5. Create Samba shares for the data that you want to save. See the Samba documentation for more information about creating shares.
6. Ensure the Samba services can be accessed through your server's firewall. See your Linux distribution documentation for information about how to configure your firewall to allow Samba traffic.
7. Start Samba. For example, enter `smbd -D` at the Linux command line.
8. Use the Work with Object Links (WRKLNK) CL command to verify that the i5/OS operating system can access the Samba shares on the Linux server through the QNTC file system.

Adding members to the QAZLCSAVL file using Linux backup utilities:

Do these steps to add members to the QAZLCSAVL file using Linux backup utilities.

Create a member for each share that you want to back up. *nwsdname* is the name of the network server description (NWSD) for the server.

1. On the i5/OS command line, use the Add Physical File Member (ADDPFM) command to add a file member. Type `ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(`*nwsdname*`) TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)`.

2. In the file member that you just created, list all the shares that you want to be able to save. List each share name that you defined for the server on a separate line. Share names can have embedded blanks. For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as shares on LINSVR1, your member name LINSVR1 would look like this:

   ```
   QUSRSYS/QAZLCSAVL LINSVR1
   0001.00 cshare
   0002.00 dshare
   0003.00 eshare
   0004.00 fshare
   0005.00 gshare
   0006.00 my share
   ```

   Note: If you specify multiple share names that point to the same directory, the i5/OS operating system saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not include multiple shares that include the same directory or data.

Saving and restoring files for integrated Linux servers:

Use the Save (SAV) CL command to save your files.

To be able to restore a directory or file by share name, you must specify that file or share name on the SAV command.

Note: To avoid duplicating data, specify each share only once. If you specify multiple share names that point to the same directory on the Linux server, i5/OS saves the data multiple times.

Do these steps to save your files.

1. Ensure that the Linux server is active. See "Starting integrated servers" on page 190.
2. Also ensure that the QSYSWRK subsystem, QSERVER, and TCP/IP are active. You can use the Work with Active Jobs (WRKACTJOB) command).
3. On the i5/OS command line, type SAV and press F4.
4. In the `Device` field, specify the device on which you want i5/OS to save the data. For example, 'QSYS.LIB/TAP01.DEVD' saves the data to tape.
5. In the `Object` field, specify what you want i5/OS to save in the form '/QNTC/*servername*/sharename' You can use wildcard characters. See "Examples: Saving files for integrated Linux servers" for how to specify particular parts of the Linux server.
6. Use the `Directory subtree` field to specify whether you want to save subtrees under a directory. The default is to save all directories.
7. To specify that you want to save changes since the last save, specify *LASTSAVE in the `Change period` field. You can also specify a specific range of dates and times.
8. Press `Enter` to save the shares that you specified.

Examples: Saving files for integrated Linux servers:

These examples show how to use the save (SAV) or restore (RST) commands for specific parts of integrated Linux servers.

Here are examples for server *server1*, where *server1* is the name of the Linux server.

Note: The CHGPERIOD(*LASTSAVE) option is not supported on integrated Linux servers.

To save or restore this:	Specify this:
All server objects.	`OBJ('/QNTC/*') SUBTREE(*ALL)`
All objects for *server1*.	`OBJ('/QNTC/server1/*') SUBTREE(*ALL)`
All objects for *server1* that changed during a certain period (in this case between 10/19/2007 and 10/25/2007).	`OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD('10/19/2007' '00:00:00' '10/25/2007' '23:59:59')`
All directories, files, and shares to which a particular share (for example, 'fshare') refers. i5/OS does not save and restore the directory over which the share is built.	`OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)`
Only files to which the specified share (for example, 'fshare') refers that match the specified pattern (pay*). i5/OS does not save directories nor shares.	`OBJ('/QNTC/server1/fshare/pay*')`
Only directories and shares (no objects) for 'fshare' and its immediate children.	`OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)`
Directories, shares, and files for 'terry' and its subtrees (not directory 'terry').	`OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)`
Only the specific file 'myfile.exe'.	`OBJ('/QNTC/server1/gdrive/myfile.exe')`

Uninstalling integrated Linux or VMware ESX servers

Use the Delete Linux Server (DLTLNXSVR) CL command to delete integrated Linux or VMware ESX servers and the associated i5/OS objects.

You can use the Delete Linux Server (DLTLNXSVR) on i5/OS V5R4 or later to delete integrated Linux and VMware servers and the associated i5/OS objects, including:

- Network server description (NWSD) and associated line descriptions
- Point-to-Point Virtual Ethernet LAN line descriptions
- TCP/IP interfaces bound to Virtual Ethernet LAN line descriptions
- Predefined storage spaces (virtual disks) linked to the NWSD

You cannot delete an integrated server using System i Navigator. This command is available through CL commands only.

To run the delete command, enter:

`DLTLNXSVR NWSD(nwsd-name)`

If you no longer want to run integrated VMWare ESX, Linux, or Windows servers on the System i product, you can also delete the i5/OS Integrated Server Support option (5761-SS1 option 29) and the IBM Extended Integrated Server Support (5761-LSV) licensed program.

To remove the integrated server support software, run these commands at the i5/OS console:

```
DLTLICPGM LICPGM(5761SS1) OPTION(29)
DLTLICPGM LICPGM(5761LSV)
```

Managing and configuring iSCSI-attached integrated server environments

Use these tasks to administer all types of iSCSI-attached integrated server environments.

Starting and stopping integrated servers

Use these tasks to stop and start integrated servers.

Starting integrated servers

You can start integrated servers from System i navigator or the i5/OS command line.

Starting a single integrated server using System i Navigator:

The Integrated Server Administration function of System i Navigator provides an interface for starting singe or multiple integrated servers.

To start a single integrated server using System i Navigator, complete the following steps:
1. Click **Integrated Server Administration** → **Servers**.
2. Right-click the server you want to start.
3. Select **Start**. After a few moments, you should see the status change to Started.

Starting multiple integrated servers using System i Navigator:

To start all integrated servers select one of the following methods:
- Right-click **Servers** in the left pane and select **Start all**.
- Click **Start all integrated servers** in the Taskpad pane.

To start selected servers only, hold down the control key (Ctrl) and click each of the servers you want started. Then right-click one of the selected servers and click Start.

Tips:
- If you have two or more server instances created for the same integrated server hardware, you should not try to start all servers simultaneously. Remember, these are server instances, not physical servers.
- Because of interdependencies between servers, you might wish to start the servers in a specific order.

Starting integrated servers using CL commands:

To start an integrated server from an i5/OS command line, select one of the following CL commands:

Work With Configuration Status (WRKCFGSTS)
1. Type WRKCFGSTS *NWS. Press **Enter**.
2. Type 1 in the Opt column next to the network server description (NWSD) that you want to vary on. Press **Enter**.

   To start multiple integrated servers using the WRKCFGSTS command, simply type 1 in the Opt column next to all the network server descriptions (NWSD) that you want to vary on. Press **Enter**.

Vary Configuration (VRYCFG)
1. Type VRYCFG. Press **F4**.
2. Enter the NWSD that you want to vary on. Press **Enter**. Here is an example:
   ```
   VRYCFG CFGOBJ(nwsd-name) CFGTYPE(*NWS) STATUS(*ON)
   ```

To start multiple network server descriptions (integrated servers) using the VRYCFG command, simply list all the network server descriptions (NWSDs) that you want to vary on in the CFGOBJ parameter. Press **Enter**. For example:

```
VRYCFG CFGOBJ(nwsd-name1 nwsd-name2 nwsd-name3) CFGTYPE(*NWS) STATUS(*ON)
```

Using the VRYCFG command in this way could lock up your green screen session for several minutes.

Starting integrated servers automatically when i5/OS starts:

If you only have a single integrated server, or you do not need to start your servers in a specific order, you can configure integrated servers to start when i5/OS starts.

1. On the i5/OS command line type CFGTCP. Press **Enter**.
2. On the Configure TCP/IP display type 1. Press **Enter**.
3. Locate the interface for the Point-to-Point Virtual Ethernet line that corresponds to the server you want to start automatically. It is of the form nwsd-namePP. Enter 2 next to the interface. Press **Enter**.
4. Change the Autostart parameter to *YES*. Press **Enter**.

When you next power up the System i product, the integrated server starts automatically.

Starting an integrated server when i5/OS TCP/IP starts

To configure integrated servers to start when i5/OS TCP/IP starts, do these steps.

However, if multiple integrated servers use a single file server resource, configure only one of them to autostart. Only one network server can use the file server resource at a time. Configuration of multiple TCP/IP interfaces to autostart for network servers that share the same resource can cause unpredictable results.

To have an integrated server automatically vary on when you start TCP/IP, follow these steps:

1. On the i5/OS command line, enter the Configure TCP/IP (CFGTCP) command.
2. Choose Option 1 `Work with TCP/IP interfaces` and press Enter.
3. Specify 2 (change) in the Option field next to the interface for the point to point virtual Ethernet (virtual Ethernet point to point) line description for the server, and press Enter.

   Note: The point to point virtual Ethernet line description has a name that consists of the network server description (NWSD) name followed by 'PP' for the virtual Ethernet point to point LAN. For example, if the NWSD name is MYSVR, then the point to point virtual Ethernet LAN line description is MYSVRPP.

4. Change the **Autostart** parameter value to *YES and press Enter. The integrated server automatically varies on when you start TCP/IP.

   Note:

   a. TCP/IP can be automatically started by the system at IPL by changing the system's IPL attributes. A startup procedure is no longer necessary. Any TCP interfaces with the Autostart parameter set to *YES will be started along with TCP/IP at IPL.
   b. Be aware that an IP address entered at the integrated console for the point to point virtual Ethernet overrides the value set in the NWSD for the TCPPRTCFG parameter *VRTETHPTP port. However, operations such as SBMNWSCMD use the value set in the NWSD to find the server. Both values must be consistent.

Shutting down your System i hardware when integrated servers are present

Learn how to safely shut down your system when integrated servers are installed.

The easiest way to ensure your integrated servers will be shut down safely is to always manually shut them down before shutting down the System i hardware. The CL command PWRDWNSYS *CNTRLD will attempt to power-down each of the integrated servers, giving each of them a period of time (the NWSD attribute SHUTDTIMO, by default 15 minutes) in which to shut down. Note that there is no guarantee that they will finish shutting down within this time period.

CAUTION:
The CL command PWRDWNSYS *IMMED is not recommended. This will power down the System i product immediately, without attempting to shut down any integrated servers.

Table 18. Methods for shutting down the System i product

Action	Result
Shut down the integrated server manually.	The integrated server is varied off properly, with no risk of data loss.
Issue the CL command pwrdwnsys *cntrld.	The integrated server is given the length of time specified in the shutdown timeout attribute of its NWSD in which to shut down, then the System i hardware continues to power down.
Issue the CL command pwrdwnsys *immed.	The System i hardware powers down immediately and does not shut down any integrated servers. Data corruption may result.

If your i5/OS system uses the Power On/Off Schedule, the Power-Off exit program (QEZPWROFFP) should be changed to vary off all NWSDs before calling the PWRDWNSYS command. Careful consideration must be given to scheduling as the number and activity of each server will determine the amount of time necessary to completely vary off each server. Use the Submit multiple jobs (SBMMLTJOB) and Job description (JOBD) parameters of the Vary Configuration (VRYCFG) command to vary multiple servers at the same time in batch. The scheduled power on must not occur before the system has a chance to vary off all servers and issue the PWRDWNSYS. See the Schedule a system shutdown and restart topic.

Stopping integrated servers

To shut down an integrated server, follow these steps.

Attention: If you use this method to shut down VMware ESX Servers, the system does not attempt to shutdown any virtual machines that the ESX server is hosting. You must manually shutdown the virtual machines before shutting down the ESX server to ensure a clean shutdown.

1. Select **Integrated Server Administration** → **Servers**.
2. Right-click the server you want to stop and select **Shut Down**. If you want to shut down all integrated servers, right-click the Integrated Servers icon in the left navigation and select **Shut Down All**. The status changes to **Shutting down...**, **Partially shut down**, and eventually **Shutdown**.

Configuring multipath I/O for integrated servers

Use these tasks to configure i5/OS and your integrated server operating system for multipath I/O.

Multipath I/O enables multiple storage connections for an integrated server. You need to configure both i5/OS and the integrated server operating system.

Before you configure multipath I/O, make sure that you have the latest firmware and software updates installed on the integrated server. For more information, see the iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/) Web page.

Configuring the Windows operating system for multipath I/O

Do these steps to install the Microsoft Software Initiator service on the integrated server.

1. Download and install the Microsoft iSCSI Software Initiator.

   For information about versions of the software that have been tested with iSCSI-attached integrated servers, see the iSCSI install read me first➡️ (www.ibm.com/systems/i/bladecenter/iscsi/readme/) Web page.

   a. Go to the Microsoft Download Center➡️ (www.microsoft.com/downloads/) Web page.

   b. Search for iSCSI initiator.

   c. Install **Virtual Port Driver**, **Initiator Service**, and **Microsoft MPIO Multipathing Support for iSCSI**.

      Important:

      1) Do not select the option for Software Initiator.

      2) Do not manually configure the installed Microsoft components. The i5/OS Virtual Ethernet Manager Service is aware of the target storage configured in the i5/OS operating system and provides the optimal multipath configuration.

2. Restart the Windows operating system.

Configuring integrated servers for multipath input/output (I/O)

To configure your integrated Windows or VMware ESX server to use a multipath group, do these steps.

1. Shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. Expand **Integrated Server Administration** → **Servers**.
3. Right-click a server from the list available.
4. Select **Properties**.
5. Click the **Storage Paths** tab.
6. At least two storage paths are required to enable multipath I/O. If there is only one storage path currently shown in the table, do these steps to add an additional storage path:
   a. Click the **Add** button on the **Storage Paths** tab.
   b. On the next panel, select the network server host adapter (NWSH) to use for the storage path.
   c. Click **OK**.
7. Below the storage paths table, click the **Properties** button for the multi-path group.
8. Select the defined storage paths to be members of the multi-path group.
9. Click **OK** to update the multi-path group information on the server properties panel.
10. Select the multi-path group as the default path for disk drives.
11. Click **OK** on the server properties panel to save the changes to the NWSD.
12. Verify that the disks for the server are linked to the default path or the multipath group. If you need to change the links for a disk, do the following steps.
    a. Unlink the disk from the integrated server. See "Unlinking integrated server disks" on page 161.
    b. Link the disk to the server. Specify either the multipath group or the default path. See "Linking disks to integrated servers" on page 232.
13. Ensure all information for the iSCSI initiator ports exists in the remote system configuration for the integrated server. You need to know the MAC address and IP address for each initiator port. To add information for additional iSCSI initiator ports to the remote system configuration object, follow these steps.
    a. From System i Navigator, expand **Integrated Server Administration** → **Expand iSCSI Connections** → **Remote Systems**.
    b. Right-click a remote system configuration from the list.

c. Select **Properties**.

d. Click the **Remote Interfaces** tab.

e. Click **Add** and input the MAC address and IP address. The MAC address is shown on a label on the HBA, and is also displayed when the iSCSI initiator configuration utility runs on the integrated server. For IP address guidelines, see "Selecting IP addresses for the System x or blade iSCSI initiator" on page 74.

f. Click **OK** to save and exit.

If you want to use a CL command, see the STGPTH, MLTPTHGRP and DFTSTGPTH keywords on the Change Network Server Description (CHGNWSD) command.

Backing up and recovering integrated servers from i5/OS

You can back up and recover integrated server data from either i5/OS or the integrated server operating system. Use these tasks to configure backup and recovery from i5/OS.

- Do a full system backup of the i5/OS operating system. See the Backing up your system topic collection.
- Back up the network server description (NWSD) and the disk drives that are associated with the integrated server on i5/OS.
- Back up individual integrated Windows and Linux server files by using the i5/OS SAV and RST commands and i5/OS NetServer or a backup utility.

See "Backing up and recovering integrated Linux servers" on page 178 and "Backing up and recovering integrated Windows servers" on page 147 for information about configuring the integrated server operating system to use System i tape and optical devices, file-level backup from i5/OS, and saving active servers.

Use these tasks to back up and recover integrated servers from the i5/OS operating system.

Backing up the NWSD and other objects associated with integrated servers

Do these tasks to back up the i5/OS configuration objects and files related to integrated servers.

Backing up the NWSD of an integrated server:

Do these steps to save an NWSD with the Save Configuration (SAVCFG) command.

Note: when you save the associated storage space objects, you also need to save the Network Server Description (NWSD). To save an NWSD, you use the Save Configuration (SAVCFG) command:

1. On the i5/OS command line, type SAVCFG.
2. Press Enter to have i5/OS save the NWSD configuration.

Backing up the NWSH for an iSCSI-attached integrated server:

Use the Save Configuration (SAVCFG) command to back up a network server host adapter (NWSH) object.

1. On the i5/OS command line, type SAVCFG.
2. Press Enter to have i5/OS save the NWSH configuration.

Backing up iSCSI NWSCFGs and validation lists:

For servers attached by iSCSI HBAs, the additional configuration objects are stored in the QUSRSYS library. These include the network server configuration objects (type *NWSCFG) and an associated validation list object (type *VLDL).

Note: The *NWSCFG and *VLDL objects will share the same name.

To save the network server configuration and validation list objects, use the Save Object (SAVOBJ) command:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
2. Shut down the Windows server to release any object locks.
3. On the i5/OS command line, type SAVOBJ and press F4.
4. In the **Objects** field, specify the NWSCFG names.
5. In the **Library** field, specify QUSRSYS.
6. If you are saving the objects to tape, specify the name of your tape device in the **Device** field (for example, TAP01). If you want to use a save file instead of tape, specify *SAVF as the device and enable the data compression option.
7. For **Object type**, specify both *NWSCFG and *VLDL.
8. If you are using a save file, press F10 to see additional parameters.
9. In the **Save file** field, specify the path to your save file (for example winbackup/nwscfg).
10. If you are using a save file, page down change the value for Data compression to *YES.

Backing up predefined disks for integrated servers:

Do these steps to back up predefined disks.

When you install an integrated server, i5/OS creates the system and installation source drives as predefined drives that you need to save.

Note: Treat the network server description, predefined disk drives, and any user-defined disk drives linked to an integrated server as a unit. Save and restore them at the same time. Together they constitute a complete system, and should be treated as such. Otherwise, the integrated server might not start or run correctly.

The virtual disks that you create for your integrated servers are in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command..

Note: You can use the same steps for backing up predefined disks (the system disk and the installation disk) and user defined disks.

1. Ensure that the auxiliary storage pool (ASP) that contains the disk is varied on.
2. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
3. Select one of the following options.

Option	Description
Save a disk for an active Linux or Windows server.	See "Using i5/OS to back up disks for active integrated Windows servers" on page 154 or "Customizing storage space backup for an active integrated Linux server" on page 186.
Shut down the integrated server to prevent users from updating files during the backup.	See "Starting and stopping integrated servers" on page 190.

4. On the i5/OS command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device . For example, specify /QSYS.LIB/TAP01.DEVD in the *Device* field.
6. If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device.

For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.

7. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc', where stgspc is the name of the network server storage space.

   For example, if the NWSD for the integrated server is named *testserver*, you can save the system and install disks by saving these network server storage spaces:

   - /QFPNWSSTG/*testserver*1
   - /QFPNWSSTG/*testserver*2

8. If you are saving a disk for an active server, specify the following values:

   a. Specify *YES for the **Save active** parameter. This option allows the storage space to be saved while it is still being used the system.

   b. Specify *NWSSTG for the **Save active option** parameter. This option allows network server storage spaces in directory '/QFPNWSSTG' to be saved when they are active.

9. Specify values for any other parameters that you want and press Enter to save the storage space.

10. If you stopped the integrated server, restart it now. See "Starting and stopping integrated servers" on page 190.

Backing up user-defined disks for integrated servers:

Use the Save (SAV) command to back up user-defined disks for your integrated server.

The virtual disks that you create for your integrated servers are in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command..

Note: You can use the same steps for backing up predefined disks (the system disk and the installation disk) and user defined disks.

Note: Treat the network server description, predefined disk drives, and any user-defined disk drives linked to an integrated server as a unit. Save and restore them at the same time. Together they constitute a complete system, and should be treated as such. Otherwise, the integrated server might not start or run correctly.

To save disk drives in a user disk pool (ASP) on i5/OS, do this:

1. Ensure that the auxiliary storage pool (ASP) that contains the disk is varied on.
2. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
3. Select one of the following options.

Option	Description
Save a disk for an active Linux or Windows server.	See "Using i5/OS to back up disks for active integrated Windows servers" on page 154 or "Customizing storage space backup for an active integrated Linux server" on page 186.
Shut down the integrated server to prevent users from updating files during the backup.	See "Starting and stopping integrated servers" on page 190.

4. On the i5/OS command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device . For example, specify /QSYS.LIB/TAP01.DEVD in the *Device* field.
6. If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device.

   For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.

7. In the `Name` field under `Objects:`, specify '/QFPNWSSTG/stgspc', where `stgspc` is the name of the network server storage space.

   For example, if the NWSD for the integrated server is named *testserver*, you can save the system and install disks by saving these network server storage spaces:
   - `/QFPNWSSTG/testserver1`
   - `/QFPNWSSTG/testserver2`

8. If you are saving a disk for an active server, specify the following values:
   a. Specify `*YES` for the **Save active** parameter. This option allows the storage space to be saved while it is still being used the system.
   b. Specify `*NWSSTG` for the **Save active option** parameter. This option allows network server storage spaces in directory '/QFPNWSSTG' to be saved when they are active.

9. Specify values for any other parameters that you want and press `Enter` to save the storage space.

10. If you stopped the integrated server, restart it now. See "Starting and stopping integrated servers" on page 190.

You can find more information about backing up system objects and the appropriate save commands in Backup and recovery.

Saving and restoring user enrollment information for integrated Windows servers:

Use CL commands and APIs to save and restore user profiles and enrollment information for an integrated Windows server

More i5/OS backup and recovery security information may be found in the Backup and Recovery of Security Information section in the Security Reference topic collection.

User profiles may be saved using the SAVSECDTA command or the QSRSAVO API. The i5/OS system value QRETSVRSEC must be set to 1 for integrated Windows server enrollment support. User profiles saved with the SAVSECDTA command or QSRSAVO API may be restored using the RSTUSRPRF command and specifying the parameter USRPRF(*ALL). If the parameter USRPRF(*ALL) is not specified, then user profiles may be restored if the parameter and value SECDTA(*PWDGRP) is specified.

If you save user profiles using the QRSAVO API, and a previous target release value is used, the user profile enrollment definitions will not be restored. After restoring the user profiles, the enrollment needs to be defined. Use System i Navigator or the Change Network Server User Attributes (CHGNWSUSRA) command to define the enrollment.

User profiles need to be saved and restored using the above methods for integrated Windows server enrollment. User profiles saved and restored using other commands or API are not supported for Windows.

What objects to save and their location on i5/OS:

Use these tables to determine which objects need to be saved when you save your integrated server.

Many objects are created as a result of installing integrated servers. Some of these objects are system-related, others user-related. You need to save them all if you want to restore properly. You can save these objects by using options of the i5/OS GO SAVE command. Option 21 saves the entire system. Option 22 saves system data. Option 23 saves all user data (which includes objects in QFPNWSSTG).

If you want to save a particular object, use one of the following tables to see the location of that object on i5/OS and the command to use. The topic Manually saving parts of your system has more information about using the save commands. In addition to saving the entire drive (storage space), you can also save and restore individual files and directories.

| Important: Ensure that the auxiliary storage pool (ASP) is available when you save the data.

Objects to save for all types of integrated servers

Object content	Object name	Object location	Object type	Save command
Integrated server disks	Various	/QFPNWSSTG	Network server storage space	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/*TAP01*.DEVD')
Messages from the integrated server	Various	Various	Message queue	GO SAVE, option 21 or 23 SAVOBJ OBJ(msgq) LIB(qlibrary) DEV(*TAP01*) OBJTYPE(*MSGQ)
i5/OS config objects for integrated servers	Various	QSYS	Device config objects	GO SAVE, option 21, 22, or 23 SAVCFG DEV(TAP01)
i5/OS based and Windows-based IBM iSeries Integrated Server Support code	QNTAP, NTAP and subdirectories	QSYS and /QIBM/ProdData/ NTAP	Library and Directory	SAVLICPGM LICPGM(5761SS1) OPTION(29)
Windows server file shares	QNTC and subdirectories	/QNTC/ servername/ sharename	Directory	GO SAVE, option 21 or 22 SAV
i5/OS TCP interfaces	QATOCIFC	QUSRSYS	physical file **Note:** TCP/IP must be ended when you save the TCP interface physical files.	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
i5/OS TCP interfaces	QATOCLIFC	QUSRSYS	logical file **Note:** TCP/IP must be ended when you save the TCP interface physical files.	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)

Additional objects to save for iSCSI-attached integrated servers

Object content	Object name	Object location	Object type	Save command
iSCSI NWSCFG and associated validation list	Various	QUSRSYS	Network Server Configuration and associated values	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDL)

Object content	Object name	Object location	Object type	Save command
iSCSI path certificate store	nwsdname.*	/QIBM/UserData/ NWSDCert	Certificate store file	GO SAVE, option 21 or 23 SAV OBJ('/QIBM/UserData/NWSDCert/ nwsdname.*')

Restoring the network server description (NWSD) and disks for integrated servers

One method of restoring your integrated server data is to restore the Network Server Description (NWSD) and disk drives that i5/OS associates with that server. It is the fastest method for restoring large amounts of data.

If you used file-level backup, you can also restore specific integrated server files.

When you restore saved objects from i5/OS, you need to be aware of these considerations:

1. Treat a network server description (NWSD), its predefined disk drives (see "Predefined disks and naming conventions for integrated servers" on page 18), and any user-defined disk drives that are linked to it as a unit. Restore them at the same time. Otherwise, the integrated server may not be able to re-establish items such as Windows server File System permissions.

2. To have i5/OS automatically relink restored disk drives in the integrated file system to the appropriate NWSD, restore the NWSD after you restore the disk drives.

3. If you restore an NWSD before restoring the predefined and user-defined disk drives in the integrated file system, you might need to relink those disk drives. The system will attempt to relink the storage space to the NWSD that it was linked to when it was saved. You link the storage by using the Add Network Server Storage Link (ADDNWSSTGL) command for each disk drive that is associated with the NWSD. For example, enter

   ```
   ADDNWSSTGL NWSSTG(Storage_Name) NWSD(NWSD_Name)
   ```

   at the i5/OS command line.

4. For integrated Windows servers, when you restore a domain controller, ensure that the domain database held on the server is synchronized with the other domain controllers.

   Follow normal Windows procedures to do this and refer to documentation from Microsoft as necessary.

5. Restoring NWSD installed on certain hardware types to different hardware type might be restricted. For more information, see "Restoring integrated server NWSDs" on page 201.

Restoring predefined disk drives for integrated servers:

The system disk for the integrated server operating system and the installation disk are stored in the integrated file system. You restore these predefined disk drives just as you do user-defined disks.

To restore disk drives in the integrated file system on i5/OS, use the Restore (RST) command:

1. Ensure that the auxiliary storage pool (ASP) that you are restoring data to is varied on and available.

   By default, a storage space that is being restored will be recreated into the ASP from which it was saved. If you want to restore the data to a different ASP than it was saved from, do the following steps.

   a. Use the Create Network Server Storage Space (CRTNWSSTG) command to create a temporary storage space with the same name as the storage space you are restoring and specify the name of the ASP that you want the data to be restored to.

   b. Use the following steps to restore the data to the temporary storage space. The restore command will replace the data in the temporary storage space with the data that is being restored.

2. If you are restoring from save media, ensure that you have mounted your media.

3. If there are no network server storage spaces that currently exist on the system (none appear when you use the Work With Network Server Storage Space (WRKNWSSTG) command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:

   a. On the i5/OS command line, type `CRTNWSSTG` to create a network server storage space and press F4.

   b. Provide a name for the storage space.

   c. Use the minimal size allowed and specify the appropriate disk pool (ASP).

   d. Press Enter to create the storage space. i5/OS creates the storage space in the /QFPNWSSTG directory.

4. To restore the storage spaces, type `RST` and press F4.

5. In the `Name` field under `Objects:`, specify `'/QFPNWSSTG/`*stgspc*`'`.

   To restore the system drive, use `/QFPNWSSTG/nwsdname1`. To restore the installation drive, use `/QFPNWSSTG/nwsdname2`.

6. If you are restoring a storage space that resided in a user ASP or an independent ASP and was saved on i5/OS V5R4 or earlier releases, you must also specify the UDFS object. Starting with i5/OS V6R1, the UDFS file is not specified on the save or restore commands since it is automatically included with the storage space directory.

   Note: To restore the .UDFS object to an independent disk pool, the disk pool device must be varied on. Specify `dev/`*independent ASP name*`/stgspc.UDFS` where *independent ASP name* is the name of the independent disk pool and *stgspc* is the name of the network server storage space.

7. Specify values for any other parameters that you want and press Enter to restore the storage space.

8. You also need to restore any user defined disk drives that are associated with the server and restore the NWSD. When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restoring user-defined disks for integrated servers:

Do these steps to restore user-defined disks for integrated servers.

1. Ensure that the auxiliary storage pool (ASP) that you are restoring data to is varied on and available.

   By default, a storage space that is being restored will be recreated into the ASP from which it was saved. If you want to restore the data to a different ASP than it was saved from, do the following steps.

   a. Use the Create Network Server Storage Space (CRTNWSSTG) command to create a temporary storage space with the same name as the storage space you are restoring and specify the name of the ASP that you want the data to be restored to.

   b. Use steps 2 to 8 on page 201 to restore the data to the temporary storage space. The restore command replaces the data in the temporary storage space with the data that is being restored.

2. If you are restoring from save media, ensure that you have mounted your media.

3. If there are no network server storage spaces currently exist on the system (none appear when you use the WRKNWSSTG command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:

   a. On the i5/OS command line, type `CRTNWSSTG` to create a network server storage space and press F4.

   b. Provide a name for the storage space.

   c. Use the minimal size allowed and specify the appropriate disk pool (ASP).

   d. Press Enter to create the storage space. i5/OS creates the storage space in the /QFPNWSSTG directory.

4. To restore the storage spaces, type `RST` and press F4.

5. In the `Objects:` name field, specify '/QFPNWSSTG/stgspc', where `stgspc` is the name of the network server storage space.
6. For disks that were saved on i5/OS V5R4 or earlier versions, you must also specify 'dev/QASPnn/stgspc.UDFS', where `stgspc` is the name of the network server storage space.

   Note:

   - To restore the .UDFS object to an independent disk pool, the disk pool device must be varied on. Specify 'dev/independent ASP name/stgspc.UDFS' where `independent ASP name` is the name of the independent disk pool and `stgspc` is the name of the network server storage space.
   - For disks that were saved on V6R1, the UDFS file does not need to be restored.
7. Specify values for any other parameters that you want and press Enter to restore the storage space.
8. You also need to restore any predefined disk drives that are associated with the server and restore the NWSD. See "Restoring integrated server NWSDs." When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restoring integrated server NWSDs:

Use the Restore Configuration (RSTCFG) command to restore a network server description (NWSD) object for an integrated server.

In a disaster recovery situation, you would restore all the configuration objects, one of which is the integrated server's network server description (NWSD). In some situations, for example when you migrate to new integrated server hardware, you need to specifically restore the NWSD. To have i5/OS automatically relink disk drives within the integrated file system to the restored NWSD, restore those disk drives first.

1. On the i5/OS command line, type `RSTCFG` and press F4.
2. In the `Objects` field, specify the name of the NWSD followed by an '*'. This will restore both objects (NWSD, LIND) that have used the standard naming convention in one pass and in the proper sequence.
3. In the `Device` field, specify the device name if you are restoring from media. If you are restoring from a save file, specify *SAVF and identify the name and library for the save file in the appropriate fields.
4. Press Enter to have i5/OS restore the NWSD.
5. When you are done restoring the NWSD and all its associated storage spaces, start the integrated server. See "Starting integrated servers" on page 190.

Restoring NWSH objects for iSCSI-attached integrated servers

Use the Restore Configuration (RSTCFG) command to restore the Network Server Host Adapter (NWSH) object for iSCSI-attached integrated servers.

In a disaster recovery situation, you would restore all the configuration objects, one of which is the network server host adapter (NWSH).

1. On the i5/OS command line, type `RSTCFG` and press F4.
2. In the `Objects` field, specify the name and type of the NWSH.
3. In the `Device` field, specify the device name if you are restoring from media. If you are restoring from a save file, specify *SAVF and identify the name and library for the save file in the appropriate fields.
4. Press Enter to have i5/OS restore the NWSH.

Note:

   1. When you restore an NWSH, you must start the NWSH before you start the integrated server.

Restoring NWSCFG objects and validation lists for iSCSI-attached integrated servers

Use the Restore Object (RSTOBJ) command to restore network server configuration (NWSCFG) objects.

For servers attached by iSCSI HBAs, the additional configuration objects need to be restored to the QUSRSYS library. These include the network server configuration objects (type *NWSCFG) and an associated validation list object (type *VLDL).

Note: The *NWSCFG and *VLDL objects will share the same name.

To restore server storage spaces, you use the Restore Object (RSTOBJ) command:

1. On the i5/OS command line, type RSTOBJ and press F4.
2. If you are restoring from save media, ensure that you have mounted your media.
3. In the **Objects** field, specify the name the network server configuration.
4. In the **Save Library** field, specify QUSRSYS.
5. In the **Device** field, specify either the name of the device that contains the save media or specify *SAVF if you are restoring from a save file.
6. In the **Object** types field, specify both *NWSCFG and *VLDL.
7. If you are restoring from a save file, specify the name and library for the save file.
8. Press Enter to restore the network server configuration and associated validation list.

Viewing or changing integrated server configuration information

Use either System i Navigator or CL commands to change integrated server configuration information.

System i Navigator allows you to view and change most integrated server configuration information.

1. In System i Navigator, select **Integrated Server Administration** → **Servers**.
2. Right-click an integrated server and select **Properties**.

For iSCSI attached servers, additional configuration information can be viewed or changed using System i Navigator as follows:

1. In System i Navigator, select **Integrated Server Administration** → **iSCSI Connections**.
2. Select one of the following folders to show the corresponding list of objects. In the lists, right click an object and select **Properties**.
   - Network Server Host Adapters
   - Remote Systems
   - Service Processors
   - Connection Security

Using the character-based interface you can view and change all integrated server configuration information. The following table summarizes the relevant CL commands.

Table 19. CL commands for changing integrated server configuration information

Tasks	CL Command
Vary on and off integrated servers, check the status of the integrated server and objects that are associated with the network server description (NWSD).	WRKCFGSTS CFGTYPE(*NWS)
Manage your integrated servers.	WRKNWSD
Manage line descriptions that are created when you install the integrated server.	WRKLIND

Table 19. CL commands for changing integrated server configuration information (continued)

Manage TCP/IP interfaces that are created during server installation.	Work with TCP/IP Network Status, option 1: NETSTAT Configure TCP/IP, option 1 CFGTCP
Monitor network server storage spaces.	WRKNWSSTG
Manage network server configurations	WRKNWSCFG
Manage network server host adapters	WRKDEVD DEVD(*NWSH)

Using hot spare integrated server hardware

If there is a problem with your System x or blade hardware, use these steps to change your i5/OS configuration objects to point to new hardware.

Integrated server solutions and storage virtualization provide options that can enable you to enhance the reliability and recoverability of your integrated server environment. This might reduce the total number of systems needed to provide increased availability. It also adds flexibility by enabling one spare server to be used to protect multiple production servers.

the iSCSI local host adapters can also take advantage of hot spare support. See "Using hot spare iSCSI HBAs for integrated servers" on page 204.

Attention: If you have multiple Network Server Description (NWSD) objects configured to use the same iSCSI-attached integrated server hardware, there is a potential compatibility problem when different operating systems are used. This might affect the functionality of the server.

For example, Microsoft Windows and ESX Server might require different versions of iSCSI initiator HBA BIOS and firmware which might not be compatible between the two servers. If you update the i5/OS Integrated Server Support software on an integrated Windows server, the update process might automatically update the iSCSI initiator HBA BIOS and firmware without prompting you.

When you start an integrated server with hot spare hardware, verify that the BIOS and firmware of the iSCSI initiator HBA is compatible with the operating system installed on the integrated server. See IBM

BladeCenter and System x iSCSI HBA update for integration with System i - Servers in the IBM Systems Support Knowledge Base.

Use these tasks to switch to hot spare integrated server hardware.

> **Related concepts**
>
> "Hot spare support for integrated servers" on page 44
> If your integrated server hardware fails, you can configure your integrated server to use replacement hardware with your existing storage spaces.

Switching to hot spare integrated server hardware using System i Navigator

1. Expand **Integrated Server Administration**.
2. Select **Servers**.
3. If the server for which you want to swap hardware is not already shut down:
   a. Right-click the server and select **Shut Down**.
   b. Click **Shut Down** on the confirmation panel.
4. Change the server configuration to point to the hot spare server hardware.
   a. Right-click the server and select **Properties**.
   b. Select the **System** tab and select the new **Remote system configuration name**.

   Click **OK**.
5. To start the integrated server, right-click the server and select **Start**.

Switching to hot spare integrated server hardware using the character-based interface

1. If the server for which you want to swap hardware is not already varied off, use the **Vary Configuration (VRYCFG)** command to vary it off.
2. To change the server configuration to point to the hot spare server hardware, use the **Change Network Server Desc (CHGNWSD)** command. Change the value for the **Remote system name** element of the **Network server configuration (NWSCFG)** parameter to specify the new remote system network server configuration object name.
3. To start the integrated server, use the **Vary Configuration (VRYCFG)** command.

Using hot spare iSCSI HBAs for integrated servers

If there is a problem with your System i iSCSI HBA, use these steps to change your i5/OS configuration objects to point to another iSCSI HBA.

The target iSCSI HBA installed in the System i product provides hot spare capabilities to enhance the reliability and recoverability of the integrated server environment. It also adds flexibility by enabling one "spare" iSCSI local host adapter to be used to protect multiple production iSCSI local host adapters.

Note: This iSCSI local host adapter hot spare capability complements the hot spare capability that is provided for the integrated server hardware. For more information, "Using hot spare integrated server hardware" on page 203.

To hot spare iSCSI local host adapter hardware using System i Navigator, do the following steps:

1. Stop the integrated servers that use the NWSH.
   a. Expand **Integrated Server Administration**.
   b. Select **Servers**.
   c. Right-click the server and select **Shut down**.

      Note: You will need to do this step for each server that uses the NWSH.
   d. Click **Shut down** on the confirmation panel.
2. If the network server host adapter (NWSH) for which you want to swap hardware is not already stopped:
   a. Expand **iSCSI Connections**.
   b. Select **Local Host Adapters**.
   c. Right-click the NWSH and select **Stop**.
   d. Click **Stop** on the confirmation panel.
   e. If active servers are currently using the NWSH, a warning message is shown. Click **Continue**.
3. Change the NWSH to point to the hot spare iSCSI local host adapter:
   a. Right-click the NWSH and select **Properties**.
   b. Select the **General** tab and select a new value for the **Hardware resource** prompt.
   c. Click **OK**.
4. Start the NWSH.
   a. Right-click the NWSH and select **Start**.
5. Start the servers that use the NWSH.
   a. Expand **Integrated Server Administration**.
   b. Select **Servers**.
   c. Right-click the server and select **Start**.

      Note: You will need to do this step for each server that uses the NWSH.

If you are using CL commands, do the following steps.

1. Use the Vary Configuration (VRYCFG) CL command to vary off the NWSDs that use the NWSH.
2. Use the Vary Configuration (VRYCFG) CL command to vary off the NWSH.
3. Use the Change Device Description (NWSH) (CHGDEVNWSH) CL command to change the value for the Resource Name (RSRCNAME) parameter to specify the new hardware resource name.
4. Vary on the NWSH.
5. Vary on the NWSDs that use the NWSH.

Related concepts

"Hot spare support for integrated servers" on page 44
If your integrated server hardware fails, you can configure your integrated server to use replacement hardware with your existing storage spaces.

Managing the iSCSI network for integrated servers

Use these tasks to manage and configure the iSCSI network for iSCSI-attached integrated servers.

Managing iSCSI configuration objects

Use these tasks to manage the objects that control the communication between i5/OS and iSCSI-attached integrated servers.

Managing network server host adapters:

Network server host adapter (NWSH) objects are used to configure the System i target iSCSI host bus adapter (iSCSI HBA). Use these tasks to manage NWSH objects.

An NWSH object must be started (varied on) in order for an integrated server to use the corresponding iSCSI HBA for storage or virtual Ethernet data flows. Stopping (varying off) a NWSH object will make the corresponding iSCSI HBA unavailable to any integrated servers that have storage or virtual Ethernet paths defined to use it. For more information, see "Network server host adapters" on page 42.

Creating a network server host adapter object:

A network server host adapter (NWSH) object must be created for each System i target iSCSI host bus adapter (iSCSI HBA) port.

Note: If you are using the iSCSI Network Planning Guide, use the "i5/OS network server host adapter object work sheet" on page 88 to help you do the following tasks.

Note: The network server host adapter and the remote system configuration define IP address information for opposite sides of the iSCSI network. When connected by a simple, switched network, the following rules apply:

- The SCSI internet addresses in these two objects that are connected by a switch must be in the same subnet. For example, with IP addresses of the form a.b.x.y and 255.255.255.0 subnet masks, a.b.x must be the same value for both objects.
- The LAN internet addresses in these two objects that are connected by a switch must be in the same subnet.
- In the network server host adapter, the gateway elements can be any unassigned IP address in any subnet if you don't have a gateway in your network.
- In the remote system configuration, the gateway elements should be blank if you don't have a gateway in your network.

Creating a network server host adapter (NWSH) object with System i Navigator:

To create a network server host adapter using System i Navigator, follow these steps:

1. Determine the i5/OS hardware resource name that was assigned to iSCSI HBA. Find the Network Server Host Adapter resource with physical location values that match the location of the newly installed iSCSI HBA. Use either of the following methods.

   a. Expand **Configuration and Service** → **Hardware** → **Communications**.

   b. Display the **Properties** of each resource with the description Network Server Host Port.

   c. On the **Physical Location** tab of the property sheet, look at the **Frame ID** and **Card position** values.

2. Expand **Integrated Server Administration**.

3. Expand **iSCSI Connections**.

4. Right-click **Network Server Host Adapters**.

5. Select **New Network Server Host Adapter**.

6. On the **General** tab:

   a. Enter the NWSH device **Name** and **Description**.

   b. Select the **Hardware resource**.

   c. Select the **Object authority**. You can use the default value **Change**.

7. On the **Local (Target) Interface** tab:

   a. Select the cable connection type. If the hardware is physically connected to an Ethernet switch, you can use the default value **Network**.

   b. Enter information to define the SCSI and LAN interface attributes for the iSCSI HBA.

8. Click **OK**.

Creating a network server host adapter object (NWSH) with the character-based interface:

Do these steps to create a Network Server Host Adapter (NWSH) object for an iSCSI HBA using the character-based interface.

1. Determine the hardware resource for the iSCSI HBA.

   a. Run the following command to display a list of the communications resources: WRKHDWRSC *CMN

   b. Use **option 7=Display resource detail** on each resource with the description **Network Server Host Port**.

   c. Examine the **Location:** entry to determine the frame ID and card position values.

   For more information see Work With Hardware Resources (WRKHDWRSC).

2. Type CRTDEVNWSH and press F4 to display the command prompt screen. For more information, see Create Device Desc (NWSH) (CRTDEVNWSH) in the CL command reference topic collection.

3. Fill in the command parameters and press Enter to run the command.

Creating a network server host adapter object based on another one:

Create a new network server host adapter (NWSH) object based on an existing object.

This saves time when some of the new NWSH attributes are the same or similar to the attributes of an existing NWSH.

To create a network server host adapter based on an existing one using System i Navigator, follow these steps:

1. Expand **Integrated Server Administration**.

2. Expand **iSCSI Connections**.

3. Select **Network Server Host Adapters**.

4. Right-click the local host adapter to copy from the list available.

5. Select **New Based On**.

6. Enter the new NWSH device **Name**.
7. Specify any other attributes that should be different from the NWSH that is being copied.
8. Click **OK**.

If you want to use a CL command, see WRKDEVD.

Displaying network server host adapter properties:

A network server host adapter (NWSH) object contains configuration information for an System i target iSCSI host bus adapter (iSCSI HBA).

To display the attributes of a network server host adapter using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Network Server Host Adapters**.
4. Right-click a network server host adapter from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to display.
7. Click **Cancel** to close the panel.

If you want to use CL commands, see DSPDEVD or WRKDEVD.

Changing network server host adapter properties:

A network server host adapter (NWSH) object contains configuration information for an System i target iSCSI host bus adapter (iSCSI HBA).

To change the attributes of a network server host adapter using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Network Server Host Adapters**.
4. Right-click a network server host adapter from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to change.
7. Click **OK** to save any changes.

If you want to use CL commands, see CHGDEVNWSH or WRKDEVD.

Starting a network server host adapter:

Start a network server host adapter (NWSH) object to make an iSCSI HBA port available to an integrated server.

Make sure that you have cabled the System i target iSCSI host bus adapter to the iSCSI network. See the "Cabling the iSCSI network" on page 105

To start a network server host adapter using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Network Server Host Adapters**.
4. Right-click a network server host adapter from the list available.

5. Select **Start**.

If you want to use CL commands, see VRYCFG or WRKCFGSTS.

| If the NWSH does not start or returns a `failed` status, see Troubleshooting ![icon] (www.ibm.com/
| systems/i/bladecenter/troubleshooting.html) web page.

Stopping a network server host adapter:

Stopping (varying off) a network server host adapter (NWSH) object will make the corresponding System
i target iSCSI host bus adapter (iSCSI HBA) unavailable to any integrated servers that have storage or
virtual Ethernet paths defined to use it.

Stopping a NWSH that is being used by active servers can cause the servers to fail if critical storage
resources can no longer be accessed without using the iSCSI HBA that corresponds to the NWSH.
Normally, you should shut down any integrated servers that are using the NWSH before stopping the
NWSH. See "Starting and stopping integrated servers" on page 190 for more information.

To stop a network server host adapter using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
| 3. Select **Network Server Host Adapters**.
| 4. Right-click a network server host adapter from the list available.
5. Select **Stop**.
6. Click **Stop** on the confirmation panel.
7. If active servers are currently using the NWSH, a warning message is shown. Click **Continue**.

If you want to use CL commands, see VRYCFG or WRKCFGSTS.

Deleting a network server host adapter:

To delete a network server host adapter using System i Navigator, follow these steps.
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
| 3. Select **Network Server Host Adapters**.
| 4. Right-click a network server host adapter from the list available.
5. Select **Delete**.
6. Click **Delete** on the confirmation panel.

If you want to use CL commands, see DLTDEVD or WRKDEVD.

Managing remote system network server configurations:

Use these tasks to manage remote system configuration objects for iSCSI-attached integrated servers.

Remote system network server configuration (NWSCFG subtype RMTSYS) objects are used to configure
attributes of an iSCSI attached remote System x or BladeCenter blade server.

The remote system configuration is used to identify the specific System x or BladeCenter hardware that
the integrated server uses. It also defines how the remote system boots and communicates with the
System i hardware. For more information, see "Remote system configuration" on page 42.

Creating a remote system configuration object:

A remote system network server configuration (NWSCFG subtype RMTSYS) object must be created for each System x or blade system that will be used to run an iSCSI-attached integrated server.

Note: If you are using the iSCSI Network Planning Guide, you should use the "i5/OS remote system configuration object work sheet" on page 84 to help you do the following task.

To create a remote system configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Remote Systems**.
4. Select **New Remote System Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Select the **Service processor configuration**.
   - Specify the **Remote system identity**.
   - Select the **Object authority**. You can use the default value **Change**.
6. On the **Remote Interfaces** tab, enter information to define the SCSI and LAN interface attributes for the remote system.
7. Specify values on the **Boot Parameters** and **CHAP Authentication** tabs if wanted.
8. Click **OK**.

Note: The network server host adapter and the remote system configuration define IP address information for opposite sides of the iSCSI network. When connected by a simple, switched network, the following rules apply:
   - The SCSI internet addresses in these two objects that are connected by a switch must be in the same subnet. For example, with IP addresses of the form a.b.x.y and 255.255.255.0 subnet masks, a.b.x must be the same value for both objects.
   - The LAN internet addresses in these two objects that are connected by a switch must be in the same subnet.
   - In the network server host adapter, the gateway elements can be any unassigned IP address in any subnet if you don't have a gateway in your network.
   - In the remote system configuration, the gateway elements should be blank if you don't have a gateway in your network.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Creating a remote system configuration object based on another one:

Create a remote system configuration object based on an existing object.

You can copy an existing remote system network server configuration (NWSCFG subtype RMTSYS) object when creating a new one. This saves time when some of the new remote system configuration attributes are the same or similar to the attributes of an existing remote system configuration.

To create a remote system configuration based on an existing one using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Remote Systems**.

4. Right-click the remote system configuration to copy from the list available.
5. Select **New Based On**.
6. Enter the new remote system configuration **Name**.
7. Specify any other attributes that should be different from the remote system configuration that is being copied.
8. Click **OK**.

Note: There is no equivalent CL command for this task.

Displaying remote system configuration properties:

A remote system network server configuration (NWSCFG subtype RMTSYS) object contains configuration information for an System x or BladeCenter system that will be used to run an iSCSI-attached integrated server.

To display the attributes of a remote system configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Remote Systems**.
4. Right-click a remote system configuration from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to display.
7. Click **OK** to close the panel.

If you want to use CL commands, see DSPNWSCFG or WRKNWSCFG.

Changing remote system configuration properties:

A remote system network server configuration (NWSCFG subtype RMTSYS) object contains configuration information for an System x or BladeCenter system that will be used to run an iSCSI-attached integrated server.

To change the attributes of a remote system configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select**Remote Systems**.
4. Right-click a remote system configuration from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to change.
7. Click **OK** to save any changes.

If you want to use CL commands, see CHGNWSCFG or WRKNWSCFG.

Displaying remote system status:

Do these steps to display the status for the System x or BladeCenter hardware for iSCSI-attached integrated servers.

You can use the status to help you determine if hardware is available for use by an iSCSI-attached integrated server.
1. Expand **Integrated Server Administration**.

2. Expand **iSCSI Connections**.
3. Select **Remote Systems**.
4. Right-click a remote system configuration from the list available.
5. Select **Status**.
6. The status of the remote system hardware is shown.
7. Click **Cancel** to close the panel.

If you want to use a CL command, see WRKNWSCFG.

Deleting a remote system configuration object:

Do these steps to delete remote system configuration objects for integrated servers.
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Remote Systems**.
4. Right-click a remote system configuration from the list available.
5. Select **Delete**.
6. Click **Delete** on the confirmation panel.

If you want to use CL commands, see DLTNWSCFG or WRKNWSCFG.

Managing service processor network server configurations:

Use these tasks to manage service processor configuration objects for integrated servers.

Service processor network server configuration (NWSCFG subtype SRVPRC) objects are used to configure attributes of the service processor or Management Module of each iSCSI attached remote System x or BladeCenter hardware.

The service processor configuration defines attributes that are used to discover and securely connect to the service processor or Management Module on the network. Remote system network server configuration objects contain a reference to the corresponding service processor configuration object that is used to control the remote system hardware. For more information, see "Service processor configuration" on page 43.

Note: A service processor configuration is not needed for each IBM BladeCenter server in a BladeCenter chassis. Just one service processor configuration is needed for the IBM BladeCenter chassis.

Creating a service processor configuration object:

A service processor network server configuration (NWSCFG subtype SRVPRC) object must be created for the service processor or Management Module of each System x or BladeCenter system that is used to run an iSCSI-attached integrated server.

Notes:
1. If you are using the iSCSI Network Planning Guide, you should use the network planning worksheets to help you do the following task.
2. A service processor configuration is not needed for each blade in an IBM BladeCenter chassis. Just one service processor configuration is needed for the BladeCenter chassis.

To create a service processor configuration using System i Navigator , follow these steps:
1. Expand **Integrated Server Administration**.

2. Expand **iSCSI Connections**.
3. Right-click **Service Processors**.
4. Select **New Service Processor Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Specify either a **Host name**, **Internet address**, or **Serial number** to identify the service processor on the network
   - Select the **Object authority**. You can use the default value **Change**.
6. On the **Security** tab, define the type of security to be used when connecting to the service processor.
7. Click **OK**.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Creating a service processor configuration object based on another one:

You can copy an existing service processor network server configuration (NWSCFG subtype SRVPRC) object when creating a new one. This saves time when some of the new service processor configuration attributes are the same or similar to the attributes of an existing service processor configuration.

To create a service processor configuration based on an existing one using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click the service processor configuration to copy from the list available.
5. Select **New Based On**.
6. Enter the new service processor configuration **Name**.
7. Specify any other attributes that should be different from the service processor configuration that is being copied.
8. Click **OK**.

Note: There is no equivalent CL command for this task.

Displaying service processor configuration properties:

A service processor network server configuration (NWSCFG subtype SRVPRC) object contains configuration information for a service processor or Management Module of an System x or BladeCenter system that is used to run an iSCSI-attached integrated server.

To change the attributes of a service processor configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click a service processor configuration from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to display.
7. Click **OK** to close the panel.

If you want to use CL commands, see DSPNWSCFG or WRKNWSCFG.

Changing service processor configuration properties:

A service processor network server configuration (NWSCFG subtype SRVPRC) object contains configuration information for a service processor or Management Module of an System x or BladeCenter system that is used to run an iSCSI attached integrated server.

To change the attributes of a service processor configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click a service processor from the list available.
5. Select **Properties**.
6. Click on the appropriate tabs for the properties you want to change.
7. Click **OK** to save any changes.

If you want to use CL commands, see CHGNWSCFG or WRKNWSCFG.

Initializing a service processor:

A service processor must be initialized with a user name and password before it can be used with an integrated server.

A service processor network server configuration (NWSCFG subtype SRVPRC) object contains configuration information for a service processor or Management Module of an System x or BladeCenter system that is used to run an iSCSI-attached integrated server. The service processor needs to be initialized before it can be used with an integrated server. You might also want to regenerate or synchronize the user and password that are used to secure the service processor connection or change the user or password that are used to connect to the service processor.

To initialize a service processor using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click a service processor configuration from the list available.
5. Select **Initialize**.
6. Choose one of the following options:
   - **Validate service processor user ID and password and store in {NWSCFG NAME}**

     Tip: If you are initializing a configuration object of a service processor for the first time, use this option.
   - **Validate and set user ID and password in a new service processor**
   - **Change service processor user ID and password**
7. Enter the **User** and **Password**, if needed.
8. Click **Initialize** to perform the selected option.

If you want to use CL commands, see INZNWSCFG or WRKNWSCFG.

Deleting a service processor configuration object:

To delete a service processor configuration using System i Navigator, follow these steps.
1. Expand **Integrated Server Administration**.

2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click a service processor configuration from the list available.
5. Select **Delete**.
6. Click **Delete** on the confirmation panel.

If you want to use CL commands, see DLTNWSCFG or WRKNWSCFG.

Managing connection security network server configurations:

Connection security network server configuration (NWSCFG subtype CNNSEC) objects are used by the System i product to connect to the integrated server hardware.

For more information, see "Connection security configuration" on page 43.

Creating a connection security configuration object:

Do these steps to create a connection security configuration object for an integrated server.

Notes:

1. If you are using the "i5/OS connection security configuration object work sheet" on page 89, you should use the network planning worksheets to help you do the following task.

To create a connection security configuration using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Connection Security**.
4. Select **New Connection Security Configuration**.
5. On the **General** tab:
   - Enter the **Name** and **Description**.
   - Select the **Object authority**. You can use the default value **Change**.
6. Click **OK**.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Creating a connection security configuration object based on another one:

You can copy an existing connection security network server configuration (NWSCFG subtype CNNSEC) object when creating a new one. This saves time when some of the new connection security configuration attributes are the same or similar to the attributes of an existing connection security configuration.

To create a connection security configuration based on an existing one using System i Navigator, follow these steps:
1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Connection Security**.
4. Right-click the connection security configuration to copy from the list available.
5. Select **New Based On**.
6. Enter the new connection security configuration **Name**.
7. Specify any other attributes that should be different from the connection security configuration that is being copied.

| 8. Click **OK**.

| **Note:** There is no equivalent CL command for this task.

| *Displaying connection security configuration object properties:*

| Do these steps to display the properties of a connection security configuration object for an
| iSCSI-attached integrated server.
| 1. Expand **Integrated Server Administration**.
| 2. Expand **iSCSI Connections**.
| 3. **Connection Security**.
| 4. Right-click a connection security configuration object from the list available.
| 5. Select **Properties**.
| 6. Click on the appropriate tabs for the properties you want to display.
| 7. Click **OK** to close the panel.

| If you want to use CL commands, see DSPNWSCFG or WRKNWSCFG.

| *Changing connection security configuration properties:*

| Do these steps to change the properties of a connection security configuration object for an integrated
| server.
| 1. Expand **Integrated Server Administration**.
| 2. Expand **iSCSI Connections**.
| 3. Select **Connection Security**.
| 4. **Right-click** a connection security configuration object from the list available.
| 5. Select **Properties**.
| 6. Click on the appropriate tabs for the properties you want to change.
| 7. Click **OK** to save any changes.

| If you want to use CL commands, see CHGNWSCFG or WRKNWSCFG.

| *Deleting a connection security configuration object:*

| Do these steps to delete a connection security configuration object for an integrated server.
| 1. Expand **Integrated Server Administration**.
| 2. Expand **iSCSI Connections**.
| 3. Select **Connection Security**.
| 4. Right-click a connection security configuration object from the list available.
| 5. Select **Delete**.
| 6. Click **Delete** on the confirmation panel.

| If you want to use CL commands, see DLTNWSCFG or WRKNWSCFG.

Configuring security between i5/OS and integrated servers

Use these tasks to manage security for integrated servers.

Configuring CHAP for integrated servers:

Use these tasks to configure the challenge handshake authentication protocol (CHAP) for the remote
system configuration for an iSCSI-attached integrated server.

You must have security administrator (*SECADM) special authority to create, change, or display CHAP information.

> **Related information**
>
> ➡ iSCSI Initiator Hardware Configuration

Configuring target CHAP for iSCSI-attached integrated servers:

Do these steps to configure the initiator to authenticate the target.

1. Vary off the network server description (NWSD) for your integrated server.
2. Expand **Integrated Server Administration** → **iSCSI Connections** → **Remote system connections**.
3. Right-click the remote system configuration for the integrated server and select **Properties**.
4. On the **CHAP Authentication** tab, click **Enable Challenge Handshake Authentication Protocol (CHAP)** to enable CHAP.
5. Specify information for **Target CHAP Values**.
   a. Select an option for **CHAP name**.
   b. Select **Generate CHAP secret once** or select **Specific CHAP secret** and specify a CHAP secret.
6. Configure target CHAP on the iSCSI-attached server. See the Configuring target CHAP task in the
   iSCSI Initiator Hardware Configuration 📖 document.

Configuring initiator CHAP for iSCSI-attached integrated servers:

If you have configured a target CHAP, you can also use these steps to configure initiator CHAP for your iSCSI-attached integrated server.

1. Vary off the NWSD for your integrated server.
2. From System i Navigator, expand **Integrated Server Administration** → **iSCSI Connections** → **Remote systems**.
3. Right-click the remote system configuration for the integrated server and select **Properties**.
4. On the **CHAP Authentication** tab, click **Enable Challenge Handshake Authentication Protocol (CHAP)** to enable CHAP.
5. Specify information for **Initiator CHAP Values**.
   a. Select an option for **CHAP name**.
   b. Select **Generate CHAP secret once** or select **Specific CHAP secret** and specify a CHAP secret.
6. Configure initiator CHAP on the iSCSI-attached server. See the Configuring initiator CHAP task in the
   iSCSI Initiator Hardware Configuration 📖 document.

Changing a service processor password for an integrated server:

Do these steps to change the service processor password for an iSCSI-attached integrated server.

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Service Processors**.
4. Right-click a service processor configuration from the list available.
5. Select **Initialize**.
6. Select the **Change service processor user ID and password** option.
7. Specify the new **User**, **Password**, and **Confirm new password values**.
8. Click **Initialize** to perform the operation.

Configuring a firewall to allow integrated server connections:

Use this information to configure a firewall to allow integrated server connections.

If there is a firewall between the System i and the iSCSI network for the integrated server, then the firewall must be configured to allow incoming iSCSI and virtual Ethernet traffic to pass.

The values that affect firewall configuration are listed below:

For storage paths and virtual Ethernet connections protected by the firewall:

Remote IP address
> Use the procedure described in "Displaying remote system configuration properties" on page 210 to display the properties of the remote system configuration for the server. Go to the **Network Interfaces** tab and note the **SCSI Internet Address** and **LAN Internet Address** values.

- **Local IP address and TCP port:** Use the procedure described in "Displaying network server host adapter properties" on page 207 to display the properties of the network server host adapter (NWSH). Go to the **Local Interfaces** tab to see information that is used by the NWSH. Record the following values:
  - Local SCSI interface: Internet address
  - Local SCSI interface: TCP port
  - Local LAN interface: Internet address
  - Local LAN interface: Base virtual Ethernet port
  - Local LAN interface: Upper virtual Ethernet port

  > **Note:** Virtual Ethernet traffic is encapsulated in UDP packets. Each virtual Ethernet adapter is automatically assigned a UDP port from a range that begins at the specified base virtual Ethernet port number and ends at the base virtual Ethernet port number plus the number of configured virtual Ethernet adapters. Each virtual Ethernet adapter is also has a UDP port assigned at the Windows server. UDP ports for virtual Ethernet are normally automatically allocated by Windows. If you want to override automatic allocation, you can manually allocate a UDP port by performing the following steps at the Windows console.

  1. Navigate to the **Network Connections** Window.
  2. Double-click the **IBM i5/OS Virtual Ethernet x** adapter that you want to configure.
  3. Click **Properties**.
  4. Click **Configure**.
  5. Click **Advanced**.
  6. Click **Initiator LAN UDP Port**.
  7. Enter the UDP port that you want the virtual Ethernet adapter to use.

- **TCP ports associated with all Local IP addresses:**

  Using System i Navigator:

  1. Expand **Integrated Server Administration**.
  2. Select **Servers**.
  3. Right-click the server from the list available and select **Properties**.
  4. Go to the **System** tab and click the **Advanced** button.
  5. Note the following values:
     - **Virtual Ethernet control port**

Configuring high availability for integrated servers
Use these tasks to configure high availability iSCSI-attached integrated servers.

> **Related concepts**

"High availability concepts for integrated servers" on page 44
Integrated servers can be made highly available through hot spare hardware, clustering, multipath
storage connections, or by configuring the integrated server as a switchable device.

Configuring an integrated server as a System i switchable device

Integrated servers can be configured to work with i5/OS high availability technologies.

Integrated servers can be included in i5/OS clustering or cross-site mirroring. If you configure cross-site
mirroring, you need to configure all of the integrated server hardware, disks, and software objects. See
"What objects to save and their location on i5/OS" on page 197 for a list of objects and disks to include.

For more information, see the High availability topic collection.

Managing iSCSI adapters

Use this information to anage and configure how the iSCSI initiator and target adapters communicate on
the iSCSI network.

Managing iSCSI initiator hardware:

A configuration utility is used to set up the iSCSI initiator hardware in the System x or blade server.

Refer to the iSCSI Initiator Hardware Configuration manual for the following tasks:
* Restoring factory defaults for an iSCSI initiator.
* Resetting cached iSCSI initiator configuration information.
* Verifying the iSCSI connection using ping.
* Changing the iSCSI initiator CHAP secret.
* Changing the iSCSI initiator maximum transmission unit (MTU).
* Updating iSCSI initiator firmware

   Related information

   ➡ iSCSI Initiator Hardware Configuration

Removing or replacing a blade or System x iSCSI initiator for an integrated server:

Use these tasks to uninstall or replace the iSCSI initiator for an integrated server.

Stopping the iSCSI integrated System x or blade server:

Do these steps to stop an integrated server.

To stop the iSCSI-attached integrated server, see "Starting and stopping integrated servers" on page 190

Removing the System x or blade system iSCSI initiator:

After the iSCSI-attached integrated server has been stopped, removing the iSCSI initiator from a System x
or blade system is the same as removing any other adapter from either server. See the documentation for
your System x or blade system and complete the configuration.

Note: You must label and disconnect any Ethernet cables plugged into the System x iSCSI initiator before
removing the iSCSI initiator. You do not have to disconnect any Ethernet cables from the blade
system because these connections are made through the BladeCenter midplane.

Replacing a System x or blade server iSCSI initiator for an integrated server:

Do these steps to replace an iSCSI initiator for an integrated server.

Select the System x or blade replacement from the following list:

Important: In either procedure, note the MAC addresses from the sticker on the iSCSI initiator in the *iSCSI Network Planning Worksheets*.

- System x: refer to the System x documentation to perform this task. Any Ethernet cables that are connected to the original iSCSI initiator need to be reconnected after the replacement iSCSI initiator is installed.
- Blade system: refer to the blade system documentation to perform this task.

  Related tasks
  "Completing the replacement iSCSI initiator configuration" on page 220
  After you have updated the *iSCSI Network Planning Worksheets* with the new information from the procedures Replacing a System X or blade server iSCSI and Collecting and updating remote system network server configuration, you can complete the configuration of the iSCSI initiator by following the procedure in Installing and configuring the iSCSI initiator.

Configuring the replacement iSCSI initiator:

Do these tasks to configure a new iSCSI initiator and i5/OS configuration objects for an integrated server.

Collecting and updating remote system network server configuration object information:

Use this task to update the remote system network server configuration object information after you reinstall the adapter.

To complete the following procedure, you need the "iSCSI network planning work sheets" on page 81. If you cannot locate these work sheets, you have to print and fill in a new set. For instructions, see "iSCSI Network Planning Guide" on page 62.

Remember: Ensure that you record the Media Access Control (MAC) addresses from the new iSCSI initiator in items RS13 and RS17 of the planning work sheets.

If you have a copy of the work sheets that you completed during the initial installation of the iSCSI-attached server, go to steps 12 on page 220 and 14 on page 220 to update the work sheet items RS13 and RS17 with the new iSCSI initiator MAC addresses. If you have not completed "iSCSI network planning work sheets" on page 81, do these steps to record the information for the current configuration.

1. From System i Navigator, expand **Integrated Server Administration** → **iSCSI Connections** → **Remote Systems**.

2. Right-click the remote system configuration object and select **Properties**.

3. Click the **Boot Parameters** tab.

4. Record in the i5/OS remote system configuration object work sheet (item **RS6**) if either **Dynamically delivered to remote system via DHCP** or **Manually configured on remote system options** is indicated.

5. Click the **CHAP Authentication** tab.

6. If **Enable Challenge Handshake Authentication Protocol (CHAP)** is not selected, check **Disabled** for i5/OS remote system configuration object work sheet items **RS7** and **RS10** and continue to step 10.

7. Record the target CHAP values.

   a. Check **Use the following values for CHAP authentication** in i5/OS remote system configuration object work sheet item **RS7**.

   b. Record the setting for **CHAP name** in i5/OS remote system configuration object work sheet item **RS8**.

   c. Record the value for **CHAP secret** in i5/OS remote system configuration object work sheet item **RS9**.

8. If **Enable bidirectional CHAP** is selected, record the initiator CHAP information.

   a. Record the setting for **CHAP name** in i5/OS remote system configuration object work sheet item **RS11**.

   b. Record the setting for **CHAP secret** in i5/OS remote system configuration object work sheet item **RS12**.

9. Click the **Network Interfaces** tab.

10. Select the interface you are configuring and click the **Properties** tab.

11. Change the value for **Remote SCSI interface: Local adapter (MAC) address** to the value copied from the adapter and entered in the i5/OS remote system configuration object work sheet (item **RS13**).

12. If the **Manually configured on remote system** option is selected, note the values for **Remote SCSI interface: Internet address** (item **RS14**), **Remote SCSI interface: Subnet mask** (item **RS15**) and **Specific iSCSI qualified name** (item **CQ6**) in the i5/OS remote system configuration object work sheet.

13. Change the value for **Remote LAN interface: Local adapter (MAC) address** to the value that is copied from the sticker on the adapter and that is entered in the i5/OS remote system configuration object work sheet (item **RS17**).

   Note: For an iSCSI HBA, the LAN interface MAC address is different from the SCSI interface MAC address. The LAN interface MAC address is labeled **TOE** on the sticker. For an Ethernet Network Interface Card (NIC), the LAN interface MAC address is the same as the SCSI interface MAC address.

14. If the **Manually configured on remote system** option is selected, note the values for **Remote LAN interface: Internet address** (item **RS18**) and **Remote LAN interface: Subnet mask** (item **RS19**) in the i5/OS remote system configuration object work sheet.

15. Click **OK** to complete the update.

16. Click **OK** to close the window.

17. Click the **Storage Paths** tab on the network server description properties window.

18. Select the storage path with the desired NWSH name and click the **Properties** button.

19. If the **Manually configured on remote system** option is selected, record the value for **iSCSI qualified name (IQN)** in the iSCSI initiator work sheet (item **CQ6**).

Related tasks

"Completing the replacement iSCSI initiator configuration"
After you have updated the *iSCSI Network Planning Worksheets* with the new information from the procedures Replacing a System X or blade server iSCSI and Collecting and updating remote system network server configuration, you can complete the configuration of the iSCSI initiator by following the procedure in Installing and configuring the iSCSI initiator.

Related reference

"i5/OS remote system configuration object work sheet" on page 84
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

"iSCSI initiator work sheet" on page 86
Select the parameters to configure the iSCSI initiator in the System x or blade hardware.

Completing the replacement iSCSI initiator configuration:

After you have updated the *iSCSI Network Planning Worksheets* with the new information from the procedures Replacing a System X or blade server iSCSI and Collecting and updating remote system network server configuration, you can complete the configuration of the iSCSI initiator by following the procedure in Installing and configuring the iSCSI initiator.

Related tasks

"Replacing a System x or blade server iSCSI initiator for an integrated server" on page 218
Do these steps to replace an iSCSI initiator for an integrated server.

"Collecting and updating remote system network server configuration object information" on page 219
Use this task to update the remote system network server configuration object information after you reinstall the adapter.

"Installing and configuring the iSCSI initiator" on page 105
Complete these tasks to install a new iSCSI initiator in the System x or blade product and configure the initiator to communicate on the iSCSI network.

Configuring the integrated server Management Module or RSAII using the Web interface:

Do these steps to configure the management module or remote supervisor adapter II (RSA II) service processor for an integrated server.

You can use the Remote Supervisor Adaptor II (RSA II) or Management Module web interface to do the following tasks:
- Change the service processor IP host name.
- Manage certificates for the manual security setting on the service processor configuration.
  - Perform a certificate signing request to obtain a certificate from a certificate authority such as Verisign.
  - Import the certificate into the service processor.
- Configure static IP addresses.
- Update RSA II firmware.

Attention: If you use the RSA II web interface to change the user name or password for the service processor, you must synchronize the password in your i5/OS service processor configuration object with the new password. If you do not synchronize the passwords, you cannot connect to the service processor because the i5/OS objects contains the old user name and password. See "Initializing a service processor" on page 213.

Connecting to the service processor:

1. Optional: If you need to connect the browser to the RSA II through a router, first configure the IP address of the RSA II using the BIOS interface.
2. Enter the user name and password for the RSA II or Management Module.

   The RSA II or Management Module comes with a default user name of USERID and default password of PASSW0RD (0 = zero).

   The RSA II or Management Module factory defaults are set as follows: DHCP "Try DHCP. If it fails, use static IP config." Static IP address of 192.168.70.125. Note that this is a non-routable address. This means that you cannot connect a browser through a router to the RSA II or Management Module using this address. You might be able to connect a browser to the RSA II or Management Module with the default IP address through most (but not all) brands of switches, and most Ethernet hubs.

Managing the service processor:

After you have connected the browser to the RSA II/Management Module's Web interface, you can do the following tasks:
- Select "Network Interfaces" under ASM control. Enter the hostname. It is recommended to set the host name field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name asmcard1.us.company.com, the nonqualified IP host name is asmcard1.
- Select **Login Profiles** under ASM control to change user name and passwords. This is required for Manual security mode.

- Select **Firmware Update** under Tasks to update the RSA II or Management Module firmware to the latest level.

Alternate method to update Remote Supervisor Adapter II network configuration to defaults:

Use this method to set RSA II network settings when the defaults are no longer set. This method does not work if the RSA II does not have firmware compatible with the System x product that it is installed in. Perform this procedure on the System x console.

1. Turn on the System x product. Refer to the system documentation to complete this step.
2. When the IBM eServer logo appears on the display, press F1 to go to setup.
3. Highlight **Advanced Setup** using the up or down arrow keys and press **Enter** to select.
4. Highlight **RSA II Settings** (This setting is available only when RSA II hardware is installed.) using the up or down arrow keys and press **Enter** to select.
5. Highlight **DHCP Control** using the up or down arrow keys and use the left or right arrow keys to change the value to **Use Static IP**.
6. Highlight **Static IP Address** using the up or down arrow keys and use the backspace key to position the cursor and enter the IP address 192.168.070.125.
7. Highlight **Subnet Mask** using the up or down arrow keys and use the backspace key to position the cursor and enter 255.255.255.000.
8. Highlight **Gateway** using the up or down arrow keys and use the backspace key to position the cursor and enter 192.168.070.001.
9. Highlight **OS USB Selection** using the up or down arrow keys and use the right or left arrow keys to change the value to **Other OS**.
10. Highlight **Save Values and Reboot RSA II** using the up or down arrow keys and press **Enter** to select and perform the action. A screen displays confirming the action.
11. Press **Esc** two times to return to the main setup menu.

Managing iSCSI target and initiator usage for integrated servers:

Use these tasks to manage the iSCSI network.

Sharing an iSCSI target among multiple integrated servers:

A single iSCSI target installed in the System i product might be able to handle the workload for several servers that do not require high bandwidth for the SCSI and virtual Ethernet LAN traffic. For example, you can share an iSCSI target among several development and test servers if their workload is light.

There are limits to the number of storage and virtual Ethernet paths that an iSCSI target can support. Each active server storage path uses a file server resource in the network server host adapter (NWSH) object that corresponds to the iSCSI target. Likewise, each active server virtual Ethernet path uses a virtual Ethernet resource in the NWSH object. There is a limit to the number of file servers and virtual Ethernet resources that a NWSH can support. This restriction limits how many active servers can use the NWSH.

To see the NWSH file server and virtual Ethernet resource limits, follow these steps:
1. From System i Navigator, expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.
4. Right-click a NWSH from the list available.
5. Select **Properties**.
6. Click the **Resource Usage** tab.

| The table shows the active servers that are currently using the NWSH and the file server and virtual
| Ethernet resources that they are currently using. Below the table it shows how many file server and
| virtual Ethernet resources are still available for use by inactive servers and the total number of file
| server and virtual Ethernet resources that the NWSH supports.
| 7. Click **Cancel** on the NWSH properties panel to close the panel.

| If you want to use a CL command, see the WRKDEVD or DSPDEVD commands.

| There is also a practical limit to the number of servers that an iSCSI target can support. The practical
| limit is determined by the available iSCSI target bandwidth and the workload that is run through the
| iSCSI target. The practical limit determines how many hosted systems the iSCSI target can support before
| the limits for the file server and virtual Ethernet resource are reached. The practical limits depend on
| your server configurations and workloads.

| *Sharing iSCSI network traffic between multiple iSCSI targets:*

| You can segment the network traffic by identifying which virtual disks and virtual Ethernet LANs require
| high bandwidth and which ones do not. For example, you can dedicate an iSCSI target to a disk that
| needs high bandwidth and share another iSCSI target among disks or other servers that do not require
| high bandwidth.

| The way you spread a server's SCSI and virtual Ethernet workload over multiple iSCSI targets is to
| define multiple storage or virtual Ethernet paths in the network server description (NWSD) and assign
| which virtual disks and which virtual Ethernets use each path.

| To define additional storage paths, follow these steps:
| 1. Shut down the server (see "Starting and stopping integrated servers" on page 190).
| 2. From System i Navigator, expand **Integrated Server Administration**.
| 3. Expand **Servers**.
| 4. Right-click a server from the list available.
| 5. Select **Properties**.
| 6. Click the **Storage Paths** tab.
| 7. Click the **Add** button to define a new storage path.
| 8. Select the network server host adapter (NWSH) that corresponds to the iSCSI target that you want to
| use for the storage path.
| 9. Click **OK** to add the storage path to the server properties panel.
| 10. Make note of the path number that is assigned to the new path. The path number is used to identify
| this path when linking disks later on.
| 11. On the server properties panel, click **OK** to save the new storage path in the NWSD.

| If you want to use a CL command, see the STGPTH keyword on the CHGNWSD command.

| Now that the new storage path is defined, you need to re-link one or more of the server's virtual disks to
| use the new storage path. First unlink the disk (see "Unlinking integrated server disks" on page 161).
| Then link the disk to the server again (see "Linking disks to integrated servers" on page 232), using the
| new storage path number that was added above.

| To define additional virtual Ethernet paths, follow these steps:
| 1. Shut down the server (see "Starting and stopping integrated servers" on page 190).
| 2. From System i Navigator, expand **Integrated Server AdministrationServers**.
| 3. Right-click a server from the list available.
| 4. Select **Properties**.

5. Click the **Virtual Ethernets** tab.

6. Select the virtual Ethernet port that you want to use a new path for and click the **Properties** button.

7. Select the NWSH that you want to use for the virtual Ethernet port.

8. Click **OK** to update the virtual Ethernet port information about the server properties panel. The virtual Ethernet path for the port is implicitly updated as well.

9. On the server properties panel, click **OK** to save the changes in the NWSD.

If you want to use a CL command, see the VRTETHPTH keyword on the CHGNWSD command.

Managing iSCSI initiator allocation at the Windows side of the iSCSI network:

Use these tasks to configure iSCSI initiator ports and virtual Ethernet information from the Windows operating system.

An iSCSI-attached integrated Windows server can use multiple physical iSCSI initiator ports. An iSCSI initiator port can carry traffic for i5/OS storage paths and virtual Ethernet networks. Several factors influence the nature of the traffic that flows through each iSCSI initiator port for the Windows server.

IP addresses

iSCSI initiator ports can have a SCSI IP address, a LAN IP address, or both. A port with a SCSI IP address can carry storage traffic. A port with a LAN IP address can carry virtual Ethernet traffic. A port with both addresses can carry both types of traffic.

Boot storage configuration

You select the iSCSI initiator port that is used to boot Windows with the iSCSI initiator configuration utility. After the Windows Server has started, the selected iSCSI initiator port continues to provide a connection to the i5/OS storage path that corresponds to the system drive.

Automatic allocation of iSCSI initiator ports to virtual Ethernet and non-boot storage paths

IBM i5/OS Integrated Server Support includes several applications for Microsoft Windows. These applications automatically read the i5/OS objects that contain the server configuration information. These programs automatically allocate the iSCSI initiator ports to virtual Ethernet and non-boot storage paths.

The following conditions will cause Virtual Ethernet ports to be automatically allocated:
- You start the server (vary on the NWSD).
- You restart the Windows server.
- You restart the **IBM i5/OS Virtual Ethernet Manager service** from **Control Panel** → **Administrative Tools** → **Services**.
- You run the qvndvimr /restart command at a Windows command prompt.
- A connection fails. In this case, the affected virtual Ethernet connections are automatically assigned to a different iSCSI initiator port at the hosted system if one initiator is available. Virtual Ethernet uses the failed connection again after the cause of the failure is corrected and one of these conditions for virtual Ethernet automatic allocation occurs.

Any of the following things cause non-boot storage path automatic allocation to occur:
- You start the server (vary on the NWSD).
- You restart Windows.
- You restart the **IBM i5/OS Manager** service from **Control Panel**→**Administrative Tools**→**Services**.
- You run the lvmaster /restart command at a Windows command prompt.

Manual allocation of storage to a physical iSCSI initiator port

You can manually allocate storage to a physical iSCSI initiator port. You must have a Windows server with multiple iSCSI initiator ports and an i5/OS system with multiple iSCSI targets. This task affects iSCSI port usage at both sides of the iSCSI network.

Run the qvnimap command at the integrated server console to generate a Storage Device Connection table. In the table look for all rows that show a physical connection to the desired iSCSI initiator port at the Windows server. Note the path numbers in these rows. If there is more than one path number, decide which one you want to use. Then relink the storage space to that path.

Manual allocation of a virtual Ethernet adapter to a physical iSCSI initiator port

If you want to override automatic allocation for virtual Ethernet, you can manually allocate an iSCSI initiator port. At the integrated server console, complete these steps:

1. Navigate to the **Network Connections** window.
2. Double-click the **IBM i5/OS Virtual Ethernet x** adapter that you want to configure.
3. Click **Properties**.
4. Click **Configure**.
5. Click **Advanced**.
6. Click **Initiator LAN IP Address**.
7. In Windows, enter the IP address of the iSCSI initiator port that you want the virtual Ethernet adapter to use for its physical connection.

You can use the qvnimap and qvndvimr commands at the Windows console to view more information about iSCSI initiator allocation.

Related tasks

"Viewing iSCSI initiator allocation for an integrated Windows server"
You can use the qvnimap command to display how iSCSI initiators are used for a Windows server.

"Displaying information about virtual Ethernet adapters" on page 226
To display information about virtual Ethernet adapters for a particular Windows server such as UDP port numbers, enter qvndvimr /status at a Windows command prompt on that server.

Viewing iSCSI initiator allocation for an integrated Windows server:

You can use the qvnimap command to display how iSCSI initiators are used for a Windows server.

Make sure that you have administrator privileges on the integrated server and enter **qvnimap** at a Windows command prompt on the integrated server console. The output consists of several tables. You can also enter **qvnimap /?** for a list of options that you can use with the qvnimap command.

There are two connection tables, one for storage devices and one for virtual Ethernet networks. In connection tables, a plus sign (+) represents a physical connection that is used by the storage device and path or that is used by the virtual Ethernet described to the left of the plus sign (+). The two endpoints of the physical connection are the initiator port identified above the plus sign (+), and the target NWSH identified to the immediate left of the plus sign (+). By looking for all occurrences of the plus sign (+) in a column, you can determine how a particular initiator port is being used.

The Storage Device Connections table also shows relationships between storage devices and paths. If you have not assigned a drive letter to a storage space in Microsoft Windows, a blank appears in the drive column. If a storage space is being used to provide multiple drives, there is a row for each drive. Logically connected storage paths that are not currently used by any storage device are displayed with a disk value of *None*.

In addition to the connection tables, there are other tables that provide details about the following information:

- iSCSI initiator ports, identified by names such as P1 and P2
- Windows-side Virtual Ethernet port, identified by names such as VRTETHPTP and VRTETH0
- iSCSI targets, identified by NWSH name

If you do not have administrator privileges on the Windows server, you might see some incorrect or missing information such as these:

- "Unknown" for an entire column of a table
- "Unknown" for all virtual Ethernet information
- "RMTIFC MAC address not found" for all configured SCSI MAC addresses

Errors might appear in the output of the qvnimap command.

Table 20. Errors that might occur when you run the qvnimap command and some possible causes

Condition	Possible causes
RMTIFC MAC address not found	• MAC address in the remote system configuration object is not correct. • Corresponding SCSI or LAN driver is disabled or is not installed.
Not operational	The corresponding LAN or virtual Ethernet driver might be disabled or is not installed.
Link down	On a physical port, such as P1, this might be a cable or switch problem. On a virtual Ethernet port, such as VRTETHPTP, the following situation might cause the error: • A physical port, network, or network server host adapter (NWSH) problem occurs. • The target and initiator might be on different LAN IP subnets without a router. • The iSeries Manager, Shutdown Manager, or Virtual Ethernet Manager service might not be started in Windows.

Related tasks

"Managing iSCSI initiator allocation at the Windows side of the iSCSI network" on page 224
Use these tasks to configure iSCSI initiator ports and virtual Ethernet information from the Windows operating system.

Displaying information about virtual Ethernet adapters:

To display information about virtual Ethernet adapters for a particular Windows server such as UDP port numbers, enter qvndvimr /status at a Windows command prompt on that server.

Related tasks

"Managing iSCSI initiator allocation at the Windows side of the iSCSI network" on page 224
Use these tasks to configure iSCSI initiator ports and virtual Ethernet information from the Windows operating system.

Configuring virtual Ethernet for applications that support frame sizes larger that 1500 bytes:

Do these steps to configure virtual Ethernet to support jumbo frames for an integrated server.

For information about configuring the virtual Ethernet frame size for your iSCSI HBAs, see the Changing the iSCSI initiator MTU task in the iSCSI Initiator Hardware Configuration mannual.

Related configuration items listed below should be left at their default values:

- For Windows virtual Ethernet adapters, Maximum Frame Size defaults to Auto. This value causes virtual Ethernet to calculate a maximum frame size based on the Ethernet Frame Size of the iSCSI HBA port used. See "Managing iSCSI initiator allocation at the Windows side of the iSCSI network" on page 224 for an explanation of iSCSI HBA port useage.
- In i5/OS virtual Ethernet line descriptions, **Maximum frame size (MAXFRAME)** defaults to **8996**.
- In i5/OS TCP/IP interfaces for virtual Ethernet, **Maximum transmission unit (MTU)** defaults to ***LIND**.

   Related concepts

   "Maximum transmission unit considerations for iSCSI network" on page 39
   The default MTU size for iSCSI-attached integrated servers is 1500 bytes. You can configure the network to use other Ethernet frame sizes to adjust network performance.

Configuring virtual Ethernet for iSCSI networks that have a maximum frame size that is less than 1500 bytes:

Do these steps to configure virtual Ethernet for iSCSI networks that have a maximum frame size that is less than 1500 bytes.

At the Windows console, perform the following steps:

1. Navigate to the **Network Connections Window**.
2. Double click **the IBM i5/OS Virtual Ethernet x** adapter that will use an iSCSI HBA connected to the iSCSI network having a maximum frame size less than 1500 bytes.
3. Click on **Properties**.
4. Click on **Configure**.
5. Click on **Advanced**.
6. Click on **Maximum Frame Size**.
7. Select a value that is as large as possible without exceeding the maximum frame size of the iSCSI network.

   Related concepts

   "Maximum transmission unit considerations for iSCSI network" on page 39
   The default MTU size for iSCSI-attached integrated servers is 1500 bytes. You can configure the network to use other Ethernet frame sizes to adjust network performance.

Configuring virtual Ethernet to support non-TCP applications that do not negotiate MTU:

Do these steps to configure virtual Ethernet for an integrated server to support applications that do not use TCP and do not negotiate maximum transmission unit (MTU).

Note: To avoid impacts to normal applications that negotiate MTU, before performing this procedure, define a separate virtual Ethernet network or separate IP addresses for the application that does not negotiate MTU.

1. Do one of the following steps:
   a. If all Windows endpoints will use an iSCSI network having a maximum frame size of 1500 bytes or greater, configure the iSCSI HBA Ethernet frame size at all Windows endpoints to a value as large as possible without exceeding the maximum frame size of the most constrained iSCSI network.
   b. If any Windows endpoint will use an iSCSI network having a maximum frame size less than 1500 bytes, configure the virtual Ethernet Maximum frame size at all Windows endpoints to a value as large as possible without exceeding the maximum frame size of the most constrained iSCSI network.
2. At other endpoints, set the MTU to a value determined by subtracting 116 from the smaller of the Windows iSCSI HBA Ethernet frame size and the virtual Ethernet Maximum frame size. For i5/OS endpoints, you can accomplish this by performing the following procedure:

a. From System i Navigator, expand **Network → TCP/IP Configuration → IPv4 → Interfaces**.

b. Right-click the interface with the IP address and line description name of interest and select **Properties**.

c. On the **Advanced** tabbed page, type the calculated value in the Maximum transmission unit field and click **OK** to save the change.

> **Note:** If you want to use the command line interface, use CFGTCP and select option 1, Work with TCP/IP interfaces.

Related concepts

"Maximum transmission unit considerations for iSCSI network" on page 39
The default MTU size for iSCSI-attached integrated servers is 1500 bytes. You can configure the network to use other Ethernet frame sizes to adjust network performance.

Configuring initiator system discovery and management

Use the information from the i5/OS remote system configuration and service processor configuration objects to locate and manage the hardware of iSCSI-attached System x and blade integrated servers.

Related concepts

"Initiator system and service processor discovery" on page 14
The i5/OS operating system uses either the Service Processor Manager of i5/OS Integrated Server Support or IBM Director Server to locate System x or BladeCenter hardware on the network, to turn the initiator system hardware on and off, and to retrieve power status.

"Service processor connection for integrated servers" on page 23
This physical connection is required so that the hosting i5/OS partition can communicate with the service processor of the initiator (System x or BladeCenter) system.

Verifying that Director Server is installed and running:

If you are using IBM Director for integrated server discovery and power control, do these steps to verify that IBM Director Server is installed and running on the i5/OS partition that hosts your integrated server.

> **Note:** If you use the Service Processor Manager function of i5/OS Integrated Server Support, then you do not need to install or run IBM Director on the i5/OS host system (unless you need it for some other purpose). See "Configuring i5/OS to use Service Processor Manager" on page 107 for more information.

IBM Director Server is used for power control and some management functions for your integrated System x or blade hardware.

- If you are using System i Navigator, do the following steps.
  1. Expand **Network → Servers → User-Defined**.
  2. Verify that the status for **IBM DIRECTOR** is **Started**.
- If you are using CL commands, do the following steps.
  1. Type the following command at the i5/OS command line: QSH CMD('/qibm/userdata/director/bin/ twgstat')
  2. Verify that the status is **active**.

If you cannot verify the IBM Director status, see Troubleshooting on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Configuring service processor discovery for integrated servers:

Use these tasks to configure how i5/OS will locate your integrated server hardware on the network.

Configuring service processor discovery by IP address for integrated servers:

Do these steps to configure service processor discovery by internet protocol (IP) address. This method of service processor discovery uses unicast addressing.

1. On the hosted system, configure a static IP address that is suitable for the network in the service processor. If possible, do this step before connecting the service processor to the LAN. Use either the system BIOS setup menu or the web interface, whichever is supported by your service processor. For details on connecting and using a web browser, see "Configuring the integrated server Management Module or RSAII using the Web interface" on page 221.
2. On i5/OS, configure the service processor configuration:
   a. Ensure that the **Use service processor connection to determine remote system enclosure identity** option is checked.
   b. Select the **Internet address** option and specify the service processor IP address.
   c. (Optional) Specify the stand-alone server's serial number or a IBM BladeCenter chassis serial number. An error will occur if the serial number of the service processor discovered by IP address is different that the configured serial number.

   See "Changing service processor configuration properties" on page 213.
3. Using the procedure described in "Changing remote system configuration properties" on page 210 ensure that the remote system identity is set correctly:
   a. For a stand-alone server, select the **Use enclosure identity from the service processor configuration** option.
   b. For a IBM BladeCenter blade, select the **Use the following values** option and specify the blade serial number.

Configuring service processor discovery by host name for integrated servers:

Do these steps to configure service processor discovery by host name. This method of discovery uses unicast addressing.

To configure discovery by host name, perform the following steps.

1. On the initiator system, configure the host name in the service processor. If possible, do this step before connecting the service processor to the LAN.
   a. You must use the web interface for this step. Use the current IP address to connect to the RSA II web interface. For details on connecting and using a web browser, see "Configuring the integrated server Management Module or RSAII using the Web interface" on page 221.
   b. Use your browser to change the host name to one that is suitable for your network.
   c. Optional: You can also configure a static IP address that is suitable for your network.
2. On your i5/OS partition, configure the service processor:
   a. Ensure that the **Use service processor connection to determine remote system enclosure identity** option is checked.
   b. Select the **Host name** option and specify the service processor host name.
   c. Optional: Specify the stand-alone server's serial number or a IBM BladeCenter chassis serial number. An error will occur if the serial number of the service processor discovered by host name is different that the configured serial number.

   See "Changing service processor configuration properties" on page 213.
3. Using the procedure described in "Changing remote system configuration properties" on page 210, ensure that the remote system identity is set correctly
   a. For a stand-alone server, select the **Use enclosure identity from the service processor configuration** option.

    b. For an IBM BladeCenter blade, select the **Use the following values** option and specify the blade
       serial number.

Configuring service processor discovery by SLP for integrated servers:

Do these steps to configure service processor discover by Service Location Protocol (SLP). This discovery
method uses multicast addressing and Service Location Protocol (SLP) is used.

To configure SLP discovery, you must configure the i5/OS operating system. Do the following steps.
1. Using the procedure described in "Changing service processor configuration properties" on page 213:
    a. Ensure that the **Use service processor connection to determine remote system enclosure identity**
       option is not selected.
    b. In the **Serial number** field, specify the serial number of the stand-alone server enclosure or the
       IBM BladeCenter chassis.
2. Using the procedure described in "Changing remote system configuration properties" on page 210,
   ensure that the remote system identity is set correctly:
    a. For a stand-alone server, select the **Use enclosure identity from the service processor**
       configuration option.
    b. For an IBM BladeCenter blade, select the **Use the following values** option and specify the blade
       serial number.

Managing storage for integrated servers

Use these tasks to manage storage for an integrated server.

Administering integrated server disks from i5/OS

Use these tasks to administer integrated server disks from the i5/OS operating system.

Accessing the i5/OS integrated file system from an integrated server:

You can access the i5/OS integrated file system from an integrated server through IBM i5/OS Support for
Windows Network Neighborhood (i5/OS NetServer). This allows you to easily work with file system
resources on i5/OS.

For information about using i5/OS NetServer, see:
* Creating i5/OS NetServer file shares
* Configuring and connecting your PC clientSet up your PC client
* Access i5/OS NetServer file shares with a Windows client

For more information, see "Installing and configuring i5/OS NetServer" on page 149.

Displaying information about integrated server disks:

Do these steps to display information about what percentage of an integrated server disk drive (network
server storage space) is in use or the format of the disk from the i5/OS.
1. In System i Navigator, select **Integrated Server Administration** → **All Virtual Disks**.
2. Select a disk drive from the list available
3. Right-click the disk drive and select **Properties** or click the appropriate icon on the System i
   Navigator toolbar

If you want to use the CL command, see Work with Network Server Storage Spaces (WRKNWSSTG).

Adding disks to integrated servers:

Use these tasks to add a disk to an integrated server.

For conceptual information about network server storage spaces, see "Network server storage spaces" on page 43.

> **Related concepts**
>
> "Storage space linking for integrated servers" on page 20
> Integrated servers do not use physical disks. i5/OS creates virtual disks (network server storage spaces) within its own file system and integrated servers use them as if they were normal physical disk drives.

Creating virtual disks for integrated servers:

Do these steps to create a virtual disk for an integrated server with the System i Navigator interface or a CL command.

It is important to use a naming convention for your storage spaces. Otherwise you might have trouble correlating storage space names that you see from the i5/OS side with disks that you see from the integrated server side. This can be especially difficult if you have both statically linked and dynamically linked disks.

For example, the Linux operating system allocates the SCSI device names /dev/sda and /dev/sdb to the system and installation disks. You can name the first additional storage space you create for a server nwsd-namesdc, nwsd-namesdd, and so on. Using this naming convention for an NWSD named REDHAT1, additional storage spaces would be named REDHAT1SDC, REDHAT1SDD, and so on. Note that the maximum length of a storage space name is 10 characters.

Creating virtual disks for integrated servers with System i navigator:

To create an integrated server disk drive, do these steps.

1. In System i Navigator, select **Integrated Server Administration**.
2. Right-click the **All Virtual Disks** folder and select **New Disk** or click the appropriate icon on the System i Navigator toolbar.
3. Specify a disk drive name and description.
   This name is also used for the storage space object created in the /QFPNWSSTG directory of the integrated file system. You should consider using a naming scheme to allow easy identification of storage spaces and to allow using generics (*) on the save commands.
4. If you want to copy data from another disk, select **Initialize disk with data from another disk**. Then select the source disk to copy data from.
5. Specify the disk capacity in megabytes (MB) or gigabytes (GB).
6. Select a disk pool (auxiliary storage pool) to contain the disk.
7. Select the planned file system for the disk.
   - For integrated Windows servers, you can change the file system when you format the disk from the Windows operating system.
   - For integrated Linux servers, you can use the value that you prefer. The suggested value is *OPEN for Linux specific file systems such as ext2, ext3, etc.
8. If you want to immediately link the disk to a server after it is created, check **Link disk to server** and fill in the linking attributes.
9. Click **OK**.

The process of creating a storage space can range from a few minutes to a few hours, depending on the size. When i5/OS finishes creating the storage space it is listed with the other storage spaces.

Note:

1. Created disks must be partitioned and formatted using Disk Management by Windows or by using the DISKPART command line utility.
2. Creating or starting a server with a disk drive in an independent disk pool (ASP) requires that the disk pool device be available.

After creating the disk drive, you must link it to the network server description of your integrated server and format it. The time that you need to create a disk drive is proportional to the size of the drive.

Creating virtual disks for integrated servers using CL commands:

Do these steps to create a virtual disk for an integrated server with the Create network server storage space (CRTNWSSTG) command. A storage space appears as a virtual disk in the System i Navigator interface.

1. Type CRTNWSSTG at the i5/OS command line. Press Enter. The Create Network Server Storage Space display appears.
2. Type in the name of the storage space that you want to create.
3. Enter values for the following parameters.

Table 21. Parameters for the CRTNWSSTG command

Label	Description
Storage space name	The name of the storage space. This name is also used for the storage space object created in the /QFPNWSSTG directory of the integrated file system. You should consider using a naming scheme to allow easy identification of storage spaces and to allow using generics (*) on the save commands.
Size	Enter a size for the new storage space in megabytes (MB) or gigabytes (GB).
From storage space	The storage space to copy data from. This option is used when copying or cloning a virtual disk.

Format	A nominal format for the new storage space.
	• For integrated Windows servers, you can change the file system when you format the disk from the Windows operating system
	• For Linux and VMware ESX Server, use **Open source** for most file systems.
	  – For the typical Linux file systems (such as ext2, ext3, reiserfs), if you use **Open source** format, then use the **Advanced Data Offset** button and select the **Align the first logical partition sector** option.
	  – For the Virtual Machine File system (VMFS) on VMware ESX Server, use the **Advanced Data Offset** button and select **Align the first logical disk sector**.

ASP ID	The System i auxiliary storage pool where the storage space is created. The default is the system ASP, but storage spaces can be created in user ASPs and independent ASPs.
Description	Descriptive name of the storage space.

4. Press **Enter**. The virtual disk is created.
5. Link the disk to the integrated server.

Linking disks to integrated servers:

Integrated servers can only access disks that are linked to the Network Server Description (NWSD) for the server.

You must create a disk drive before you can link it. See "Creating virtual disks for integrated servers" on page 231. After you create and link a new integrated server disk drive, it appears as a new hard disk drive to the integrated server. Then you must format it before you can use it.

To link a disk drive to an integrated server, follow these steps:

1. If you are not linking a disk drive dynamically, then shut down your integrated server. See "Starting and stopping integrated servers" on page 190.
2. In System i Navigator, select **Integrated Server Administration** → **All Virtual Disks**.
3. Right-click an available disk drive and select **Add Link**, or select the drive and click the appropriate icon on the System i Navigator toolbar.
4. Select the server you want to link the disk to.
5. Select one of the available link types and the link sequence position.
6. If you are linking the disk to an iSCSI attached server, select one of the available storage paths.
7. Select one of the available data access types.
8. Click **OK**.
9. Start the integrated server. See "Starting and stopping integrated servers" on page 190.
10. When the server is started, format the disk. You can use the utilities provided by the integrated server operating system or "Formatting virtual disks for integrated Windows servers" on page 234 for servers running the Windows operating system.

If you want to use the CL command, see ADDNWSSTGL.

Manage disk drives for the Windows operating system when running out of drive letters:

The maximum number of disk drives that can be linked to an integrated server is greater than the number of drive letters that are available on Windows. Since not all drives will have a drive letter, other options must be used to utilize all storage linked to the server. Here are two options to utilize all disk drives which are linked to a server.

1. A disk drive letter can be made up of multiple disk drives using a spanned volume set.

   Note: When you create a volume set, all of the existing data on the partitions that you use for the new volume set is erased. You should consider volume sets while you are setting up your server.

   a. From **Disk Management**, right-click each disk drive number and select **Upgrade to Dynamic Disk...** from pop-up menu.
   b. Right-click a disk drive partition and select **Create Volume...** from pop-up menu.
   c. Follow the create volume wizard to create a spanned volume, making sure to add the multiple disks. Note: This feature is nice because if the volume gets full, a disk can be dynamically added, and it will be immediately joined to the spanned volume without ever requiring to reboot the server.
2. A disk drive can be mounted over a subdirectory of an existing disk drive letter.
   a. Create a directory on a disk drive letter that is formatted with NTFS. For example, MD C:\MOUNT1.
   b. From **Disk Management**, click over disk drive partition you want to format and select **Format** from the pop-up menu.
   c. Once drive is formatted, right-click over disk drive partition again and select **Change Drive Letter and Path...** from pop-up menu.
   d. Select **Add**.

e. Select radio button **Mount in this NTFS folder:**

f. Use **Browse** button to find directory C:\MOUNT1 that was created in step 1.

g. Click **OK** to make that directory a mount point for this disk drive.

Related tasks

"Linking disks to integrated servers" on page 232
Integrated servers can only access disks that are linked to the Network Server Description (NWSD) for the server.

Formatting virtual disks for integrated Windows servers:

Do these steps to format a disk for an integrated server with the Microsoft Windows operating system.

In order to use integrated server virtual disks (network server storage spaces), you must format them. Before you can format them, you must first create (see "Creating virtual disks for integrated servers" on page 231) and link (see "Linking disks to integrated servers" on page 232) the disk drives, then start the integrated server from i5/OS (see "Starting and stopping integrated servers" on page 190).

Note: Servers can dynamically link disk drives while the server is varied on using the dynamic storage link parameter of the Add Server Storage Link (ADDNWSSTGL) command.

To format disk drives, follow these steps.

1. On the integrated Windows server console, from the **Start** menu, select **Programs**, then **Administrative Tools**, then **Computer Management**.

2. Double-click **Storage.**

3. Double-click **Disk Management.**

4. To create a new partition, right-click the unallocated space on the basic disk where you want to create the partition, and then click **New Partition**.

5. Follow the prompts to format the new drive.

    a. Specify the storage space name for the volume label.

    b. Select the file system you specified when you created the disk drive.

    c. Select the quick format for a storage space that has just been created. It has already been low level formatted by i5/OS when it was allocated.

Copying an integrated server disk:

Do these steps to create a new virtual disk for an integrated server with information from an existing disk.

1. Expand **Integrated Server Administration** → **All Virtual Disks**.

2. Select a disk drive from the list available.

3. Right-click the disk drive and select **New Based On** or click the appropriate icon on the System i Navigator toolbar.

4. Specify a disk drive name and description.

5. Specify the disk capacity. See the online help for details on valid disk sizes associated with a particular file system format. If you want to increase the size of the disk while copying it, you can specify a larger size. The extended portion of the disk will be unpartitioned free space.

    Note: For integrated Windows servers, you can use the DISKPART command line utility to expand an existing partition in order to utilize any additional free space. Refer to the Microsoft Knowledge base articles for DISKPART for details and limitations.

6. Select a disk pool (auxiliary storage pool) to contain the disk.

7. Click **OK**.

If you want to use the CL command, see Create Network Storage Space (CRTNWSSTG).

Expanding an integrated server disk:

Do these steps to expand an integrated server disk.

For information about expanding a boot disk, see "Expanding system disks for integrated Windows servers."

To expand a disk drive, follow these steps:
1. Expand **Integrated Server Administration** → **All Virtual Disks**.
2. Select a disk drive from the list available.
3. Right-click the disk drive and select **Properties** or click the appropriate icon on the System i Navigator toolbar.
4. Click on the **Capacity** tab of the disk drive property sheet.
5. Specify the increased disk size in the **New capacity** field. See the online help for details on valid disk sizes associated with a particular file system format. The extended portion of the disk will be unpartitioned free space.
6. Click **OK**.
7. If the disk is linked to an active server, a confirmation panel is shown to indicate that the disk drive will be temporarily unavailable to the server while the disk is being expanded. Click **Change** on the confirmation panel to confirm that this is acceptable, or click **Cancel** on the confirmation panel to cancel the disk expansion operation.

Expanding system disks for integrated Windows servers:

To expand an integrated Windows server system disk, unlink the disk from the integrated server, expand the disk, and then relink the disk to the server.

Attention: You should back up your system drive before you expand it. For more information about using the DISKPART utility, see the Microsoft   Web page and search for "DISKPART".

To expand a system drive, do the following steps.
1. Shut down the server. See "Starting and stopping integrated servers" on page 190..
2. Unlink the system drive disk from the server. See "Unlinking integrated server disks" on page 161.
3. Change the size of the disk. See "Expanding an integrated server disk."
4. Link the disk to a temporary server network server description as a data disk. See "Linking disks to integrated servers" on page 232.
5. Start the temporary server. See "Starting and stopping integrated servers" on page 190.
6. On the temporary server Windows console, extend the partition of the disk using the DISKPART utility.
7. Shut down the temporary server. See "Starting and stopping integrated servers" on page 190.
8. Unlink the disk from the temporary server. See "Unlinking integrated server disks" on page 161.
9. Link the expanded disk to the original server as the system disk. See "Linking disks to integrated servers" on page 232.
10. Start the original server. See "Starting and stopping integrated servers" on page 190.

Unlinking integrated server disks:

Do these steps to unlink an integrated server disk from the Network Server Description (NWSD) object. When you unlink a disk, you make it inaccessible to the integrated server.

Restrictions:

1. For integrated Windows servers, see "Storage space linking for integrated servers" on page 20 for information about when disks can be dynamically unlinked.
2. For servers running VMware ESX Server, you can not unlink a disk from an active server (dynamic unlinking).
3. You can unlink a disk from a Linux server either when the server is shut down or when it is active (dynamic unlinking). Unlinking a dynamic storage from a running server is only possible at i5/OS V5R3 or later. Verify that the following things are true before you unlink the disk or the dynamic unlink will fail.
   - No users are using the Linux disk to be unlinked.
   - The disk was dynamically linked to the server
   - The disk is not part of an active logical volume group.

     Be careful about unlinking storage spaces from Linux servers that have an entry in /etc/fstab. If you unlink a drive from an integrated Windows server (other than the system or installation drives), Windows tolerates the missing drive and boots up normally, assuming that there are no application errors. Linux, however, detects the missing drive and halts the boot sequence. In this case, you need to sign on as root and go into maintenance mode to remove the file system entry for the drive you unlinked before the server can continue the boot process. If you relink the storage space, you need to add back the file system entry you previously deleted.

Unlinking integrated server disks with System i navigator:

To unlink a Linux disk using System i Navigator, complete the following steps:

1. If you do not want to dynamically unlink the disk, shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. If you are dynamically unlinking a disk for an integrated Linux server, use the umount command at the integrated server console to unmount the disk.
3. Expand **Integrated Server Administration** → **All Virtual Disks** or expand **Integrated Server Administration** → **Servers** → *servername* → **Linked Virtual Disks**, where *servername* is the name of the server that the disk is linked to.
4. Optional: **Optional:** To change the sequence of the disks, click **Compress link sequence**.
5. Right-click the disk you want to unlink.
6. Select **Remove link** to open the Remove Link from Server window. The disk name and description that you specified when you created the storage space are displayed.
7. Click **Remove** to unlink the disk.

Unlinking disks with the character-based interface:

To unlink integrated server disks using CL commands, do the following steps.

1. If you do not want to dynamically unlink the disk, shut down the integrated server. See "Starting and stopping integrated servers" on page 190.
2. If you are dynamically unlinking a disk for an integrated Linux server, use the umount command at the integrated server console to unmount the disk.
3. Type in WRKNWSSTG. Press **Enter**. The Work with Network Server Storage Spaces display appears. Type 11 in the Opt column next to the storage space that you want to unlink. Press **Enter**. The Remove Server Storage Link display appears.
4. Optional: Enter RMVNWSSTGL on the command line. Press **Enter**. The Remove Server Storage Link display appears.
   a. For **Network server storage space** enter the storage space name.
   b. For **Network server description** enter the NWSD that corresponds to the integrated server.

   c. You might need to press **F9** to see the **Renumber link** parameter. It is recommended that you take the default of *YES for this parameter unless you plan to relink the disk at a later time.

5. Press **Enter**. You see a message at the bottom of the display confirming that the storage space was unlinked successfully from the NWSD.

Deleting integrated server disks:

Use these tasks to delete an integrated server disk with System i Navigator or CL commands.

Before you can delete an integrated server disk, you must unlink it from the integrated server. See "Unlinking integrated server disks" on page 161.

Deleting integrated server disks using System i Navigator:

Do the following steps to delete a virtual disk for an integrated server.
1. For integrated VMware servers, stop the server. See "Starting and stopping integrated servers" on page 190.
2. Unlink the disk from the server. See .
3. Expand **Integrated Server Administration** → **All Virtual Disks**.
4. Right-click the disk that you want to delete and select **Delete** or click the appropriate icon on the System i Navigator toolbar.

   To delete multiple disks simultaneously, hold down the control key (Ctrl) and click each of the disks you want to delete. Then right-click one of the selected drives and click **Delete**.
5. Click **Delete** on the confirmation panel.

Deleting integrated server disks with the character-based interface:

Do these steps to delete a network server storage space (known as a virtual disk).

You can use either the Delete network server storage space (DLTNWSSTG) command or Work with network server storage space (WRKNWSSTG) command to delete a virtual disk. Use these steps to delete a disk with the WRKNWSSTG command.
1. For integrated VMware servers, stop the server. See "Starting and stopping integrated servers" on page 190.
2. Unlink the disk from the server. See "Unlinking integrated server disks" on page 161.
3. Type WRKNWSSTG. Press **Enter**. The Work with Network Server Storage Spaces display appears.
4. Type 4 in the Opt column next to the storage space that you want to delete.
5. Press **Enter**. The system displays a message confirming that the storage space was deleted successfully.

Viewing integrated server messages
View i5/OS message logs for integrated servers.

The **monitor job log** is a key source of information when troubleshooting integrated server problems. It contains messages that vary from normal processing events to detailed error messages. The monitor job always runs in the QSYSWRK subsystem with the same name as the integrated server.

To find the job log in System i Navigator
1. Click **Work Management** → **Active Jobs**.
2. One of the jobs listed under the QSYSWRK section will have the same name as your integrated server. Right-click it and select **Job log**.
3. The integrated server job log window opens. Double-click a message ID to see details.

To find the job log in the character-based interface

1. At an i5/OS command line enter WRKACTJOB SBS(QSYSWRK).
2. One of the jobs listed will have the same name as your integrated server. Select option 5 (Work with job).
3. Type 10 and press Enter to display the job log.
4. Press F10 to see the detailed messages.

There are other relevant job logs that you may want to check as well. The IBM Redbooks publication

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 , includes information about integrated server event logs in i5/OS and at the Windows console.

Network server description configuration files

You can use network server description (NWSD) configuration files to customize the NWSD for integrated servers.

NWSD configuration file format

An NWSD configuration file consists of multiple occurrences of **entry types**, each with a different function.

The entry types are:

"Removing lines from an existing integrated server configuration file with CLEARCONFIG entry type" on page 240
  Use this entry type if you want to remove all lines from the integrated server file.

"Changing an integrated server file with ADDCONFIG entry type" on page 240
  Use this entry type to add, replace, or remove lines in the integrated server file.

"Change an integrated server file with UPDATECONFIG entry type" on page 245
  Use this entry type to add or remove strings within lines in the integrated server file.

"Set configuration defaults with the SETDEFAULTS entry type" on page 246
  Use this entry type to set the default values for certain keywords. i5/OS uses the defaults only when processing ADDCONFIG and UPDATECONFIG entries in the current file member.

An **entry** is one occurrence of an entry type. Each entry contains a series of keywords that are followed by equal signs (=) and values for those keywords.

Format guidelines

- Source physical file record length must be 92 bytes.
- A line can have only one entry, but an entry can occupy multiple lines.
- You can use blank spaces between the entry type and the keyword, around the equal sign, and after the commas.
- You can use blank lines between entries and between keywords.

Keywords

- You can put entry keywords in any order.
- Use a comma after all keyword values except the last one in the entry.
- Enclose keyword values in single quotation marks if they contain commas, blank spaces, asterisks, equal signs, or single quotation marks.
- When you use keyword values that contain single quotation marks, use two single quotation marks to represent a quotation mark within the value.
- Keyword value strings can have a maximum length of 1024 characters.

- Keyword values can span lines, but you must enclose the value in single quotation marks. The value includes leading and trailing blanks in each line.

Comments

- Begin comments with an asterisk (*).
- You can put a comment on its own line or on a line with other text that is not part of the comment.

Creating an NWSD configuration file for your integrated server

Create an NWSD configuration file for your integrated server.

Before creating a configuration file, read the topics "NWSD configuration file format" on page 238 and "Substitution variables for keyword values" on page 248. You might also want to read "Example: NWSD configuration file for an integrated server."

1. Create a source physical file.
   a. At the i5/OS command line, type CRTSRCPF and press F4.
   b. Supply a name for the file, any text you want to describe it, and a member name and press Enter to create the file.
2. Use an available editor to add syntactically correct entries to the file that fit the NWSD. See "NWSD configuration file format" on page 238. For example, you can use the Work with members using PDM (WRKMBRPDM) command:
   a. At the i5/OS command line, type WRKMBRPDM file(yourfilename) mbr(mbrname) and press Enter.
   b. Type 2 next to the file you want to edit.

Example: NWSD configuration file for an integrated server

This example shows some basic elements of an NWSD configuration file.

This example configuration file:

- Sets a default file path
- Deletes the time zone and uses a configuration variable to add it back
- Sets default search values that cause the display configuration lines to be added before the UserData section
- Adds lines that configure the display

```
+--------------------------------------------------------------------------------+
| *************** Beginning of data **********************************           |
| *****************************************************************               |
| * Update D:\UNATTEND.TXT                                                        |
| *****************************************************************               |
| *                                                                              |
| *===============================================================                |
| * Set default directory and file name values.                                  |
| *===============================================================                |
| SETDEFAULTS TARGETDIR = 'D:\', TARGETFILE = 'UNATTEND.TXT'                      |
| *                                                                              |
| *===============================================================                |
| * Delete and use a substitution variable to re-add TimeZone line.              |
| *===============================================================                |
| ADDCONFIG VAR    = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS'         |
| ADDCONFIG ADDSTR = 'TimeZone="%TIMEZONE%"',                                     |
|   FILESEARCHSTR  = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%'                |
| *                                                                              |
| * Add lines to configure the display.                                          |
| *===============================================================                |
| * Set default search values to add new statements to the file                  |
| * before the UserData section header line.                                     |
| SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%',           |
|             FILESEARCHPOS = 'BEFORE'                                            |
| *                                                                              |
```

```
 * Add the display statements to the file.
 ADDCONFIG ADDSTR = '%FPA_L_BRACKET%Display%FPA_R_BRACKET%',
 UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'ConfigureAtLogon = 0',   UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'BitsPerPel = 16',         UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'XResolution = 640',       UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'YResolution = 480',       UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'VRefresh = 60',           UNIQUE = 'YES'
 ADDCONFIG ADDSTR = 'AutoConfirm = 1',         UNIQUE = 'YES'
 *
```

Removing lines from an existing integrated server configuration file with CLEARCONFIG entry type

You can use the CLEARCONFIG entry type to remove all lines from an existing integrated server file.

Attention: Removing all lines from the integrated server file may result in your being unable to vary on the network server.

To clear an integrated server file, create an NWSD configuration file that contains the CLEARCONFIG entry type as follows.

```
CLEARCONFIG
 LINECOMMENT  = '<"REM "|<comment_string>>',     (optional)
 TARGETDIR    = '<BOOT|path>',                   (optional)
 TARGETFILE   = '<file_name>'                    (required)
```

For a detailed explanation of the CLEARCONFIG keywords, use the following keyword links. You can also go back to "NWSD configuration file format" on page 238, or on to "Changing an integrated server file with ADDCONFIG entry type."

- "LINECOMMENT keyword" on page 243
- "TARGETDIR keyword"
- "TARGETFILE keyword"

TARGETDIR keyword:

Use TARGETDIR to specify the path for the integrated server file to be cleared.

Note: When changing a file, i5/OS uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword:

Use TARGETFILE to specify the integrated server file to be cleared.

Changing an integrated server file with ADDCONFIG entry type

Use the ADDCONFIG entry type to change an existing integrated server Network Server Description (NWSD) configuration file.

You can use the ADDCONFIG entry type to change an integrated server file in these ways:
- Add a line to the beginning or end of the file.
- Add a new line before or after a line that contains a specific string.
- Delete a line in the file.
- Replace the first, last, or all occurrences of a line in the file.
- Specify in which directory to change the file.

To change an integrated server file, create an NWSD configuration file that contains the ADDCONFIG entry type as follows:

```
ADDCONFIG
 VAR               = '<variable_name>',          (conditionally required)
 ADDSTR            = '<line to process>',        (optional)
 ADDWHEN           = '<ALWAYS|NEVER|<expression>>',   (optional)
 DELETEWHEN        = '<NEVER|ALWAYS|<expression>>',   (optional)
 LINECOMMENT       = '<"REM "|<comment_string>>',     (optional)
 LOCATION          = '<END|BEGIN>',              (optional)
 FILESEARCHPOS     = '<AFTER|BEFORE>',           (optional)
 FILESEARCHSTR     = '<search_string>',          (conditionally required)
 FILESEARCHSTROCC  = '<LAST|FIRST>',             (optional)
 REPLACEOCC        = '<LAST|FIRST|ALL>',         (optional)
 TARGETDIR         = '<BOOT|path>',              (optional)
 TARGETFILE        = '<CONFIG.SYS|<file_name>>', (optional)
 UNIQUE            = '<NO|YES>'                   (optional)
```

For a detailed explanation of the ADDCONFIG keywords, use the following keyword links. You can also go back to "NWSD configuration file format" on page 238 or on to the "Change an integrated server file with UPDATECONFIG entry type" on page 245.

VAR keyword:

VAR specifies the value on the left side of the equal sign that identifies the line you want to add to or delete from the file.

For example:
```
ADDCONFIG
  VAR = 'FILES'
```

i5/OS requires the keyword if you do not specify REPLACEOCC,

ADDSTR keyword:

Use ADDSTR to specify the string that you want to add to the integrated server Network Server Description (NWSD) configuration file.

For example:
```
ADDCONFIG
  VAR = 'FILES'
  ADDSTR = '60'
```

ADDWHEN keyword:

Use ADDWHEN to specify when during processing you want i5/OS to add the new line or string to the Network Server Description (NWSD) configuration file for an integrated server.

You can specify:
- ALWAYS if you want i5/OS to add the line or string every time it processes the configuration file. (ALWAYS is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- NEVER if you want i5/OS to never add the line or string.
- An expression that directs i5/OS to add the line or string when the specified condition is true. Expressions are composed of operators (see "ADDWHEN and DELETEWHEN expression operators" on page 242) and must equate to either TRUE or FALSE.

  Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*))

as a mathematical operation, enclose the expression in quotation marks. For example, to add a line when the NWSD type is *WINDOWSNT, you might use this:

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

ADDWHEN and DELETEWHEN expression operators:

Use these operators for expressions in the Network Server Description (NWSD) configuration file for an integrated server.

You can use these operators for expressions:

Operator	Description
==	Returns TRUE if operands are equivalent, FALSE if they are not.
!=	Returns FALSE if operands are equivalent, TRUE if they are not.
>	Returns TRUE if the operand on the left is greater than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<	Returns TRUE if the operand on the left is less than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
>=	Returns TRUE if the operand on the left is greater than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<=	Returns TRUE if the operand on the left is less than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
&&	Logical AND. Returns TRUE if both operands have a value other than 0. Operands must be integers.
||	Logical OR. Returns TRUE if either operand has a value other than 0. Operands must be integers.
+	If the operands are both integers, the result is the sum of the integers. If the operands are both strings, the result is the concatenation of the two strings.
-	Subtracts integers.
*	Multiplies integers.
/	Divides integers.
()	Parentheses force an evaluation order.
!	Logical NOT. Returns TRUE if the value of a single operand is 0. Returns FALSE if it is not 0.
ALWAYS	Always returns TRUE.
NEVER	Always returns FALSE.

DELETEWHEN keyword:

Use DELETEWHEN to specify when during processing you want i5/OS to delete a line or string from the Network Server Description (NWSD) configuration file for an integrated server.

You can specify:
- ALWAYS if you want i5/OS to delete the line or string every time it processes the configuration file.
- NEVER if you want i5/OS to never delete the line or string. (NEVER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member)
- An expression that directs i5/OS to delete the line or string when the specified condition is true. Expressions are composed of operators (see "ADDWHEN and DELETEWHEN expression operators") and must equate to either TRUE or FALSE.

  Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to delete a line when the NWSD type is *WINDOWSNT, you can use this:

```
        DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

LINECOMMENT keyword:

LINECOMMENT specifies the prefix string that identifies comments in a Network Server Description (NWSD) configuration file for an integrated server.

Use the default value if you want LINECOMMENT to use 'REM' to identify comments. You can specify a different value. For example, to use a semicolon to identify comments, use `LINECOMMENT = ';'` within the **first** entry that refers to that file. (i5/OS ignores the LINECOMMENT keyword on any other entry.)

LOCATION keyword:

LOCATION specifies where in the file to add the new line in a Network Server Description (NWSD) configuration file for an integrated server.

The default value END directs i5/OS to add the line at the end of the file. If you want i5/OS to add the line at the beginning of the file, specify BEGIN.

LINESEARCHPOS keyword:

Use LINESEARCHPOS to specify whether to add the string you specify with the ADDSTR keyword value AFTER (the default) or before the line search string.

e

LINESEARCHSTR keyword:

Specifies the string to search for within the lines.

Note: Only the right side of the equal sign is searched for the LINESEARCHSTR value.

LINELOCATION keyword:

Use LINELOCATION to specify where in the line to add the string that you specify with the ADDSTR keyword value.

Use the default value of END if you want i5/OS to add the string at the end of the line. If you want i5/OS to add the string at the beginning of the line instead, specify BEGIN.

FILESEARCHPOS keyword (ADDCONFIG entry type):

Specify where to locate a line relative to the file search string.

You can specify:
- AFTER if you want i5/OS to add the line after the line that contains the file search string. (AFTER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- BEFORE if you want i5/OS to add the line before the line that contains the search string.

FILESEARCHSTR keyword:

Use FILESEARCHSTR with the REPLACEOCC keyword to specify the line to replace. You must specify the entire line as the value.

When you are adding a new line, FILESEARCHSTR can be any part of a line you want to find.

There is no default value, unless you defined a default value by using a SETDEFAULTS entry in the member.

FILESEARCHSTROCC keyword:

Specifies which occurrence of a string that appears multiple times in the file to use for positioning the new line.

The default value of LAST specifies the last occurrence of the search string. If you want i5/OS to use the first occurrence of the search string, specify FIRST.

REPLACEOCC keyword:

Specifies which occurrence of a line you want to replace.
- Use LAST if you want i5/OS to replace the last occurrence of the FILESEARCHSTR.
- Use ALL if you want i5/OS to replace all occurrences of the FILESEARCHSTR.
- Use FIRST if you want i5/OS to replace the first occurrence of the FILESEARCHSTR.

Use FILESEARCHSTR to specify the entire line that you want to replace.

i5/OS deletes the line that matches the FILESEARCHSTR and adds the specified VAR and ADDSTR to the file at this location.

Note: REPLACEOCC has precedence over LOCATION and FILESEARCHPOS. If i5/OS does not find the FILESEARCHSTR value used with a REPLACEOCC keyword, it adds a new line based on the value of the LOCATION keyword but does not replace a line.

TARGETDIR keyword:

Use TARGETDIR to specify the path for the integrated server file to be changed.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify the path for UNATTEND.TXT or your own integrated server file. (This keyword defaults to BOOT, which directs i5/OS to change the file in the root directory of the C drive.)

Notes:
1. Support for NWSD configuration files exists only for predefined disk drives that are formatted as FAT. Storage spaces that are converted to NTFS are not accessible for configuration files.
2. When changing a file, i5/OS uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword:

TARGETFILE specifies the integrated server file to be changed. The value of UNATTEND.TXT directs i5/OS to change the integrated server unattended install setup script file.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify UNATTEND.TXT or your own integrated server file. (This keyword defaults to CONFIG.SYS.)

UNIQUE keyword:

Specifies whether you want to allow one or multiple occurrences of a line in the file.

Specify YES if you want to allow only one occurrence of a line in the file.

The default value of NO specifies that multiple occurrences are in the file.

VAROCC keyword:

Use VAROCC to specify which occurrence of the variable you want to change.

If you want to change the last occurrence of the variable, you can use the default value. Otherwise, specify FIRST to change the

VARVALUE keyword:

Use VARVALUE if you want to change a line only if it has this particular value for the variable you specify.

You can specify all or part of the string on the right side of an expression that you want to change.

Change an integrated server file with UPDATECONFIG entry type

You can use the UPDATECONFIG entry type to change an integrated server file in these ways.

* Add strings to lines in the file.
* Add new strings before or after a specified string.
* Delete strings from lines in the file.
* Specify in which paths to change the file.

To change an integrated server file, create an NWSD configuration file that contains the UPDATECONFIG entry type as follows:

```
UPDATECONFIG
 VAR               = '<variable_name>',             (required)
 ADDSTR            = '<line to process>',           (required)
 ADDWHEN           = '<ALWAYS|NEVER|<expression>>', (optional)
 DELETEWHEN        = '<NEVER|ALWAYS|<expression>>', (optional)
 LINECOMMENT       = '<"REM "|<comment_string>>',   (optional)
 LINELOCATION      = '<END|BEGIN>',                 (optional)
 LINESEARCHPOS     = '<AFTER|BEFORE>',              (optional)
 LINESEARCHSTR     = '<string within a line>',      (optional)
 FILESEARCHPOS     = '<AFTER|BEFORE>',              (optional)
 FILESEARCHSTR     = '<search string>',             (optional)
 FILESEARCHSTROCC  = '<LAST|FIRST>',                (optional)
 TARGETDIR         = '<BOOT|<path>>',               (optional)
 TARGETFILE        = '<CONFIG.SYS|<file_name>>',    (optional)
 VAROCC            = '<LAST|FIRST>',                (optional)
 VARVALUE          = '<variable value>             (optional)
```

For a detailed explanation of the UPDATECONFIG keywords, use the following keyword links. You can also go back to "NWSD configuration file format" on page 238 or on to "Set configuration defaults with the SETDEFAULTS entry type" on page 246.

* "VAR keyword" on page 241
* "ADDSTR keyword" on page 241
* "ADDWHEN keyword" on page 241
* "DELETEWHEN keyword" on page 242
* "LINECOMMENT keyword" on page 243
* "LINELOCATION keyword" on page 243
* "LINESEARCHPOS keyword" on page 243
* "LINESEARCHSTR keyword" on page 243
* "FILESEARCHPOS keyword (UPDATECONFIG entry type)" on page 246
* "FILESEARCHSTR keyword (UPDATECONFIG entry type)" on page 246
* "FILESEARCHSTROCC keyword (UPDATECONFIG entry type)" on page 246

- "TARGETDIR keyword" on page 244
- "TARGETFILE keyword" on page 244
- "VAROCC keyword" on page 245
- "VARVALUE keyword" on page 245

FILESEARCHPOS keyword (UPDATECONFIG entry type):

You can use FILESEARCHPOS to specify which occurrence of the variable you want i5/OS to find relative to a line that contains the search string.

- AFTER if you want i5/OS to find the first occurrence of the variable on or after the line that contains the search string. (AFTER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- BEFORE if you want i5/OS to find the first occurrence of the variable on or before the line that contains the search string.

Note: If i5/OS does not find the search string, it determines the line to change from the VAROCC keyword.

FILESEARCHSTR keyword (UPDATECONFIG entry type):

Use FILESEARCHSTR to provide a search string for i5/OS to use to locate the occurrence of the variable to replace.

There is no default value, unless you defined a default value by using a SETDEFAULTS entry in the member.

FILESEARCHSTROCC keyword (UPDATECONFIG entry type):

Use FILESEARCHSTROCC to specify which occurrence of a string that appears multiple times in the file to use for finding the lines to be modified.

Use the default value of LAST if you want i5/OS to use the last occurrence of the search string. If you want i5/OS to use the

Set configuration defaults with the SETDEFAULTS entry type

You can set default values for certain keywords on the ADDCONFIG and UPDATECONFIG entry types by using SETDEFAULTS.

You can set defaults to:
- Add and delete lines.
- Search for lines.
- Identify the file name and path to change.

To set the defaults, create an NWSD configuration file that contains the SETDEFAULTS entry type as follows:

```
SETDEFAULTS
 ADDWHEN       = '<ALWAYS|NEVER|<expression>>',  (optional)
 DELETEWHEN    = '<NEVER|ALWAYS|<expression>>',  (optional)
 FILESEARCHPOS = '<AFTER|BEFORE>',               (optional)
 FILESEARCHSTR = '<search_string>',              (optional)
 TARGETDIR     = '<path>',                       (optional)
 TARGETFILE    = '<file_name>'                   (optional)
```

For a detailed explanation of the SETDEFAULTS keywords, use the following keyword links.
- "ADDWHEN" on page 247

- "DELETEWHEN"
- "FILESEARCHPOS keyword (SETDEFAULTS entry type)"
- "FILESEARCHSTR keyword (SETDEFAULTS entry type)" on page 248
- "TARGETDIR" on page 248
- "TARGETFILE" on page 248

ADDWHEN:

Use ADDWHEN with the SETDEFAULTS entry type to set the default value for the ADDWHEN keyword on ADDCONFIG and UPDATECONFIG entry types.

Set the default for when during processing you want i5/OS to add the new line or string to the file. You can specify:
- ALWAYS if you want i5/OS to add the line or string every time it processes the configuration file. (ALWAYS is the default unless you defined a different default.)
- NEVER if you want i5/OS to never add the line or string.
- An expression that directs i5/OS to add the line or string when the specified condition is true. Expressions are composed of operands (see "ADDWHEN and DELETEWHEN expression operators" on page 242) and must equate to either TRUE or FALSE.

  Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to add a line when the NWSD type is *WINDOWSNT, you might use this:

  ```
  ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
  ```

DELETEWHEN:

Use DELETEWHEN with the SETDEFAULTS entry type to set the default value for the DELETEWHEN keyword on ADDCONFIG and UPDATECONFIG entry types.

Specify when during processing you want i5/OS to delete the line or string from the file.

You can specify:
- ALWAYS if you want i5/OS to delete the line or string every time it processes the configuration file.
- NEVER if you want i5/OS to never delete the line or string. (NEVER is the default unless you defined a different default.)
- An expression that directs i5/OS to delete the line or string when the specified condition is true. Expressions are composed of operands (see "ADDWHEN and DELETEWHEN expression operators" on page 242) and must equate to either TRUE or FALSE.

  Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to delete a line when the NWSD type is *WINDOWSNT, you can use this:

  ```
  DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
  ```

FILESEARCHPOS keyword (SETDEFAULTS entry type):

Use FILESEARCHPOS with the SETDEFAULTS entry type to set the default value for the FILESEARCHPOS keyword on ADDCONFIG and UPDATECONFIG entry types.

Specify where to locate a line relative to the file search string. You can specify:
- AFTER if you want the line located after the line that contains the file search string. (AFTER is the default unless you defined a different default.)
- BEFORE if you want i5/OS to add the line before the line that contains the search string.

FILESEARCHSTR keyword (SETDEFAULTS entry type):

Use FILESEARCHSTR with the SETDEFAULTS entry type to set the default value for the FILESEARCHSTR keyword on ADDCONFIG and UPDATECONFIG entry types.

The FILESEARCHSTR value can be any part of the line you want to find.

TARGETDIR:

Use TARGETDIR with the SETDEFAULTS entry type to set the default value for the TARGETDIR keyword on ADDCONFIG and UPDATECONFIG entry types.

A path specifies the directory that contains the file to be processed.

For example, to set the default TARGETDIR value for a file on drive D, you might use this:
```
SETDEFAULTS TARGETDIR = 'D:\'
```

TARGETFILE:

Use TARGETFILE with the SETDEFAULTS entry type to set the default value for the TARGETFILE keyword on ADDCONFIG and UPDATECONFIG entry types.

A name specifies the file to be processed.

For example, to set the default TARGETFILE value for file UNATTEND.TXT on drive D, you might use this:
```
SETDEFAULTS
  TARGETDIR = 'D:\',
  TARGETFILE = 'UNATTEND.TXT'
```

Substitution variables for keyword values

You can use substitution variables for keyword values. The NWSD configuration file substitutes the correct values for the variables. These substitution variables are configured using the values stored in the NWSD or the hardware that is detected on the NWSD.

i5/OS supplies these variables:

Substitution variable	Description
%FPAIPADDRPP%	TCP/IP address (NWSD Port *VRTETHPTP) *
%FPAIPADDR01%	TCP/IP address (NWSD Port 1) *
%FPAIPADDR02%	TCP/IP address (NWSD Port 2) *
%FPAIPADDR03%	TCP/IP address (NWSD Port 3) *
%FPASUBNETPP%	TCP/IP subnet address (NWSD Port *VRTETHPTP) *
%FPASUBNET01%	TCP/IP subnet address (NWSD Port 1) *
%FPASUBNET02%	TCP/IP subnet address (NWSD Port 2) *
%FPASUBNET03%	TCP/IP subnet address (NWSD Port 3) *
%FPATCPHOSTNAME%	TCP/IP host name
%FPATCPDOMAIN%	TCP/IP domain name
%FPATCPDNSS%	TCP/IP DNS's, separated by commas
%FPATCPDNS01%	TCP/IP Domain Name Server 1
%FPATCPDNS02%	TCP/IP Domain Name Server 2

Substitution variable	Description
%FPATCPDNS03%	TCP/IP Domain Name Server 3
%FPANWSDTYPE%	The type of the NWSD that you are varying on
%FPANWSDNAME%	The name of the NWSD that you are varying on
%FPACARDTYPE%	The resource type of the NWSD that you are varying on (ex. 2890, 2892, 4812, 2689, iSCSI)
%FPAINSMEM%	The amount of installed memory detected
%FPAUSEMEM%	The amount of useable memory detected
%FPACODEPAGE%	The ASCII codepage used to translate from EBCDIC
%FPALANGVERS%	The i5/OS Language version used on the NWSD
%FPASYSDRIVE%	The drive letter used for the system drive (C, E when server was installed with V4R4 or earlier)
%FPA_CARET%	The caret symbol (^)
%FPA_L_BRACKET%	The left bracket symbol ([)
%FPA_R_BRACKET%	The right bracket symbol (])
%FPA_PERCENT%	The percent symbol (%) NOTE: Since the percent symbol is used as the substitution variable delimiter, this substitution variable should be used when a string contains a percent symbol that should NOT be interpreted as a substitution variable delimiter.
%FPABOOTDRIVE%	This is always drive E for the Integrated xSeries Server
%FPACFGFILE%	The name of the NWSD configuration file being processed
%FPACFGLIB%	The library that contains the NWSD configuration file being processed
%FPACFGMBR%	The name of the NWSD configuration file member being processed
* Values are retrieved from the NWSD	

You can configure additional substitution variables by creating a file in QUSRSYS and giving it the same name as the NWSD followed by the suffix 'VA'. You must create the file as a source physical file with a minimum record length of 16 and maximum record length of 271.

For example, at the i5/OS command line, type this:

```
CRTSRCPF FILE(QUSRSYS/nwsdnameVA) RCDLEN(271)
   MBR(nwsdname) MAXMBRS(1)
   TEXT('Congfiguration file variables')
```

The member 'nwsdname' contains data in fixed columns formatted as:

- A variable name in column 1-15 padded with blanks and
- A value that starts in column 16

For example:

```
Columns:
12345678901234567890123456789012345678901234567890...
myaddr         9.5.9.1
```

where %myaddr% is added to the list of available substitution variables and has a value of "9.5.9.1".

Appendix. Notices

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

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

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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

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

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

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

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

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
AIX 5L
AS/400
BladeCenter
DB2
IBM
iSeries
Netfinity
NetServer
i5/OS
Redbooks
ServerGuide
System i
System x
xSeries

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

Pentium is a trademark or a registered trademark of Intel Corporation in the United States, other countries, or both.

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

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

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions

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

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

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

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

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

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

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

254 System i: System i integration with BladeCenter and System x: iSCSI-attached System x and blade systems

IBM ®

Printed in USA