IBM Systems - iSeries

Windows environment on iSeries

IBM Systems - iSeries

Windows environment on iSeries

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 259.

Tenth Edition (February 2006)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722–SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Chapter 1. Windows environment on iSeries

Windows® environment on iSeries is more of an idea than any one piece of hardware or software. It is a way for iSeries™ servers and Personal Computers (PCs) to work together, and what is more, to allow the iSeries server to control PCs in order to make them easier to administer.

The first part of Windows environment on iSeries is the PC hardware which must be added to the iSeries. There are three basic ways of doing this.

- By using an *Integrated xSeries® Adapter (IXA)*, the iSeries can control IBM® xSeries servers. IBM calls its line of PCs *xSeries servers*.
- By using an *internet SCSI host bus adapter (iSCSI HBA)* the iSeries server can connect over Ethernet and control IBM xSeries or IBM BladeCenter™ servers.
- An *Integrated xSeries Server (IXS)* is an iSeries expansion card which contains Random Access Memory (RAM) and an Intel™ processor. It can be thought of as a PC which has been transplanted inside the frame of an iSeries server.

The second part is the IBM i5/OS option 29 (5722–SS1) which is installed on the iSeries server to give it the capability to control PCs. These PCs are then called integrated Windows servers.

Finally, it is necessary to install Microsoft's Windows 2000 Server or Windows Server 2003 software.

This document is divided into the following sections

Chapter 2, "What's new for V5R4," on page 3
Changes and improvements made this release.

Chapter 3, "Printable PDF," on page 5
Print a PDF of this document.

Chapter 4, "Concepts," on page 7
Understand the Windows environment on iSeries solution.

Chapter 5, "Install and configure Windows environment on iSeries," on page 57
Follow these instructions to install a new integrated Windows server from scratch.

Chapter 6, "Manage virtual Ethernet and external networks," on page 111
Learn how to use the three different types of networks available to integrated servers.

Chapter 7, "Administer connections to iSCSI attached servers," on page 117
Configure iSeries to connect to xSeries or IBM BladeCenter servers using iSCSI.

Chapter 8, "Administer integrated Windows servers," on page 149
Start and stop the server, run integrated server commands remotely, view and change configuration information, and monitor message and error logs.

Chapter 9, "Manage storage," on page 159
Information about integrated server hard disks.

Chapter 10, "Share devices," on page 171
Use iSeries devices on integrated servers.

Chapter 11, "Administer integrated Windows server users from i5/OS," on page 177
Integrate i5/OS® users into the Windows environment.

Chapter 12, "Back up and recover integrated Windows servers," on page 187
This section describes ways to back up integrated server files to tape drives or iSeries hard disks.

Chapter 13, "Uninstall the Windows server operating system from the integrated server hardware," on page 201
Everything you need to know to remove integrated server software from your system.

Chapter 14, "Troubleshoot integrated Windows servers," on page 205
Find answers to common questions.

Chapter 15, "Network server description configuration files," on page 243
You can customize your integrated servers by creating your own configuration files.

Chapter 16, "Related information," on page 257
Listed below are the iSeries™ manuals and IBM® Redbooks™ (in PDF format), Web sites, and Information Center topics that relate to the Windows Environment on iSeries topic.

Chapter 2. What's new for V5R4

For V5R4, Windows environment on iSeries has several new functions:

- Support for integrating xSeries and IBM BladeCenter systems with the iSeries server via the iSCSI host bus adapters (iSCSI HBAs) is provided. This server integration technology complements the existing Integrated xSeries Server and Integrated xSeries Adapter technologies. Support is provided for servers connected by a scalable Gigabit Ethernet network using the iSCSI protocol and supported adapters in both the iSeries and xSeries servers. For information about how the iSCSI technology is used to integrate IBM xSeries and BladeCenter systems with the iSeries server, see Chapter 4, "Concepts," on page 7. For information about how to manage and configure iSCSI attached servers, see Chapter 7, "Administer connections to iSCSI attached servers," on page 117 and Chapter 8, "Administer integrated Windows servers," on page 149.
- The product IBM iSeries Integration for Windows Server (5722-WSV) has been repackaged as i5/OS™ Integrated Server Support (5722-SS1 option 29).

  Note: When you upgrade from a prior release to i5/OS V5R4, product 5722-WSV is automatically removed and product 5722-SS1 option 29 is installed in its place.
- Increased storage capacity for iSCSI attached Windows servers. Up to 64 disk drives (network server storage spaces) can be attached to an iSCSI attached Windows server, allowing over 60 TB of disk storage per server.
- Support for extending the size of a disk drive (network server storage space) is added. See "Expand a disk drive" on page 167.
- Support for Windows Server 2003 Volume Shadow Copy Service is added to the integrated file level backup utility. This application can be used to back up your Windows data without stopping your Windows applications. The file level backup utility is enhanced to be a shadow-copy requestor that requests a snapshot of your Windows volume for backup purposes. This can improve application availability and reliability. For more information, see Chapter 12, "Back up and recover integrated Windows servers," on page 187.
- Additional iSeries Navigator GUI support, including support for managing iSCSI attached servers, managing integrated Linux® and AIX® servers, and configuring virtual Ethernet ports for integrated servers.
- Support for the 200 MHz and 333MHz IBM Integrated PC Server for AS/400® (IPCS) and IBM Integrated Netfinity® Server for AS/400 (INS) is withdrawn. The withdrawn IPCS and INS hardware resource types are 6617 and 2850 with feature codes 2854, 2857, 2865, 2866, 6617 and 6618. Since IPCS and INS servers were the only integrated server types that provided host LAN support (sharing LAN adapters between i5/OS and Windows), the host LAN function has also been withdrawn.
- Information previously in this document related to Windows NT® 4.0 servers (which are no longer supported as of V5R3), IPCS or INS hardware (types 6617 and 2850), shared network adapters (host LAN), and considerations for servers installed before V4R5 has been removed from this document. For information related to these topics, refer to the Windows environment on iSeries topic in the V5R3 iSeries Information Center.

What's new as of July 2007

- Multipath I/O is supported on iSCSI-attached integrated Windows servers. 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. See "Advanced iSCSI support" on page 20 and "Configuring multipath I/O" on page 138.
- Multiple initiator HBA ports on an integrated server can now be configured as a boot device so that the boot process can proceed in case of a hardware failure.

What's new as of January 2007

- The Restore Licensed Program (RSTLICPGM) command can be used to install Director Server. This version of Director should be used for all new integrated server installations. See "Software requirements" on page 59.
- New information is added for expanding disks. See "Expand a disk drive" on page 167 and "Expand a system drive" on page 168.
- New information about the iSCSI network and maximum transmission unit (MTU) is added. See "iSCSI network" on page 29 and "Maximum transmission unit (MTU) considerations" on page 139.

What's new as of July 2006

- New commands for viewing and managing iSCSI HBA usage are available at the integrated server console. See "Manage iSCSI HBA allocation at the Windows side of the iSCSI network" on page 136.
- New information about installing IBM Director is available. See "Software requirements" on page 59.
- The Windows server installation advisor is updated with minor technical changes.

What's new as of April 2006

Information about working with iSCSI attached servers is added.

- The Windows server installation advisor is updated with minor technical changes.
- New information is added for installing and configuring IBM Director Server to work with iSCSI attached servers. See "Software requirements" on page 59.

Information about installing and configuring IBM Director Server to work with iSCSI attached integrated servers is added.

What's new as of March 2006

The Windows environment on iSeries topic has been updated with miscellaneous technical changes.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

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

Chapter 3. Printable PDF

To view or download the PDF version of this document, select Windows environment on iSeries (about 4.2 MB).

You can view or print PDFs of related manuals and Redbooks™ from Chapter 16, "Related information," on page 257.

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

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

Chapter 4. Concepts

In this document, the term *integrated Windows server*, or just *integrated server* refers to an instance of Microsoft® Windows 2000 Server or Windows Server 2003 running on an Integrated xSeries Server, an xSeries Server attached to an iSeries with an Integrated xSeries Adapter, or on an xSeries or IBM BladeCenter server attached to an iSeries server with an iSCSI host bus adapter. Just as the term PC is often used to refer to Microsoft's Windows operating system software running on an Intel based microprocessor and associated hardware, integrated Windows server refers to the combination of hardware and software which make up the entire product.

Read the following conceptual articles:
- "Integrated server overview"
- "Advantages" on page 8
- "Terminology" on page 10
- "Hardware concepts" on page 13
- "Considerations" on page 24
- "Performance" on page 25
- "Networking concepts" on page 28
- "Software concepts" on page 37
- "High availability concepts" on page 48
- "Security concepts" on page 48
- "User and group concepts" on page 51

Integrated server overview

Several pieces of hardware and software are combined to make an integrated server.

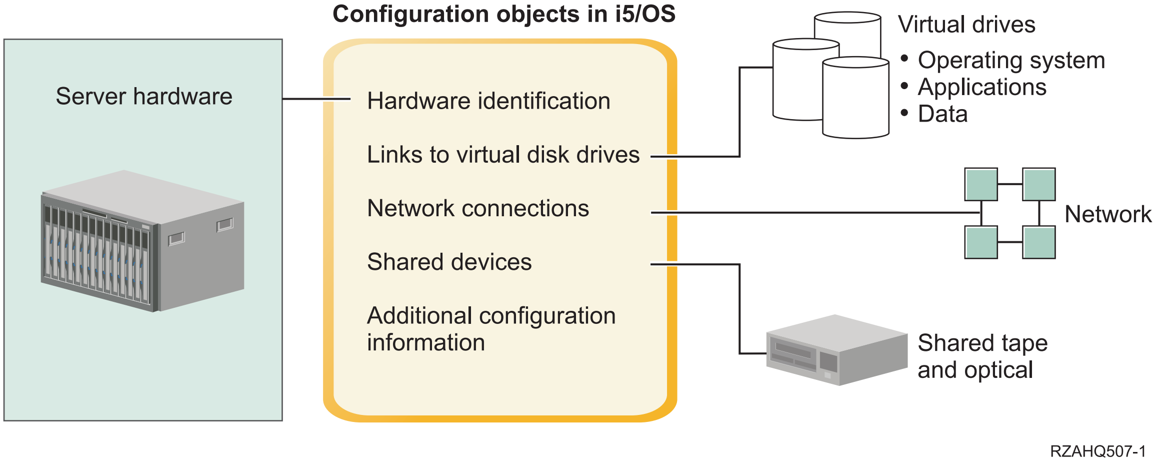


Figure 1. Integrated server overview

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 server hardware can take the form of a card that plugs into your iSeries server, an external IBM xSeries server that is attached to an iSeries server with an Integrated xSeries Adapter, or an external IBM xSeries or IBM BladeCenter server that is attached to an iSeries server 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 “Hardware concepts” on page 13 for more information about the types of hardware that can be used for integrated servers.

Each integrated server has one or more connections to a **network**. Both physical network connections with a network adapter and iSeries virtual Ethernet network connections are supported. See “Networking concepts” on page 28 for more information about the types of network connections that can be used with integrated servers.

Each integrated server uses **virtual disk drives** that contain the server’s operating system, applications, and data. These virtual disk drives 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 “Software concepts” on page 37 for more information about virtual disk drives.

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 iSeries tape and optical devices are automatically accessible by the integrated server. You can choose to restrict which of these iSeries devices the integrated server can access.

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” on page 37 for more information about the i5/OS configuration objects that describe an integrated server.

Advantages

Windows environment on iSeries provides most of the capabilities of running Microsoft Windows on a PC-based server and provides the following advantages over other computer systems.

Space savings

- There are fewer pieces of hardware to manage requiring less physical space.

Greater accessibility and protection for your data

- An integrated Windows server uses iSeries disk storage, which is generally more reliable than PC server hard disks.
- You have access to faster iSeries tape drives for integrated server backups.
- You can back up the entire Windows server as part of your iSeries server backup. This allows you to recover a failed server much faster and easier than with typical file level recovery from Windows.
- 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 iSeries disk drives than would be configured in stand-alone (non-integrated) Windows 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® UDB for iSeries data through an enhanced Open Database Connectivity (ODBC) device driver using iSeries 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 does not require additional LAN hardware and provides communications between iSeries logical partitions, Integrated xSeries Servers (IXSs), Integrated xSeries Adapters (IXAs), and iSCSI HBAs.

Simplified administration

- 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.
- Your computer system is less complicated thanks to the integration of user administration function, security, server management, and backup and recovery plans between the i5/OS and Microsoft Windows environments. 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.

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.

xSeries server attached with an Integrated xSeries Adapter (IXA) or iSCSI HBA

- You have considerably more flexibility in configuring a full size xSeries than you have in configuring an IXS, an xSeries on a card.
- Full size xSeries models are released more often, meaning that you can get the most up-to-date Intel processors and other hardware.
- More PCI feature cards are available for full size xSeries servers than for IXSs.

IBM BladeCenter server attached via an iSCSI host bus adapter

- Dense IBM BladeCenter packaging
- New IBM BladeCenter models are released more frequently than IXS.

Multiple servers

- Microsoft Cluster service allows you to connect multiple servers into server clusters. Server clusters provide high-availability and easy manageability of data and programs running within the cluster.
- Without using LAN hardware, servers and logical partitions running on the same iSeries have high-performance, secure virtual networking communications.
- You can run multiple integrated servers on a single iSeries. 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 iSeries, 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.
- An iSeries server's optical and tape drives can be shared with integrated servers running on the iSeries.

Hot spare support

- Server integration and storage virtualization provide innovative options that can enhance the reliability and recoverability of the Windows server environment.
- If the Windows server hardware fails, you can quickly and easily switch the server's configuration to another hot spare xSeries server or IBM BladeCenter server without restarting your iSeries server. 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.

Terminology

The following are terms related to Windows environment on iSeries. For other iSeries terms and definitions, see the Information Center glossary.

Baseboard Management Controller (BMC). A basic low function service processor that is used to control xSeries systems.

certificate. A standard format for combining an identity with a public key, signed by a Certificate Authority, which is valid from a specified start date/time until a specified end date/time. The identity in a certificate (also called the ″Subject″ of the certificate) says who or what the certificate was issued to. It can have a variety of syntaxes, but usually contains a distinguished name with attributes like ″CN=common name, O=organization, OU=organizational unit″. The public key is part of a private/public key pair, usually one created for use with the RSA public key cryptosystem. In contrast, the corresponding private key is not part of the certificate, and is not intended to be viewed.

certificate authority. A private key/certificate pair that can sign other certificates for authentication purposes, such as determining if a certificate is really from who it claims to be from. A certificate authority may be either owned by a third-party organization that verifies identity information and issues signed digital certificates, or it may be local and private. Once a certificate has been digitally signed, it cannot be altered without detection.

Challenge Handshake Authentication Protocol (CHAP). An authentication protocol that involves a secret known to both the authenticator and the party being authenticated. The secret is protected from eavesdropping during transmission.

connection security network server configuration. An i5/OS configuration object that is used to configure security-related values that control how the iSCSI HBA SCSI and virtual Ethernet LAN data is secured on the network. The corresponding i5/OS object type is *NWSCFG with a subtype of *CNNSEC. This object is also referred to using the shorter term **connection security configuration**.

enclosure ID. The identifying serial number, type and model of the enclosure containing the service processor. For a standard xSeries server, the service processor and the xSeries server share a common enclosure identifier. For an IBM BladeCenter server, this identifies the management module which contains the IBM BladeCenter servers which it controls.

Enterprise Identity Mapping (EIM). A mechanism for mapping/associating a person or entity to the correct user identities in various registries across multiple operating systems. User Administration function integrates user enrollment with EIM, by providing support for automatic creating of EIM Windows source associations. Also, enrolled i5/OS user profiles allow Windows user profiles to be different than the i5/OS user profile if the administrator has manually defined the EIM Windows source association.

EIM identifier. Represents an actual person or entity in EIM. When you create an EIM identifier you associate it with the user identity for that person.

EIM identity mapping association. A single sign-on environment is made possible by associating the user identity to an EIM identifier in a registry. There are 3 types of associations, source, target, and administrative. User enrollment integrates with EIM when a target i5/OS association and a source Windows association are defined. The associations may be defined either automatically using the user profile attribute, EIMASSOC, or by using iSeries Navigator to manually define the associations. Target associations are primarily used to secure existing data. Source associations are primarily used for authentication purposes.

external network. Networks accessed by integrated servers through physical networking hardware. See also **virtual networks**.

host bus adapter (HBA). A host bus adapter (HBA) is an adapter card that plugs into the bus of the host system. For example, an Ethernet adapter or an iSCSI adapter.

hot spare. Hot spare provides the ability to have spare server hardware (such as an idle IXS) set aside as a backup for the server hardware that is used by one or more active servers. If one of the active servers has a server hardware failure, that server can quickly be switched from the failed server hardware to the spare server hardware and started again, drastically reducing the server downtime that is normally associated with a server hardware failure. For more information see “Hot spare between server hardware” on page 156.

IBM Director Server. An application that provides remote xSeries and IBM BladeCenter discovery, power control and management. IBM Director is available through Virtualization Engine™ Standard Edition.

IBM i5/OS Integrated Server Support. Extension to the i5/OS operating system installed on the iSeries which allows it to work with integrated Windows and Linux servers. There is also a component of the product which runs on the integrated server.

Integrated Windows server. Also referred to as an *integrated server*, an instance of Windows 2000 Server or Windows Server 2003 running on an IXS, an IXA attached xSeries server, or an iSCSI HBA attached xSeries or IBM BladeCenter server.

Integrated xSeries Server (IXS). A PC (Intel-based computer) on a PCI expansion card that installs inside an iSeries server.

Integrated xSeries Adapter (IXA). A PCI expansion card that installs inside selected models of IBM eServer™ xSeries servers, providing a high-speed link to an iSeries server.

Internet Protocol Security (IPSec). Encrypts traffic on the iSCSI network.

IP Multicast. Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPSec. See Internet Protocol Security.

IQN. See iSCSI qualified name.

iSCSI. Internet SCSI. Encapsulation of the SCSI protocol within TCP/IP packets. Provides an interoperable solution which can take advantage of existing internet infrastructure, internet management facilities and addresses distance limitations.

iSCSI connection. A connection is a TCP connection. Communication between the initiator and target occurs over one or more TCP connections.

iSCSI initiator adapter. A host bus adapter (HBA) that initiates iSCSI requests. iSCSI initiators issue SCSI commands to request services from components, logical units, of a server known as a **target**. The iSCSI Initiator is the iSCSI HBA in the xSeries or BladeCenter server.

iSCSI qualified name (IQN). A unique name that identifies an iSCSI target adapter or an iSCSI initiator adapter as defined by the iSCSI standard (RFC 3722).

iSCSI target adapter. A host bus adapter (HBA) that services iSCSI initiator requests. An iSCSI target serves as a storage controller, hosting the logical units (LUNs). In the context of iSeries iSCSI attached servers, the iSCSI target is the iSCSI HBA for iSeries.

Kerberos. A network security protocol created by MIT. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. iSeries Navigator provides Kerberos authenticated sign-on. User Administration supports the single sign-on environment by allowing i5/OS user profile passwords to be defined to be *NONE and to allow enrolled Windows users to set their passwords in Windows. This support is provided when an enrolled user profile attribute is specified as LCLPWDMGT(*NO).

local interface. The local interface represents the configuration parameters that describe the iSCSI target adapter located in the iSeries server.

MAC. See Media Access Control.

Management Module. A high function service processor that is used to control an IBM BladeCenter chassis and the individual servers within it.

Media Access Control (MAC). In a local area network, the protocol that determines which device has access to the transmission medium at a given time.

Microsoft Windows Cluster Service (MSCS). Service in Microsoft Windows which links individual servers so they can perform common tasks.

network server configuration (NWSCFG). An i5/OS configuration object which describes attributes used with an iSCSI attached remote integrated server. Attributes include the remote system (*RMTSYS), the service processor on the remote system (*SRVPRC) or the configuration security values used to communicate with the server (*CNNSEC). The corresponding i5/OS object type is *NWSCFG.

network server description (NWSD). An i5/OS configuration object which describes an integrated server. The corresponding i5/OS object type is *NWSD.

network server host adapter (NWSH). A network server host adapter (NWSH) is an i5/OS configuration object that is used to configure the iSCSI HBA device in the iSeries server. The corresponding i5/OS device type is *NWSH.

network server storage space (NWSSTG). i5/OS disk storage allocated to an integrated server.

NWSH. See network server host adapter (NWSH).

point to point virtual Ethernet. A virtual Ethernet network configured between an iSeries and an integrated Windows server during its installation. It is the link that is used for communication between the iSeries and an integrated server.

remote interface. The remote interface represents the configuration parameters that describe the iSCSI initiator adapter located in the xSeries server or IBM BladeCenter server. The remote interface includes parameters for both the SCSI and LAN functions of the adapter.

remote system ID. The identifying serial number, type and model of the xSeries server or IBM BladeCenter server. For a standard xSeries server, the service processor and the xSeries server share a common identifier. For an IBM BladeCenter server, this identifies the server within a chassis.

remote system network server configuration. An i5/OS configuration object that is used to configure attributes that are specific to a particular remote xSeries or IBM BladeCenter server. This includes information that is necessary to identify and boot the remote system and information about the iSCSI initiator adapters that the remote system uses. The corresponding i5/OS object type is *NWSCFG with a subtype of *RMTSYS. This object is also referred to using the shorter term **remote system configuration**.

Remote Supervisor Adapter (RSA). A high function service processor that is used to control xSeries systems.

service processor. A processor that is separate from the main CPU of the system. The service processor is used to control power and perform other management and diagnostic functions for the system. There are several different types of service processors that are used with integrated xSeries and IBM BladeCenter systems. See **Remote Supervisor Adapter (RSA)**, **Baseboard Management Controller (BMC)** and **Management Module**.

service processor network server configuration. An i5/OS configuration object that holds the set of parameters that relate to the service processor on the remote system. In the case of IBM BladeCenter servers, this represents the IBM BladeCenter enclosure. The corresponding i5/OS object type is *NWSCFG with a subtype of SRVPRC. This object is also referred to using the shorter phrase **service processor configuration**.

storage path. The storage path defines which Network server host adapter (NWSH) the storage spaces can use and the IP security rule to use to secure the data traffic.

target node. iSeries iSCSI firmware object that manages the iSCSI session and connection.

unicast. Transmission of data to a single destination.

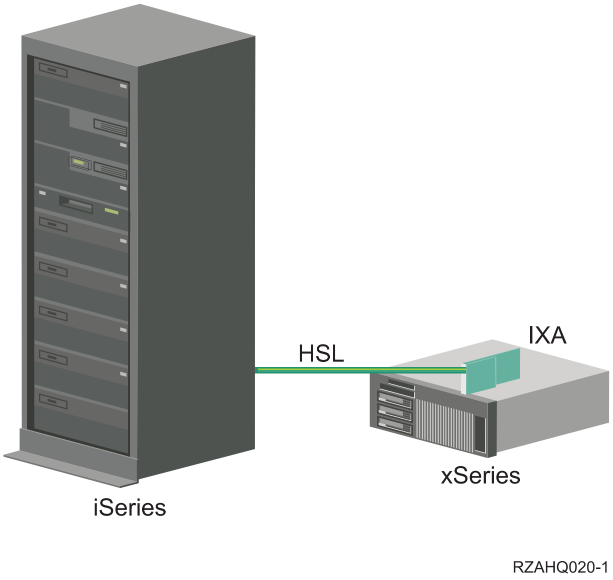
virtual network. An Ethernet network emulated inside the iSeries to allow networks to be created between i5/OS logical partitions, Linux logical partitions, and integrated Windows servers.

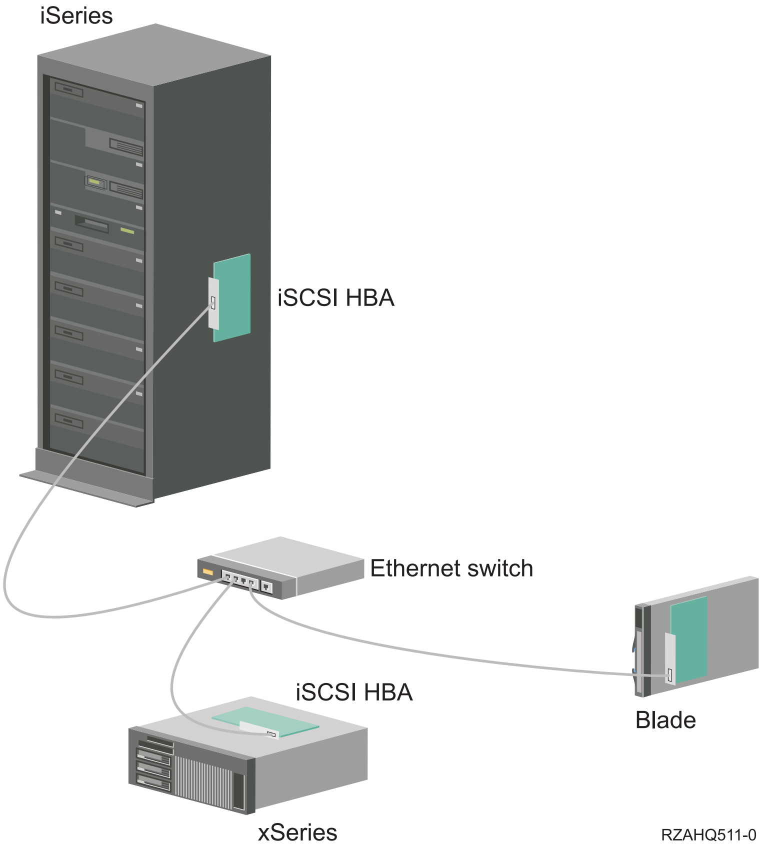
Windows server. Microsoft Windows 2000 Server or Windows Server 2003

Windows Server 2003 Volume Shadow Copy Service. Support that allows application data to be backed up without ending the application. This service improves application availability.

Hardware concepts

iSeries servers support several hardware configurations to integrate IBM xSeries or BladeCenter servers. The following table introduces the essential differences between an Integrated xSeries Server (IXS), an Integrated xSeries Adapter (IXA) attached xSeries server, and an iSCSI attached server.

Comparison of IXS, IXA and iSCSI HBA attached xSeries servers.	
IXS iSeries RZAHQ019-1	An IXS is a diskless PC Server with processor and memory that is installed inside an iSeries server.
	An IXA is a high-speed link (HSL) bus adapter plugged into a supported xSeries server. The xSeries server appears as an HSL attached expansion unit to the iSeries server.

Comparison of IXS, IXA and iSCSI HBA attached xSeries servers.	
 iSeries iSCSI HBA Ethernet switch iSCSI HBA Blade xSeries RZAHQ511-0	iSCSI technology attaches both diskless xSeries servers and IBM BladeCenter servers to iSeries systems using low cost, scalable Ethernet networks. There are iSCSI host bus adapters (HBAs) in the iSeries server, in each participating xSeries server, and on each participating IBM BladeCenter server.

IXS and IXA attached servers

Typical IXS server installation

The following graphic illustrates a typical IXS installation.

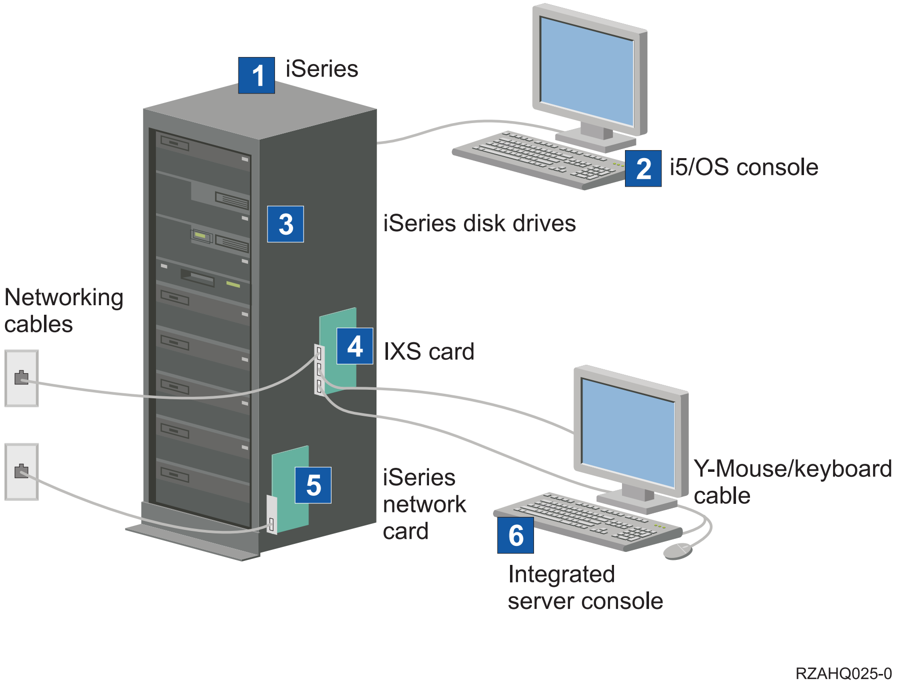


Figure 2. A typical IXS installation

1. You need a compatible iSeries server. (See "Hardware requirements" on page 57 for compatibility information.)
2. The i5/OS console, from which you connect to the iSeries server using iSeries Navigator or the character-based interface, is shown to make clear the distinction between it and the integrated server console.
3. An integrated server does not have its own hard disk drive. i5/OS emulates hard disk space for it to use from the iSeries hard disk drives.
4. The IXS card is an Intel processor with its own RAM, mounted on a PCI board and plugged into an iSeries expansion slot. The IXS physically occupies two slots.
5. A typical iSeries server will have a network card.
6. An integrated server console allows you to interact with the integrated server. An integrated server console may consist of a monitor, keyboard, and mouse directly attached to the IXS card. For more information about this and other types of integrated server consoles, see "Windows console" on page 24.

Note: Depending on the IXS type, there are different ways to provide network connectivity. Some types of IXSs can 'take over' adjacent PCI slots, allowing the IXS to control an iSeries network card (see "Hardware requirements" on page 57 for information about which network cards are supported). You can install up to three network cards in this way. Other types of IXSs have integrated network controllers and do not support network cards in adjacent slots.

Typical IXA attached server installation

IXA attached integrated servers are standard xSeries server models, containing processors, memory, and expansion cards, but no disks. All the disk space is housed in the iSeries server and managed in the same way as for IXS models.

The installation procedure for an IXA attached integrated Windows server is almost identical to that for an IXS integrated server. The major difference between them is that since new xSeries servers are released more often than IXSs, updated capabilities are available more rapidly. IXA attached xSeries servers also have their own expansion slots, so they are far more expandable than IXSs.

The following graphic illustrates a typical IXA attached server installation.

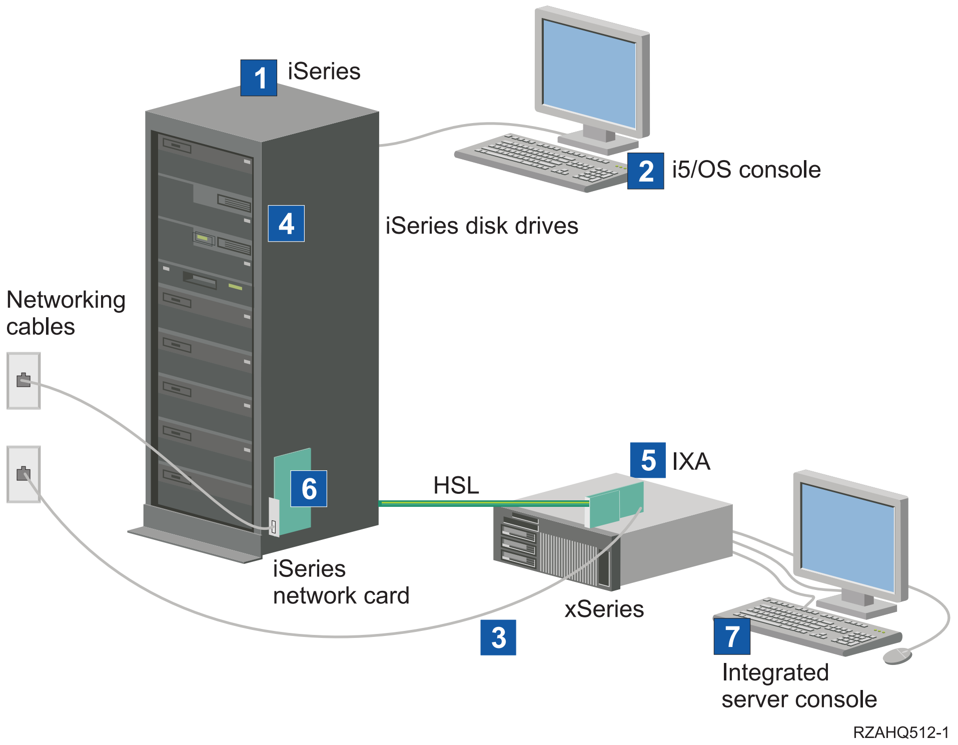


Figure 3. A typical IXA attached server installation

1. You need a compatible iSeries server. (See "Hardware requirements" on page 57 for compatibility information.)
2. The i5/OS console, from which you connect to the iSeries using iSeries Navigator or the character-based interface, is shown to make clear the distinction between it and the Windows console.
3. A typical xSeries server will have at least one integrated network controller. Additional network cards can be added to most xSeries servers to further enhance network connectivity. Information about xSeries network card compatibility can be found on the System i integration with BladeCenter and System x web site.
4. An IXA attached xSeries server does not have its own hard disk drive. i5/OS emulates hard disk space for it to use from iSeries hard disk drives.
5. The IXA card plugs into a specific slot in the xSeries server and is attached to the iSeries via HSL cables.
6. A typical iSeries server will have a network card.
7. A integrated server console allows you to interact with the IXA attached xSeries. An integrated server console may consist of a monitor, keyboard, and mouse directly attached to the xSeries server. For more information about this and other types of integrated server consoles, see "Windows console" on page 24.

iSCSI attached servers

Typical iSCSI attached IBM xSeries or BladeCenter server installation

iSCSI attached servers are standard xSeries or IBM BladeCenter server models that have processors, memory, and expansion cards, but no disks. All of the disk space is in the iSeries server and managed in the same way as for IXS and IXA models.

The installation procedure for an iSCSI attached integrated Windows server requires hardware to be installed and configured in the iSeries and xSeries or IBM BladeCenter servers. As in the IXA, the iSCSI HBA attached xSeries servers have their own expansion slots, so additional options can be installed to expand the capabilities of the server.

The following graphic illustrates a typical iSCSI HBA installation:

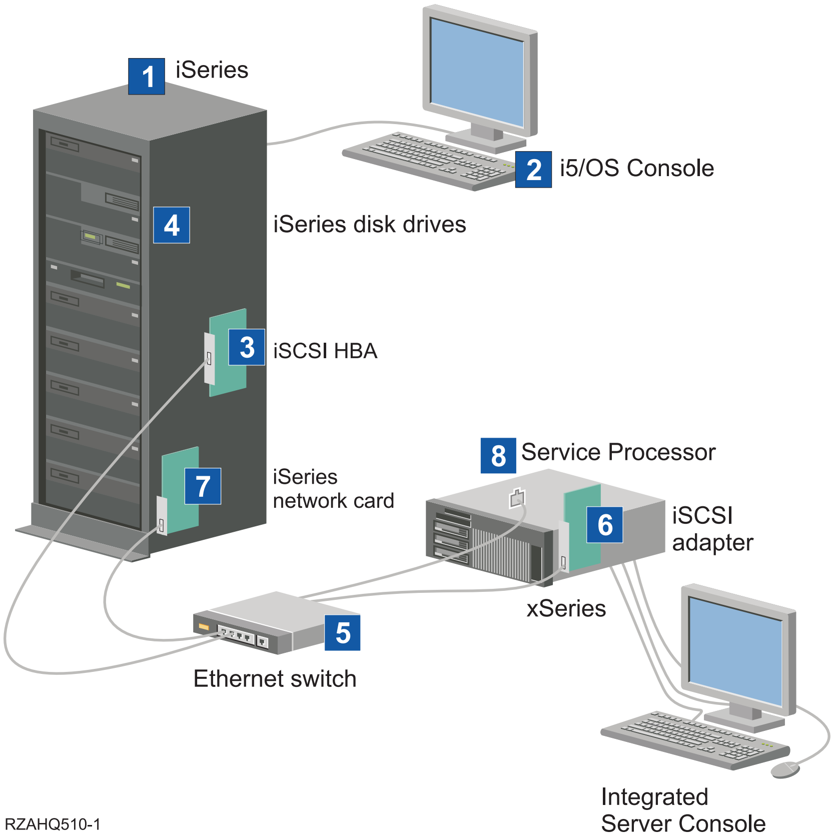


Figure 4. A typical iSCSI attached server or IBM BladeCenter installation

1. You need a compatible iSeries. See “Hardware requirements” on page 57 for compatibility information.
2. The i5/OS console, from which you connect to the iSeries using iSeries Navigator or the character-based interface, is shown to make clear the distinction between it and the Windows console.
3. Depending on the type of the physical network, copper or fiber iSCSI HBAs are available. This iSCSI adapter serves as the target device and connects to an Ethernet network using standard Ethernet cables.
4. An integrated server does not have its own hard disk drive. i5/OS emulates hard disk space for it to use from iSeries hard disk drive. These drives and other iSeries 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 xSeries server. This adapter provides the connection to the iSCSI HBA for iSeries. This adapter can be viewed from the xSeries server as the storage adapter, where the disks are found across the network.

7. A typical iSeries server will have a network card. An iSeries LAN connection is required by IBM Director to discover and manage the remote xSeries or IBM BladeCenter servers.
8. A service processor allows the iSeries server to discover and manage the remote system. The service processor may be a Remote Supervisor Adapter (RSA II), a Baseboard Management Controller (BMC), or a Management Module of an IBM BladeCenter. The RSA II, BMC, or Management Module is connected to the iSeries server over an Ethernet network.

For additional hardware information check the System i integration with BladeCenter and System x web site.
(www.ibm.com/systems/i/bladecenter/)

iSCSI attached server overview

A basic iSCSI network consists of an iSCSI target (an iSCSI HBA installed in an iSeries server) and an iSCSI initiator (an iSCSI HBA that is installed in an xSeries or IBM BladeCenter server). These target and initiator devices are connected over an Ethernet Local Area Network (LAN). The iSCSI HBA for iSeries provides the storage and removable media devices for the iSCSI Initiator. Figure 5 illustrates a basic iSCSI network.

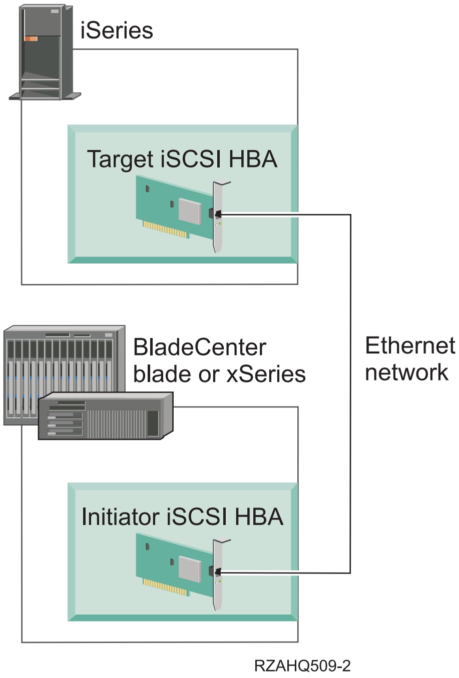


Figure 5. Basic iSCSI concepts

Both the iSCSI target and initiator must be configured with commands issued on the iSeries server. The iSCSI network is only used for iSCSI HBA traffic.

Basic single server support

To attach or host an xSeries or IBM BladeCenter server via iSCSI to an iSeries, hardware must be installed in both the iSeries and the hosted system. The hardware required at each end is an iSCSI host bus adapter (HBA) or iSCSI adapter. These two adapters are connected via an Ethernet switch, using standard Ethernet cables. The simplest form of the physical connection between a hosted system and an iSeries server is illustrated in Figure 6 on page 19.

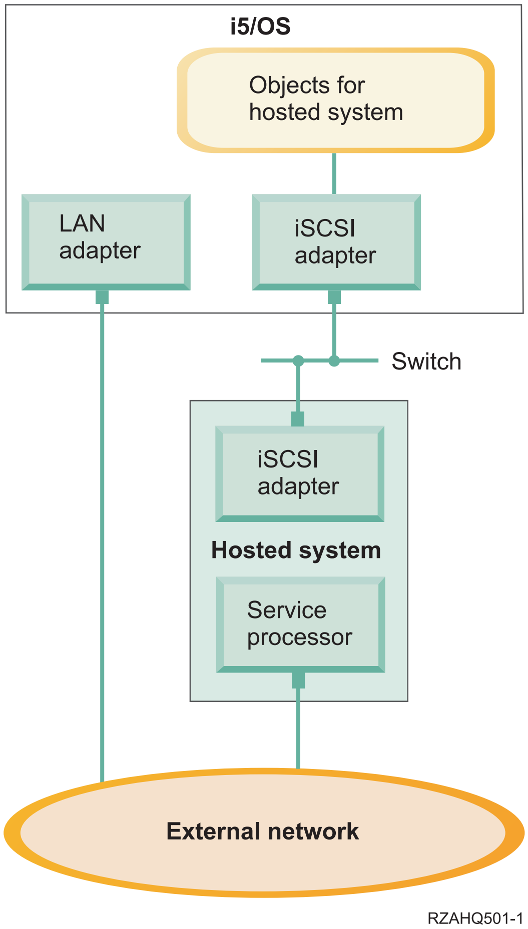


Figure 6. Single iSCSI attached server

The xSeries or IBM BladeCenter server known as the hosted system has an initiator iSCSI HBA installed. This adapter has an Ethernet network interface and it is connected via an Ethernet switch to the target iSCSI HBA installed in the iSeries server. The hosted system is a diskless server. The virtual disks and virtual removable media devices are hosted or provided by the iSCSI HBA for iSeries. The SCSI commands to access these devices are packaged in TCP/IP frames and travel from the hosted system to the iSCSI HBA for iSeries over the Ethernet network. 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" on page 37.

i5/OS can locate and manage remote systems by sending commands to the service processor of the remote system over an Ethernet network. IBM Director is used for these functions and must be installed and running on all partitions that are connected to iSCSI attached host bus adapters (HBAs). For more information, see "Remote server discovery and management" on page 142.

Two distinct networks are illustrated in Figure 6. The iSCSI network uses an isolated switch. The service processor connection uses an external network (shared network). There does not have to be two distinct networks. For example, the service processor connection could use the same isolated switch as the iSCSI network. This is one way to secure the service processor connection. However, the i5/OS 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 "Security concepts" on page 48.

Multiple server support

A single iSCSI HBA for iSeries can host multiple xSeries or IBM BladeCenter servers. This concept is illustrated in Figure 7.

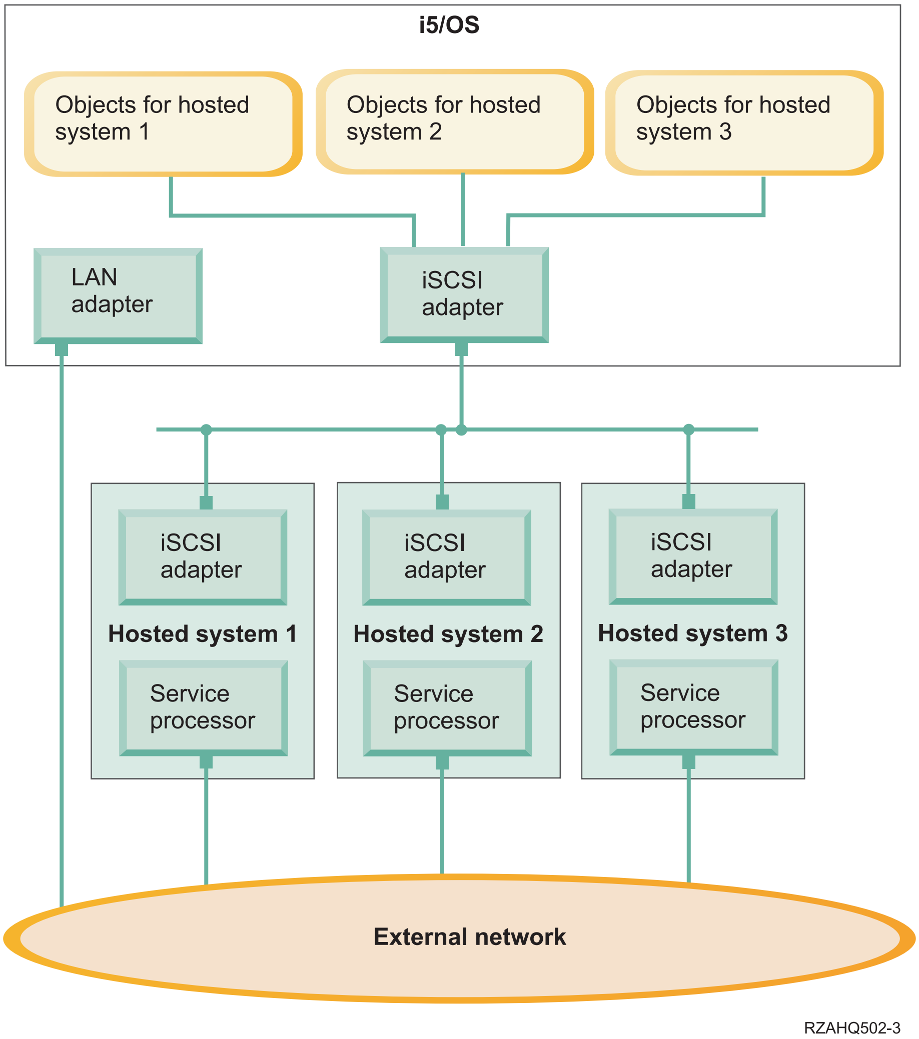


Figure 7. Multiple iSCSI attached servers

Each hosted system requires at least one iSCSI HBA to be installed in the server. Each iSCSI HBA in the hosted system is connected over an Ethernet network to the iSCSI HBA for iSeries. This network can be a physically secure or isolated network when a physically secure model is implemented. In i5/OS each of the hosted systems or remote systems are represented by a set of objects. These objects are described in more detail in "Software concepts" on page 37.

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

Advanced iSCSI support

A single target iSCSI HBA installed in the iSeries system 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 8 illustrates a hosted system that is connected to more than one target iSCSI HBA in the iSeries system.

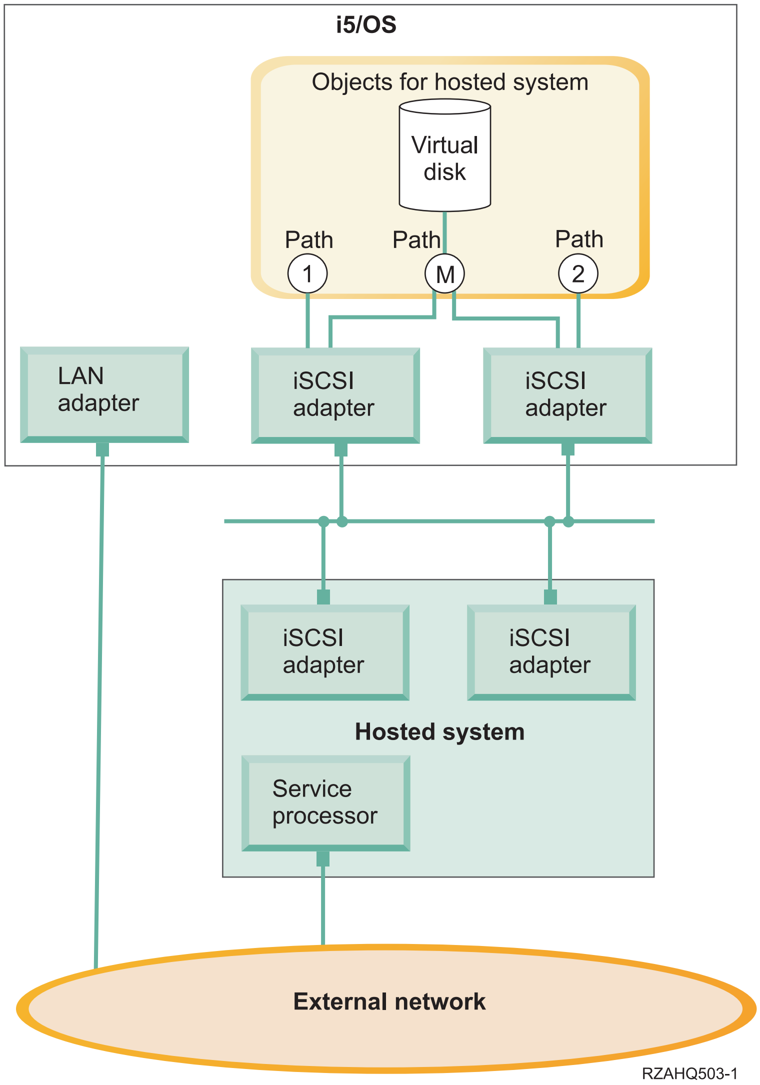


Figure 8. Advanced configuration

Figure 8 shows multiple iSCSI HBAs installed in the hosted system.

Paths

Paths are connection points between virtual devices and iSCSI HBAs in the iSeries system. 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.

iSeries 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 8. These are labelled 1, 2 and M.

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

Single paths
Virtual storage or devices that are linked to a specific iSCSI HBA can only be accessed through that adapter.

In Figure 8 on page 21, paths 1 and 2 represent specific target iSCSI HBAs in the iSeries system. Devices defined in path 1 can only be accessed by the iSCSI adapter port for which the path is defined. Similarly, devices defined in path 2 can only be accessed by the iSCSI adapter port for which the path is defined. Any devices that are linked to path 1 or 2 are said to be linked exclusively to that iSCSI HBA.

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 should 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 8 on page 21 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 iSeries system
- Configure multiple iSCSI initiators in the System x™ or blade system
- Configure multiple switches
  - If you are using an IBM 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 can not 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” on page 138 for more information about installing the required software components and linking storage for the integrated server.

Diskless booting over iSCSI

All of the iSCSI attached stand alone or IBM BladeCenter servers are diskless and require an xSeries or IBM BladeCenter iSCSI host bus adapter (HBA) as a boot device.

Both the i5/OS remote system configuration and the remote server iSCSI HBA must be configured before you install or use a new integrated Windows server. See “Remote system configuration” on page 43.

The iSCSI HBA must be configured during the xSeries or IBM BladeCenter boot process using the adapter CTRL-Q utility. It is recommended that it is configured as part of the initial server set up. There is a minimal set of parameters required to be configured in the hosted server iSCSI HBA. These parameters need to be matched to those parameters configured in the remote system configuration object. The parameters vary depending on the selected boot mode.

See the iSCSI install read me first web page for details on how to configure the hosted system iSCSI HBA as the iSCSI boot device. For details on how to configure the set of parameters in the remote system configuration object, see “Change remote system configuration properties” on page 122.

Enabling the hosted server boot device

The iSCSI HBA installed in an xSeries or IBM BladeCenter acts as a boot device during the boot process, based on the configured parameters.

When the xSeries has only one iSCSI HBA, this adapter needs to be configured as the boot device. iSCSI boot is supported on all iSCSI HBAs, but you must configure additional information.

When the xSeries server has multiple iSCSI HBAs installed, only one iSCSI HBA is required to be configured as the boot device.

The IBM BladeCenter server iSCSI HBA is a dual port adapter. Only one port is required to be configured as a boot device.

After configuring multipath I/O for storage path redundancy, you might also want to configure more than one iSCSI HBA port as a boot device. When multiple boot devices are configured, the integrated server will attempt to boot using one of the boot devices. The server will attempt to boot using the next boot device if a boot attempt fails.

Boot Modes and Parameters

The iSeries iSCSI solution supports different boot modes. Depending on the selected boot mode, different boot parameters are required to be configured in the hosted system iSCSI HBA.

The parameters are configured using the adapter CTRL-Q utility. A boot device must be selected and configured the first time a server is being deployed. It is recommended that the required parameters are configured as part of this initial set up process.

Integrated DHCP server

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 HBA. The server is automatically configured with the parameters provided in the remote system configuration when a network server description (NWSD) is varied on. For more information, see “Integrated DHCP server” on page 141.

Remote server and service processor discovery concepts

IBM Director Server is used for remote server discovery and management of iSCSI attached servers. Director Server can be installed without installing the Virtualization Engine and does not require an additional interface. See “Software requirements” on page 59 for information about installing IBM Director.

Windows environment on iSeries uses IBM Director Server to communicate with your integrated server hardware.

- **Remote server and service processor discovery**
  finding the server on the network
- **Power control**
  turning the server on or performing an operating system shutdown for appropriate i5/OS vary configuration commands.
- **Power status retrieval**

- **Configuration of the remote server**
  Some remote server functions can be configured from the iSeries remotely through the remote server's service processor.

For information about configuring IBM Director and the service processor for your integrated server hardware, see "Configure remote server and service processor discovery" on page 142.

Windows console

You interact with your integrated server using a Windows console. Depending on your configuration of hardware and software, you can use a monitor, keyboard, and mouse that is attached by one of the following methods:

Directly attached monitor, keyboard, and mouse

You can use a monitor, keyboard, and mouse that are directly attached to the IXS card, an IXA attached xSeries server, or an iSCSI attached xSeries or BladeCenter server, forming the integrated server console. You interact with the integrated server through these devices exactly as you would with a regular personal computer (PC).

The iSCSI attached servers require some preinstallation hardware set up. This set up is performed using the directly attached monitor, keyboard and mouse.

Remote GUI desktop application

You can use an application such as Microsoft Terminal Services, Remote Desktop, or another third party application to display the server's 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.

Virtual serial console

i5/OS provides the ability to connect to a virtual serial console for a type 4812 IXS. This is similar to the i5/OS virtual serial console support that is provided for iSeries logical partitions. It provides a text-mode console for the 4812 IXS server and can be used for various administration tasks that do not require access to a graphical user interface (GUI) desktop. See "Connect to the 4812 IXS virtual serial console" on page 151 for information about how to establish a session with the virtual serial console for a particular 4812 IXS.

The virtual serial console is currently supported for use with Windows Server 2003 only. It can be used to view server errors or to restore communication to the LAN. This console connection can be used before configuring TCP/IP on the server. See the Microsoft Emergency Management Services document (www.microsoft.com/whdc/system/platform/server/default.mspx) for information about the tasks that can be performed using the virtual serial console. Note that:

- i5/OS does most of the configuration for the virtual serial console automatically, so some of the configuration tasks mentioned in the Microsoft documentation are unnecessary for the i5/OS virtual serial console.
- The iSeries implementation does not require any of the additional hardware, such as modems, concentrators, or cables, which are mentioned in the Microsoft documentation.

Remote Supervisor Adapter II Graphical console redirection

For xSeries servers equipped with an RSA II, 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.

Considerations

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

- There may not be a diskette drive available. This means that you cannot use a startup diskette or an emergency repair diskette. However, you can use iSeries disk space to back up your files or the entire disk image.
- iSeries tape and disk devices are available.
- LAN adapters, cables, hubs, or switches are not required for TCP/IP communication with the iSeries server or other integrated servers when using virtual networking.
- Installing the Microsoft Windows operating system with Windows environment on iSeries is different from a typical PC server installation. You first install IBM i5/OS Integrated Server Support, then install Microsoft Windows. You enter much of the configuration information with the i5/OS Install Windows server (INSWNTSVR) command, so some of the typical installation panels do not appear. This command also includes some additional parameters that are specific to integrating the server with i5/OS, such as synchronize date and time.
- On the i5/OS side of server management, an integrated Windows 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.
- You can do a lot of your user administration tasks from i5/OS, such as creating Windows users.
- Because i5/OS manages storage differently than a PC server (see “i5/OS storage management” on page 159), some techniques necessary to administer storage on a PC server are unnecessary for integrated servers.

Performance

The IXS, IXA, and iSCSI attached servers have their own memory and one or more processors, but share the iSeries hard disk drive storage through virtual (simulated) disk drives. The disk drives are allocated to Windows by creating a storage space object on the iSeries. 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 iSeries storage spaces as virtual disks. iSeries integrated servers also include optional features such as Windows drivers to share iSeries tape drives, CD and DVD drives, along with high speed virtual Ethernet adaptors.

The use of iSeries 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.

Use the following links to see more performance-related information:

- “iSeries storage spaces versus dedicated disks” on page 26
- “Storage space balancing” on page 26
- “iSCSI attached server performance” on page 27
- “Virtual Ethernet” on page 28

- System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/)

- iSeries Performance Management (www.ibm.com/eserver/iseries/perfmgmt)

- Chapter 17 in the System i™ Performance Capabilities Reference

iSeries storage spaces versus dedicated disks

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 iSeries storage, the disk performance is dependent on the iSeries.

Greater disk performance capacity with iSeries shared disks

On most stand-alone 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 iSeries, the virtual disks are spread across more iSeries 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 iSeries disks.

On servers with dedicated disks, the disk response times tend to be relatively steady. For example, 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 may need your attention.

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

Consider the entire group of disks when you evaluate storage bottlenecks

The iSeries server 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 iSeries server 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.

Storage space balancing

When a storage space is created, the data is spread across the disks in a user specified Auxiliary Storage Pool (ASP), or Independent Auxiliary Storage Pool (IASP). 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 iSeries storage architecture, regardless of how an ASP or IASP is configured.

The iSeries sever 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 iSeries. There is no need to configure striped volumes or software RAID of the disks within the Windows operating system. Configuring these features in the Windows operating system may actually slow the effective disk operations. Even though the storage is spread across the iSeries disks in small extents, continue to defragment the associated disk on Windows to maintain efficient file-system data structures.

You can monitor how well the iSeries 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 other performance considerations, realize that integrated servers are Microsoft Windows servers. You can use Microsoft's Windows Performance Monitor as you would on any other server. See your Microsoft Windows documentation for information about using the Performance Monitor.

iSCSI attached server performance

For iSCSI attached servers, there are multiple configuration options to adjust for better performance capacity as needed. Some options may require different target disk configurations or volumes on the integrated servers. See chapter 17 of the Performance Capabilities Reference Guide for more information about iSCSI attached server performance and tuning.

Windows disk configuration

For iSCSI attached integrated servers, the virtual disk drives are optimized for:

- 1 disk partition per virtual drive.
- 2 gigabyte or larger storage spaces.
- NTFS file system formatted with 4 kilobyte or larger cluster sizes.

These guidelines allow the iSeries to efficiently manage the storage space memory, improving the disk performance. These guidelines also affect IXS and IXA attached servers, but to a much smaller degree.

If you use the Change Network Storage Space (CHGNWSSTG) CL command to increase a storage space size, be sure to use the Windows Server 2003 DISKPART command to also increase the size of the partition on Windows.

Note: For better performance, add a storage space to the server instead of adding another disk partition in the new space.

iSeries memory pools

For iSCSI attached servers, the storage operations occur through an iSeries memory pool. This memory essentially acts as a cache to the disk operations, so the size of the memory can affect the Windows disk performance. This I/O does not directly cause page faulting in the base pool. However, since pool memory is shared with other i5/OS applications, Windows disk operations may cause page faulting in other applications, or other applications may induce paging of iSCSI disk operations. In extreme cases, you may need to adjust memory pool sizes or assign applications to other memory pools to mitigate memory problems.

IXS and IXA attached servers do not perform disk operations through a base memory pool. They use reserved memory within the machine pool (System Pool ID 1). Thus, the disk operations do not share memory with other applications.

iSCSI performance configurations

On iSCSI attached integrated servers, if a single network fabric is reaching capacity, you can add channels with additional iSCSI HBAs in both the xSeries and iSeries servers (assuming the interconnecting network also has available bandwidth).

There are several ways that you can spread the iSCSI and network traffic between the separate channels:

- Dedicate SCSI operations to one channel, and virtual Ethernet operations to another.
- Use two storage targets. Each target should be linked to a separate HBA paths. See "Manage iSCSI host bus adapters" on page 132.
  - On Windows, direct applications to use both drives (if possible), or dedicate the drives to different applications to spread the total disk operations between the drives.
  - Configure the two disks in a Windows dynamic volume set with the data striped across the two drives. As applications use the volume, the disk operations will automatically balance across the drives in the volume set.

Virtual Ethernet

The Virtual Ethernet point to point connection is the default virtual network connection between the iSeries hosting 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 iSeries 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 operations on IXS and IXA adapters. 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 iSeries CPU to switch the traffic between servers, even when the iSeries server is not an endpoint of the traffic. For most connections this utilization won't be significant. But, if you expect high sustained network loads across the virtual Ethernet connection between integrated servers, you might want to balance the cost of using the Virtual Ethernet internal switch against external network adaptors on the integrated servers.

Networking concepts

Hosted systems involve several different types of network connections.

Only iSCSI attached systems have the following connection types.

- **"Service processor connection" on page 29**
  This physical connection allows the hosting i5/OS partition to communicate with the hosted system's service processor.
- **"iSCSI network" on page 29**
  This physical network connects iSCSI adapters in the hosting i5/OS partition with iSCSI adapters in the hosted system.

All types of integrated Windows servers may have the following connection types.

- **Virtual Ethernet**
  This is a simulated Ethernet connection that does not require additional networking cards or cables. There are two types of virtual Ethernet
  - **"Point to point virtual Ethernet" on page 32**
    This connection provides general purpose communication between the hosted system and the hosting i5/OS.
  - **"Virtual Ethernet networks" on page 32**
    These are networks created between hosted systems, i5/OS partitions, and other partitions (such as Linux).

- **“External networks” on page 37**
  These are the normal Windows networks which all servers use, created by networking through physical network cards controlled by the hosted system.

Service processor connection

Note: This section pertains only to iSCSI attached systems.

This physical connection is required so that the hosting i5/OS can communicate with the service processor of the hosted system. The connection can consist of a simple, switched network or a more complex, routed network. Windows environment on iSeries uses IBM Director over this connection to manage the state of the hosted system.

At one end of the connection is a LAN adapter or adapters controlled by i5/OS. This LAN adapter can still be available for other uses. The IP address and other attributes of this adapter are controlled using standard i5/OS configuration methods. Windows environment on iSeries does not configure this adapter. It can automatically discover the service processor using IBM Director and 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 server’s power cord is plugged into an energized AC outlet, even if the server is not in a powered on state. On certain xSeries models, a single Ethernet port may be shared by Windows and a particular type of service processor, known as the Baseboard Management Controller (BMC). In this case, the same physical port on the hosted system provides both the service processor connection and an external network connection.

DHCP server for the service processor
Setting the IP address of the service processor may require an external DHCP server on the network providing the service processor connection. The DHCP server should be active before plugging the hosted system’s power cord into an energized 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 hosted operating system.) For more information, see “Dynamic IP addressing (DHCP)” on page 144.

IP multicast
There are several options that Windows environment on iSeries 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 methods” on page 144.

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 “Service processor discovery configuration” on page 143.

iSCSI network

This physical network connects Ethernet iSCSI adapters in the hosting i5/OS with Ethernet iSCSI adapters in the hosted system. It is typically a simple, switched, Gigabit Ethernet network. 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 i5/OS. Each iSCSI adapter 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. For more information, see "Network server host adapters" on page 43. 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, 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 hosted 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 43. This configuration differs from the i5/OS network server adapter object in several ways:

- You can configure an iSCSI adapter port in a hosted 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 a hosted 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 a hosted 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 hosted 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.
- 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.

Notes:

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 Windows hosted system side.
2. 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.

DHCP and DHCP relay

There are several methods for delivering boot information to the hosted system. The default method of delivering IP and storage information to boot Windows uses an integrated Dynamic Host Configuration Protocol (DHCP) server on i5/OS side of the iSCSI network. 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 "Diskless booting over iSCSI" on page 22.

The integrated DHCP server is designed to coexist with any DHCP servers that might also be on the iSCSI network.

If the iSCSI networks includes routers between the iSeries server and the hosted system, and the boot information delivery method is DHCP, then an appropriately configured DHCP relay agent, also known as a BOOTP relay agent, is required in the network.

Performance and maximum transmission unit (MTU)

iSCSI HBAs can use either of the following as a maximum transmission unit (MTU) value:

- 1500 bytes. This is the standard size for Ethernet frames and is the default value in the iSCSI HBA. If you configure an iSCSI HBA to use an MTU of 1500, you do not need to be concerned about Ethernet switch MTU compatibility.
- 9000 bytes. An industry term for frames larger than 1500 bytes is 'jumbo frames'. If you configure an iSCSI HBA to use an MTU of 9000, you must ensure that all network equipment involved, such as switches, is capable of handling an MTU of at least 9000 and is configured to do so. If this condition is not satisfied, the xSeries or blade may fail to boot (typically with only a blinking cursor on the xSeries or blade console).

The MTU setting can affect performance. The MTU value that provides the best overall performance in your environment depends on several factors, including your switch characteristics, your applications, and your CPU resources.

- Of the gigabit Ethernet switches that support an MTU of 9000, some cannot sustain full wire speed with an MTU of 9000 but can with an MTU of 1500. With these switches under heavy traffic, it is possible that using an MTU of 9000 can decrease the performance of both storage and virtual Ethernet. If you are not sure that your switch performs well with an MTU of 9000, you may want to use the standard MTU of 1500.
- As long as switch limitations are not affecting performance, setting the iSCSI HBA and switch MTU configuration to 9000 typically improves performance. Virtual Ethernet performance improves more than storage performance. This is because storage uses TCP/IP hardware in the iSCSI HBAs to process Ethernet frames, while virtual Ethernet uses the System i CPU to process Ethernet frames. For large data transfers over virtual Ethernet, using an MTU of 9000 instead of 1500 reduces System i CPU utilization because there are fewer frames to process.

For information about configuring MTU, see “Maximum transmission unit (MTU) considerations” on page 139

Managing i5/OS iSCSI adapter utilization

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 “Manage iSCSI HBA usage” on page 133.

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

Managing hosted system iSCSI adapter utilization

You can configure an iSCSI adapter in a hosted system with a SCSI IP address, a LAN IP address, or both kinds of IP addresses. The presence of a SCSI IP address enables storage traffic, and the presence of a LAN IP address enables virtual Ethernet traffic. Each Windows virtual Ethernet adapter is normally automatically assigned to a physical iSCSI adapter. There is an option on the advanced properties tab of each virtual Ethernet adapter that allows a particular physical iSCSI adapter to be selected. See “Manage iSCSI HBA allocation at the Windows side of the iSCSI network” on page 136.

IBM does not support the use of the iSCSI adapter as a general purpose external network connection. For more information on external network connections, see “External networks” on page 37.

Other considerations

- 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
There are several ways to secure storage and virtual Ethernet traffic. For more information, see "Security concepts" on page 48.

Point to point virtual Ethernet

i5/OS needs a way to communicate with its integrated Windows servers. This communication takes place over a point to point virtual Ethernet network. When an integrated server is installed a special virtual network is created between it and a controlling i5/OS partition. This network is called point to point because it has only two endpoints, the integrated server and the iSeries, and also because, like a virtual Ethernet network, it is emulated within the iSeries and no additional physical network adapters or cables are used. In i5/OS, it is configured as an Ethernet line description with Port Number value *VRTETHPTP.

When you run the Install Windows server (INSWNTSVR) command it will configure a point to point virtual Ethernet.

You may wonder what makes a point to point virtual Ethernet connection different from a virtual Ethernet network. The answer is that point to point virtual Ethernet is configured differently and can only have two endpoints: the iSeries and an integrated server. 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 Integrated xSeries Server (IXS) and Integrated xSeries Adapter (IXA) attached xSeries servers, these addresses take the form of 192.168.xxx.yyy, where (xxx and yyy can be from 1 to 2 digits.) For example, for an IXS that is defined with hardware resource number LIN0**3**, the IP address will be 192.168.**3**.yyy.

For iSCSI hardware, 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 side of the point to point network will be given the IP address 192.168.100.1, and the Windows side has 192.168.100.2. As you define multiple line descriptions for the same hardware resource, yyy is incremented.

You can allow 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.

Virtual Ethernet networks

Virtual Ethernet networks are flexible and can be configured in many different ways.

Virtual Ethernet networks that do not include more than one logical partition

For the procedure explaining how to create virtual Ethernet networks, see "Configure virtual Ethernet networks" on page 111.

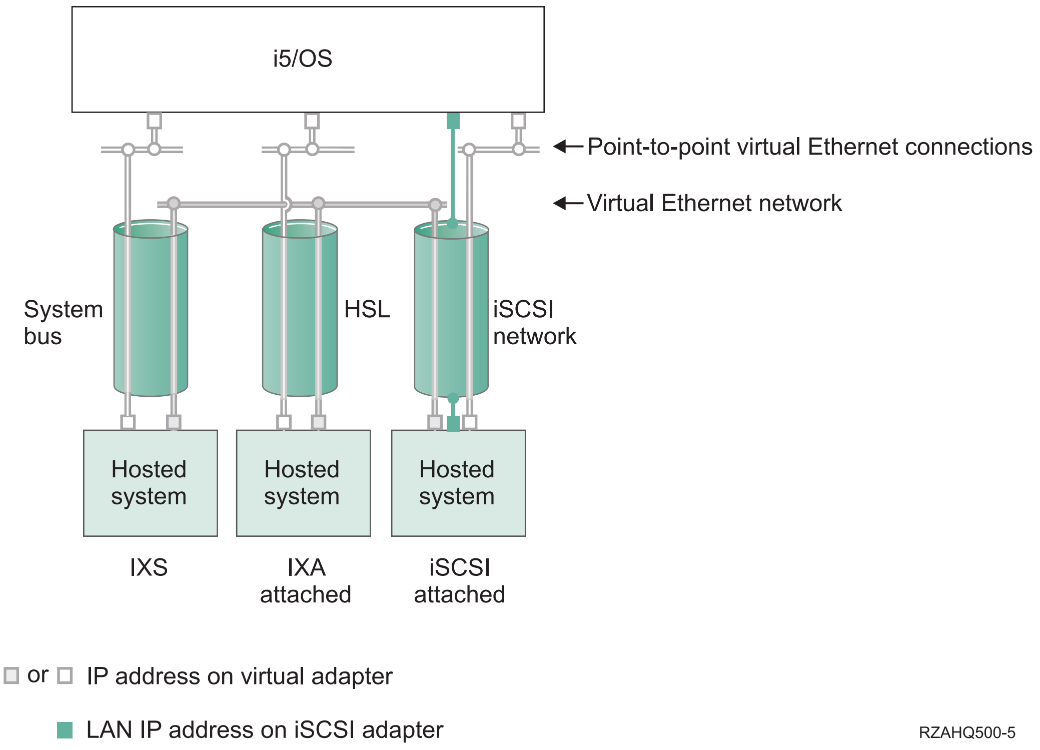


Figure 9. System bus, HSL, and iSCSI network tunnels

IXSs, IXA attached systems, and iSCSI HBA attached systems can all participate in virtual Ethernet networks and can communicate with each other.

- For IXSs, virtual Ethernet traffic flows over iSeries system buses.
- For IXA attached hosted systems, virtual Ethernet traffic flows through HSL cables.
- For iSCSI attached hosted systems, 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 in your iSeries server.
  - 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
  - With IPSec enabled, traffic through an iSCSI network is encrypted. You can think of virtual Ethernet as a powerful Virtual Private Network (VPN). Virtual Ethernet with IPSec can secure an entire virtual network, in contrast to typical VPNs which have just two endpoints

    Note: Each iSCSI HBA interface can have two IP addresses, one for storage and one for LAN function, which is used to tunnel virtual Ethernet. i5/OS TCP/IP is not aware of these IP addresses. For iSCSI HBAs, virtual Ethernet is tunneled through a physical network with iSCSI HBAs at the physical endpoints.

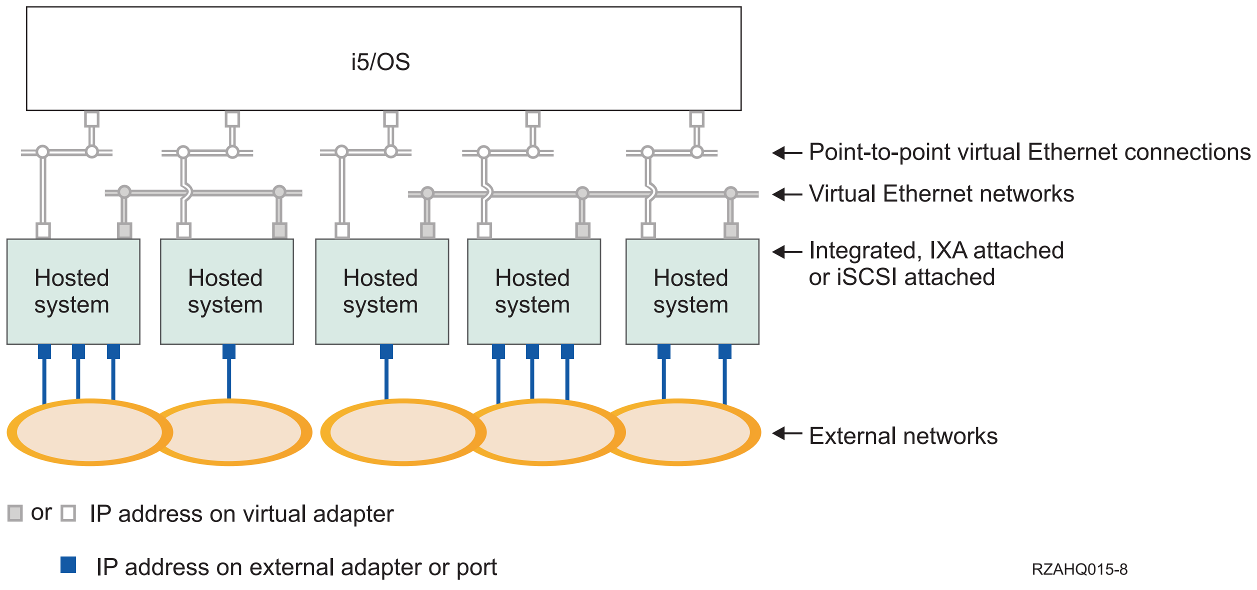

i5/OS
Point-to-point virtual Ethernet connections
Virtual Ethernet networks
Integrated, IXA attached
or iSCSI attached
Hosted system
Hosted system
Hosted system
Hosted system
Hosted system
External networks
or IP address on virtual adapter
IP address on external adapter or port
RZAHQ015-8

Figure 10. Two isolated groups of integrated Windows servers on the same iSeries server. Each group has its own virtual Ethernet network.

Figure 10 is intended to help you understand how virtual networks work within the iSeries. 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 (in white). The blue boxes on the bottom of the integrated servers represent physical network adapter cards which 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 (in grey). Each integrated server can participate in up to four virtual Ethernet networks simultaneously.

This type of connection is required when configuring a group of integrated servers for clustering.

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 having NWSDs configured with the same port number values are connected to the same virtual Ethernet network. When installing a new integrated server, the Install Windows server (INSWNTSVR) command can automatically create the required line descriptions and assign them IP addresses. In the graphic, the i5/OS side of the line descriptions is not shown. Unlike when you use virtual Ethernet, you should configure a TCP/IP address on the i5/OS side of a line description that is used in a virtual Ethernet network.

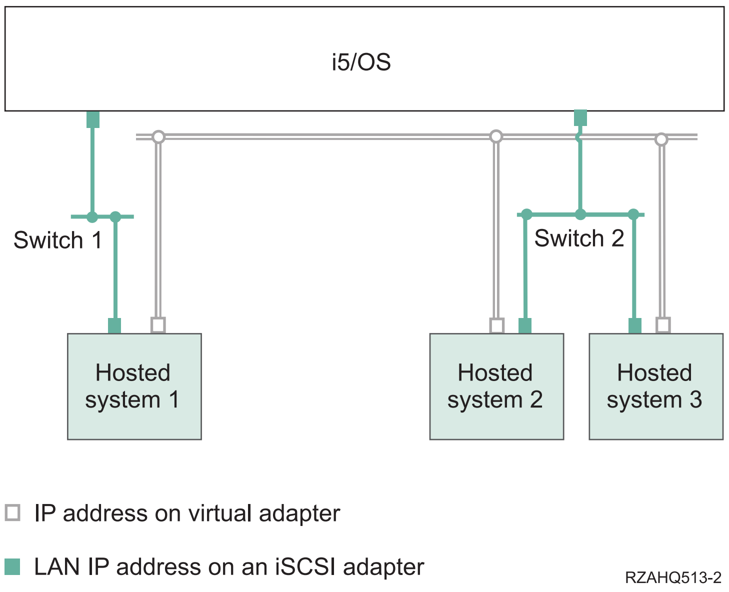


Figure 11. Virtual Ethernet tunneled through iSCSI networks

Virtual Ethernet tunneled through iSCSI networks has some special characteristics that are illustrated in Figure 11.

- Hosted system 1 can communicate with Hosted system 2 and with Hosted system 3, even though separate iSCSI networks (separate physical switches) are involved.
- Virtual Ethernet communication between Hosted system 2 and Hosted system 3 involves the iSeries system, even though both of these hosted systems are connected to the same physical switch.
- There is a pair of LAN IP addresses on the physical iSCSI network involved for each hosted system's virtual Ethernet communication. The pair for hosted system 2 and the pair for hosted system 3 have an IP address in common on the i5/OS side.

Virtual Ethernet networks that include more than one logical partition

For the procedure explaining how to create virtual Ethernet networks, see "Configure inter-partition virtual Ethernet networks" on page 112.

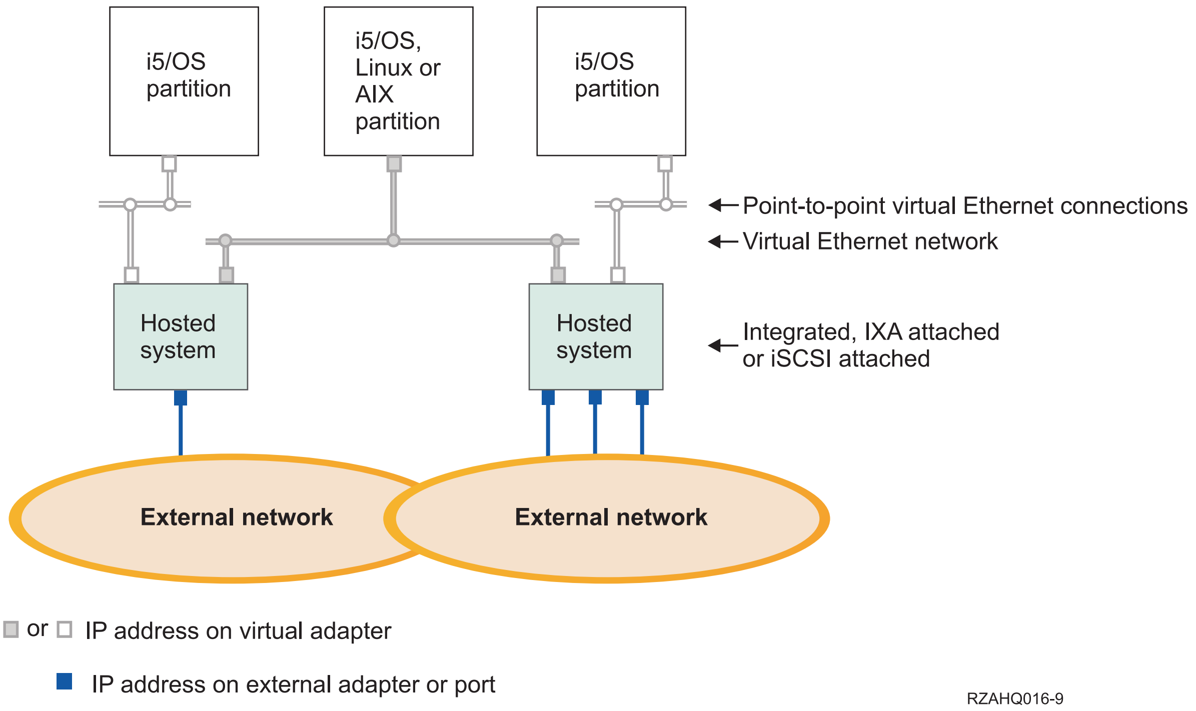

i5/OS partition
i5/OS, Linux or AIX partition
i5/OS partition
Point-to-point virtual Ethernet connections
Virtual Ethernet network
Hosted system
Hosted system
Integrated, IXA attached or iSCSI attached
External network
External network
▨ or □ IP address on virtual adapter
■ IP address on external adapter or port
RZAHQ016-9

Figure 12. A simple, inter-partition virtual Ethernet network.

Now the iSeries has been partitioned, creating three separate virtual i5/OS logical partitions inside the iSeries. Three virtual networks are represented in the graphic; two point to point virtual Ethernet networks (in white) and one virtual Ethernet network (in grey). 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 other operating system. This is called an inter-partition Ethernet network.

In servers without a Hardware Management Console (HMC), inter-partition connections exist between partitions using the same network number, and integrated servers are connected only if their controlling i5/OS partitions are connected. Network numbers 0-9 are pertinent to integrated servers. For example, if an i5/OS partition is configured for inter-partition connections on networks 1 and 5, then integrated servers controlled by that partition can participate in inter-partition communication on ports *VRTETH1 and *VRTETH5. The procedure to do this is in the iSeries Navigator online help. You can also refer to Logical partition concepts for an overview.

In servers with a Hardware Management Console (HMC), inter-partition connections exist between partitions or integrated servers using the same virtual LAN ID. 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 having a virtual LAN ID. You create the virtual adapter using the HMC. For more information, see the Partitioning with an eServer i5 topic and Configuring a virtual Ethernet adapter for i5/OS 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 will 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 simply using the same virtual Ethernet port number.

External networks

An integrated Windows server can participate in external networks just as you can with a normal PC server. There are different ways to do this. In an IXA or iSCSI attached integrated server there are PCI expansion slots available, so you can use any integrated network adapter or install a network adapter card as you would in a PC. An IXS is a PC server on a card which is installed in a PCI slot within the iSeries. It has no PCI expansion slots. Some IXSs can control the iSeries PCI slot adjacent to where it is installed, and in this way ’take over’ an iSeries network adapter. In addition, type 2892 and 4812 IXS models contain an integrated Ethernet network adapter.

For the procedure explaining how to physically install network adapter cards for your IXS or xSeries and how to configure them for use with integrated servers, see “External networks” on page 114.

Software concepts

i5/OS provides support for defining, configuring and managing integrated servers, regardless of the type of integrated server hardware. See the following diagrams for a description of the i5/OS objects that are used for the various hardware configurations. See “Hardware concepts” on page 13 for a description of the hardware configurations that are supported.

For information about the i5/OS software configuration, see the following information.

- “Integrated xSeries Server (IXS) and Integrated xSeries Adapter (IXA) attached xSeries servers”
- “iSCSI attached xSeries and IBM BladeCenter servers” on page 41
- “iSCSI attached xSeries and BladeCenter servers with security objects” on page 45

Integrated xSeries Server (IXS) and Integrated xSeries Adapter (IXA) attached xSeries servers

i5/OS represents IXS and IXA attached xSeries servers in similar ways.

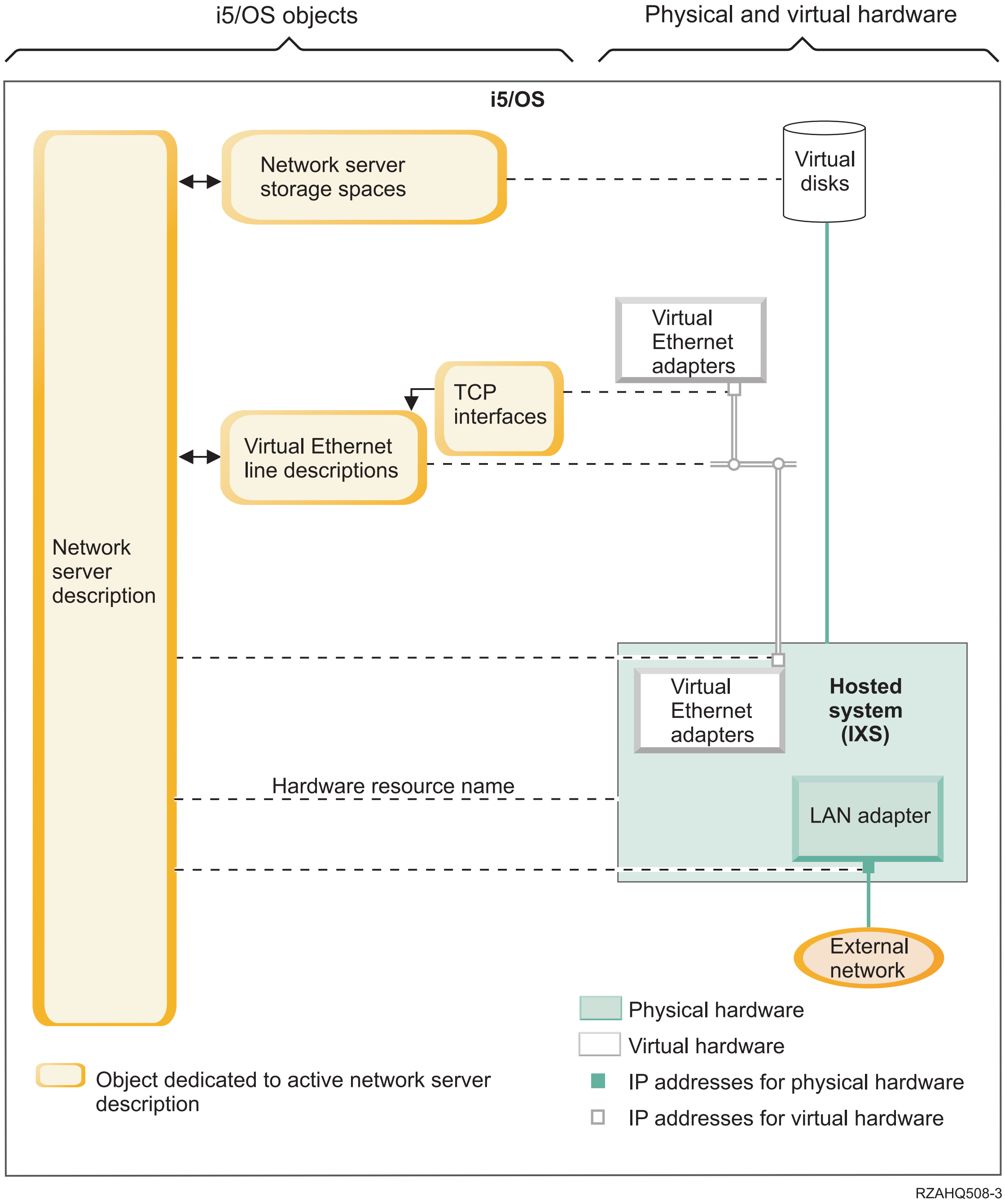

i5/OS objects
Physical and virtual hardware
i5/OS
Network server description
Network server storage spaces
Virtual disks
Virtual Ethernet adapters
TCP interfaces
Virtual Ethernet line descriptions
Virtual Ethernet adapters
Hosted system (IXS)
Hardware resource name
LAN adapter
External network
Physical hardware
Virtual hardware
IP addresses for physical hardware
IP addresses for virtual hardware
Object dedicated to active network server description
RZAHQ508-3

Figure 13. IXS Configuration objects in i5/OS

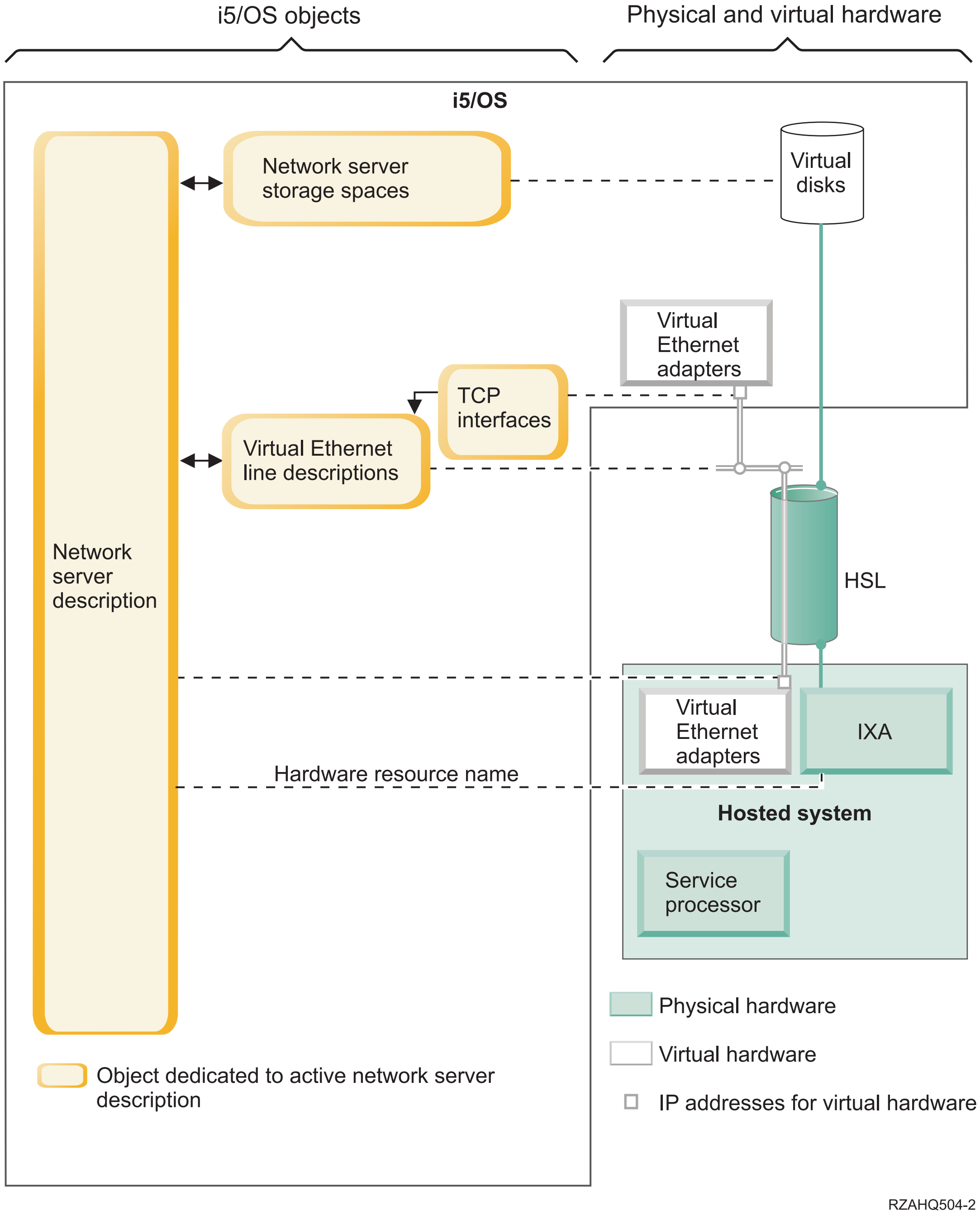

i5/OS objects
Physical and virtual hardware
i5/OS
Network server storage spaces
Virtual disks
Virtual Ethernet adapters
TCP interfaces
Virtual Ethernet line descriptions
Network server description
HSL
Virtual Ethernet adapters
IXA
Hardware resource name
Hosted system
Service processor
Physical hardware
Virtual hardware
IP addresses for virtual hardware
Object dedicated to active network server description
RZAHQ504-2

Figure 14. IXA configuration objects in i5/OS

Figure 14 shows the key i5/OS objects as well as key hardware components that are used for IXS and IXA attached xSeries servers.

See the following sections that describe the objects in Figure 13 on page 38 and Figure 14.
- "Network server description" on page 40
- "Hardware resource name" on page 40
- "Network server storage spaces" on page 40
- "Virtual Ethernet line descriptions" on page 41
- "TCP/IP interfaces" on page 41

- “System bus and HSL data flows” on page 41

Network server description

The network server description (NWSD) in Figure 13 on page 38 and Figure 14 on page 39 is the key i5/OS configuration object for all types of integrated servers. The NWSD object is used to tie together all of the other i5/OS objects that relate to an integrated server. For example, it contains a reference to the hardware that the server runs on, links to the virtual disk drives that the server uses, references to the network ports that the server uses and many other attributes of the server. The i5/OS Install Windows Server (INSWNTSVR) command is used to create the server’s NWSD and several other i5/OS objects that are needed by the server.

For a description of the values that the NWSD contains, see the i5/OS Create Network Server Description (CRTNWSD) command.

For an integrated server, the IXS and IXA attached xSeries server hardware is controlled by i5/OS.

- An integrated server is started by varying on the NWSD for that server. This initiates the Windows operating system boot process.
- An integrated server is shut down by varying off the NWSD for that server. This initiates the Windows operating system shut down process.
- For an IXS, i5/OS communicates directly with the IXS hardware to perform the start and shut down tasks.
- For an IXA attached xSeries server, i5/OS communicates over a high speed link (HSL) bus with the IXA that is installed in the xSeries server to initiate the start and shut down tasks. The IXA in turn communicates with the service processor (SP) of the xSeries system to perform the start and shut down tasks.

Note: Since the IXA provides a hard-wired connection to the xSeries service processor, an i5/OS object is not needed to configure the xSeries service processor characteristics.

Hardware resource name

For both IXS and IXA attached xSeries servers, i5/OS represents the server hardware by a hardware resource name (for example, LIN23). A reference to the hardware resource name for an IXS or IXA attached xSeries server is stored in the NWSD object. See Figure 13 on page 38 and Figure 14 on page 39.

Note: Since the hardware that an IXS or IXA attached xSeries server runs on is defined via the hardware resource name in the NWSD, it is easy to switch the hardware that an integrated server runs on. This is useful in situations where the IXS or IXA attached xSeries server hardware fails since the integrated server can quickly be switched from the failed hardware to compatible ″hot spare″ hardware and started again using the spare hardware. For more information about this ″hot spare″ capability, see “Hot spare between server hardware” on page 156.

Network server storage spaces

A network server storage space (NWSSTG) represents a virtual disk drive that the server uses. See Figure 13 on page 38 and Figure 14 on page 39. Virtual disk drives can vary in size from 1 MB to 1000 GB each. Up to 64 virtual disk drives 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 disk drives 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 INSWNTSVR command, but can also have user-defined virtual disk drives.

- The system drive (typically the C: drive) contains the Windows server operating system (such as Windows Server 2003).
- The install drive (typically the D: drive) contains a copy of the Windows server installation media as well as the portion of the i5/OS Integrated Server Support (product 5722-SS1 option 29) code that runs

on the Windows server. The install drive is used during the Windows installation process and is also used every time the server is started to pass configuration information from i5/OS to the server.

- Additional user-defined drives are typically used for server applications and data.

The actual disk storage for the virtual disk drives is allocated from the i5/OS integrated file system (IFS). 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 (IASP).

See Chapter 9, "Manage storage," on page 159 for more information about virtual disk drives.

Notes:

1. Since virtual disk drives are objects in the i5/OS IFS, an entire virtual disk drive image can be backed up and restored using the i5/OS Save (SAV) and Restore (RST) commands. Files on a virtual disk drive can be backed up individually from i5/OS using file level backup with the Network Client (QNTC) file system in the IFS or using a native Windows backup application. See Chapter 12, "Back up and recover integrated Windows servers," on page 187 for more information.
2. Even though storage spaces are allocated out of IFS, storage operations are not performed by IFS while the integrated server is varied on. This means that operations like journaling are not enabled.

Virtual Ethernet line descriptions

A Virtual Ethernet line description is used to configure an iSeries virtual Ethernet network that the integrated server participates in. See Figure 13 on page 38 and Figure 14 on page 39. A line description is used to configure the integrated server to communicate with i5/OS via the server's point to point virtual Ethernet network. A line description is also used to configure the integrated server to communicate with other integrated servers or other logical partitions via an intra-partition or inter-partition virtual Ethernet network. See "Networking concepts" on page 28 for more information about virtual Ethernet networks.

Note: LINDs are not used for any physical network adapters that the integrated server might have. The physical adapters are configured from Windows using the normal Windows network adapter configuration methods.

TCP/IP interfaces

A TCP/IP interface is used to configure the TCP/IP address for the i5/OS end of the point to point virtual Ethernet network. See Figure 13 on page 38 and Figure 14 on page 39.

Note: The TCP/IP address for the Windows end of the point to point virtual Ethernet network is configured via the TCP/IP port configuration (TCPPORTCFG) parameter in the NWSD.

System bus and HSL data flows

The disk drive SCSI and virtual Ethernet data flows between i5/OS and the integrated server over the iSeries system bus (for an IXS) or a high speed link (HSL) connection between an I/O tower and the iSeries system (for an IXA). See Figure 13 on page 38 and Figure 14 on page 39. In essence, the disk drive SCSI and virtual Ethernet protocols are encapsulated or tunnelled within the normal iSeries system bus/HSL data transfer protocols.

iSCSI attached xSeries and IBM BladeCenter servers

i5/OS represents iSCSI attached xSeries and IBM BladeCenter servers similar to the way it represents IXS and IXA attached xSeries servers. However, the iSCSI technology requires additional i5/OS objects and configuration information that were not required for IXS and IXA attached xSeries servers. Since iSCSI attached servers are connected to the iSeries system with an Ethernet network (rather than the system bus/HSL attachment that is used with the IXS and IXA), additional configuration information is required to identify and communicate with the xSeries or IBM BladeCenter server on the network. In addition, since iSCSI attached servers can coexist with other systems on the Ethernet network, security of communications and data flows between i5/OS and the iSCSI attached servers can be a concern. The following diagram shows how iSCSI attached servers are represented by i5/OS.

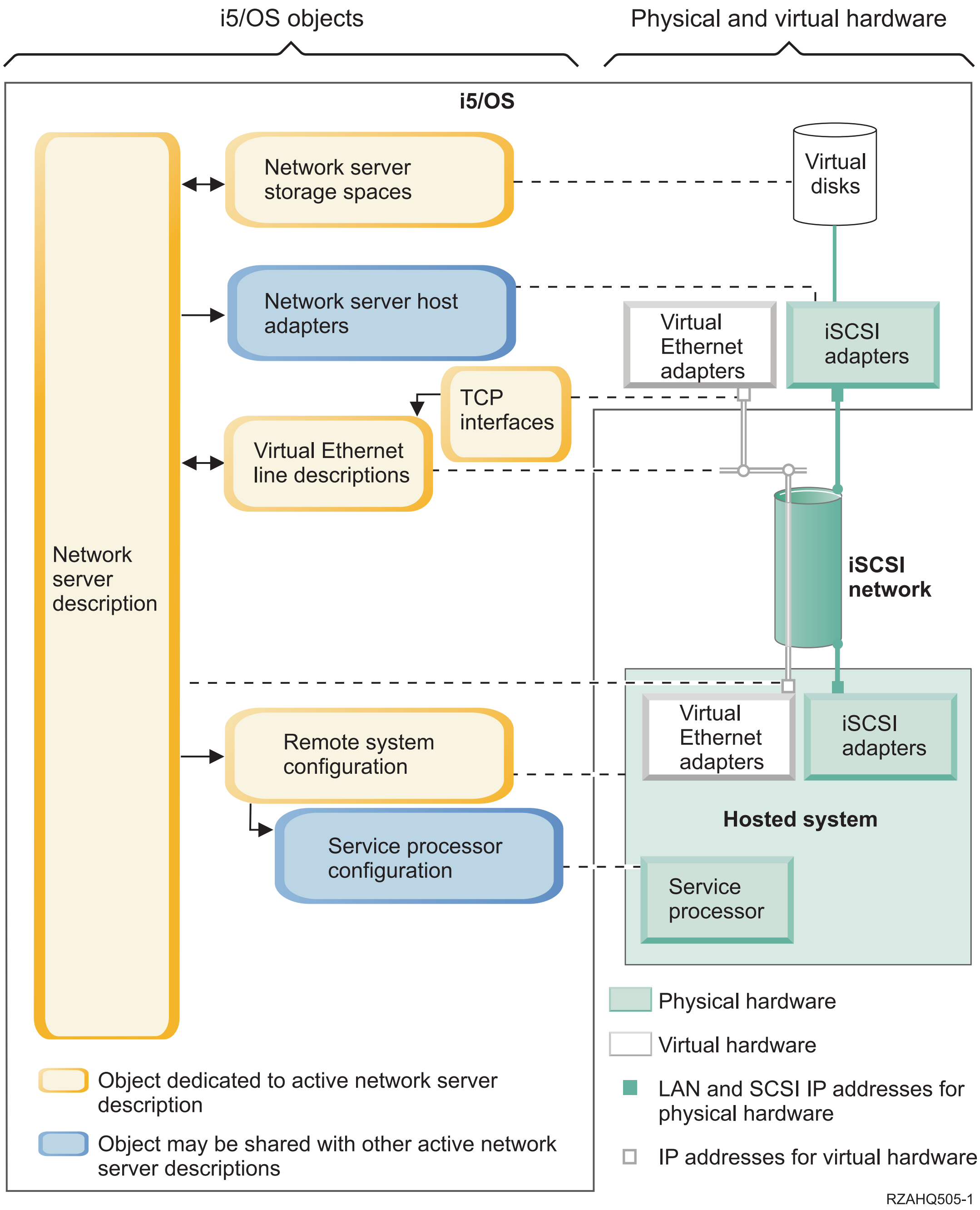

i5/OS objects
Physical and virtual hardware
i5/OS
Network server description
Network server storage spaces
Network server host adapters
TCP interfaces
Virtual Ethernet line descriptions
Remote system configuration
Service processor configuration
Virtual disks
Virtual Ethernet adapters
iSCSI adapters
iSCSI network
Virtual Ethernet adapters
iSCSI adapters
Hosted system
Service processor
Object dedicated to active network server description
Object may be shared with other active network server descriptions
Physical hardware
Virtual hardware
LAN and SCSI IP addresses for physical hardware
IP addresses for virtual hardware
RZAHQ505-1

Figure 15. iSCSI configuration objects in i5/OS without network security

Figure 15 shows key i5/OS objects as well as key hardware components that are used for iSCSI attached xSeries or IBM BladeCenter servers when network security is not used.

See the following sections that describe the objects in Figure 15 :

- “Network server host adapters” on page 43
- “Remote system configuration” on page 43
- “Service processor configuration” on page 43
- “Network server description” on page 44

- "Network server storage spaces" on page 45
- "Data flows" on page 45
- "Virtual Ethernet line descriptions" on page 41
- "TCP/IP interfaces" on page 41

For information about the i5/OS objects used for iSCSI attached xSeries and IBM BladeCenter servers with network security, see Figure 16 on page 46.

Network server host adapters

The network server host adapter (NWSH) device description object shown in Figure 15 on page 42 represents the iSCSI host bus adapter (HBA) that is used by the iSeries side of the iSCSI connection:

- It identifies the iSeries hardware resource name (for example, LIN33) 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 iSeries can have multiple iSCSI HBAs, each with 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 iSeries and the xSeries or IBM BladeCenter systems, which can provide greater bandwidth and connection redundancy.

Remote system configuration

A remote system network server configuration (NWSCFG type RMTSYS) object (shown in Figure 15 on page 42) represents the iSCSI attached xSeries or IBM BladeCenter server:

- 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 xSeries or IBM BladeCenter server.
- 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 xSeries or IBM BladeCenter server.
- The remote system configuration can optionally contain values used to secure the server boot process.

The xSeries or IBM BladeCenter server can have multiple iSCSI HBAs. This allows multiple SCSI and virtual Ethernet data paths between the iSeries and the xSeries or IBM BladeCenter systems, 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 (shown in Figure 15 on page 42) represents the xSeries service processor or the IBM BladeCenter management module:

- 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.
- The service processor object can optionally contain values used to secure the i5/OS to service processor communications.

Note: For iSCSI attached xSeries servers, there is a one-to-one relationship between the service processor object and the remote system configuration, since each service processor controls only one xSeries server. However for iSCSI attached IBM BladeCenter servers, 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 IBM BladeCenter servers that are contained within the IBM BladeCenter chassis. Therefore, with iSCSI attached IBM BladeCenter servers it would be common for several remote system configurations to share (refer to) the same service processor object.

Network server description

The network server description (NWSD) object shown in Figure 15 on page 42 is basically the same as described for Figure 14 on page 39 except for the following:

- It contains a reference to a remote system configuration object instead of an iSeries hardware resource name.
- Unlike an IXA attached server which uses one IXA card in the xSeries system to manage all of the SCSI and virtual Ethernet data flows, on an iSCSI attached server solution both the iSeries and the xSeries can have multiple iSCSI host bus adapters (HBAs). This allows multiple SCSI and virtual Ethernet data paths between the iSeries and xSeries or IBM BladeCenter systems, which can provide greater bandwidth and connection redundancy.
- 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.
- You can define a multipath group, which is a subset of the configured storage paths. You can then associate a virtual disk drive with the multipath group, instead of associating it with a specific storage path. Using the multipath group for a virtual disk drive has the advantage that if the iSCSI HBA for one of the NWSHs in the multipath group fails or the network connection to the iSCSI HBA fails, the SCSI data flow workload for that virtual disk drive is automatically routed to one of the other iSCSI HBAs that is configured in the multipath group. This provides connection redundancy and improves availability.
- 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.
- Just as with an IXS or IXA attached server, the iSCSI attached xSeries or IBM BladeCenter server hardware is controlled by i5/OS.
  - An iSCSI attached server is started and shut down the same as with an IXS or IXA attached server (see Figure 14 on page 39), by varying on or off the NWSD for that server.
  - For an iSCSI attached xSeries or IBM BladeCenter server, i5/OS communicates over an Ethernet network with the service processor (SP) for the xSeries system or the IBM BladeCenter management module for an IBM BladeCenter server to perform the start and shut down tasks.

  For server hardware power control, the main difference between the IXS/IXA configurations and the iSCSI configuration is that for IXS or IXA attached servers, the server hardware is identified by the iSeries hardware resource name, while for iSCSI attached servers, the server hardware is identified by the remote system configuration object.

  Note: Since the xSeries or IBM BladeCenter server that an iSCSI that an iSCSI attached server runs on is simply defined via the remote system configuration name in the NWSD, it is easy to switch the hardware that an iSCSI attached integrated server runs on. By changing the remote system configuration name, the xSeries or IBM BladeCenter server that the existing NWSD is booted on can be hot spared. For more information, see “Hot spare between server hardware” on page 156.

Network server storage spaces

The network server storage space (NWSSTG) objects shown in Figure 15 on page 42 are basically the same as described for Figure 14 on page 39 above, except for the following:

- 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 multipath group or let the default storage path be used.

For more information, see "Network server storage spaces" on page 40.

Data flows

In Figure 15 on page 42 the disk drive SCSI and virtual Ethernet data flows between i5/OS and the iSCSI attached integrated server over an Ethernet network. In essence, the disk drive SCSI and virtual Ethernet protocols are encapsulated or tunnelled within the normal Ethernet network protocols.

iSCSI attached xSeries and BladeCenter servers with security objects

Since iSCSI attached servers can share a network with other systems, you may want to secure the iSCSI and service processor network connections. The following diagram shows the objects that i5/OS uses to configure network security for iSCSI attached servers.

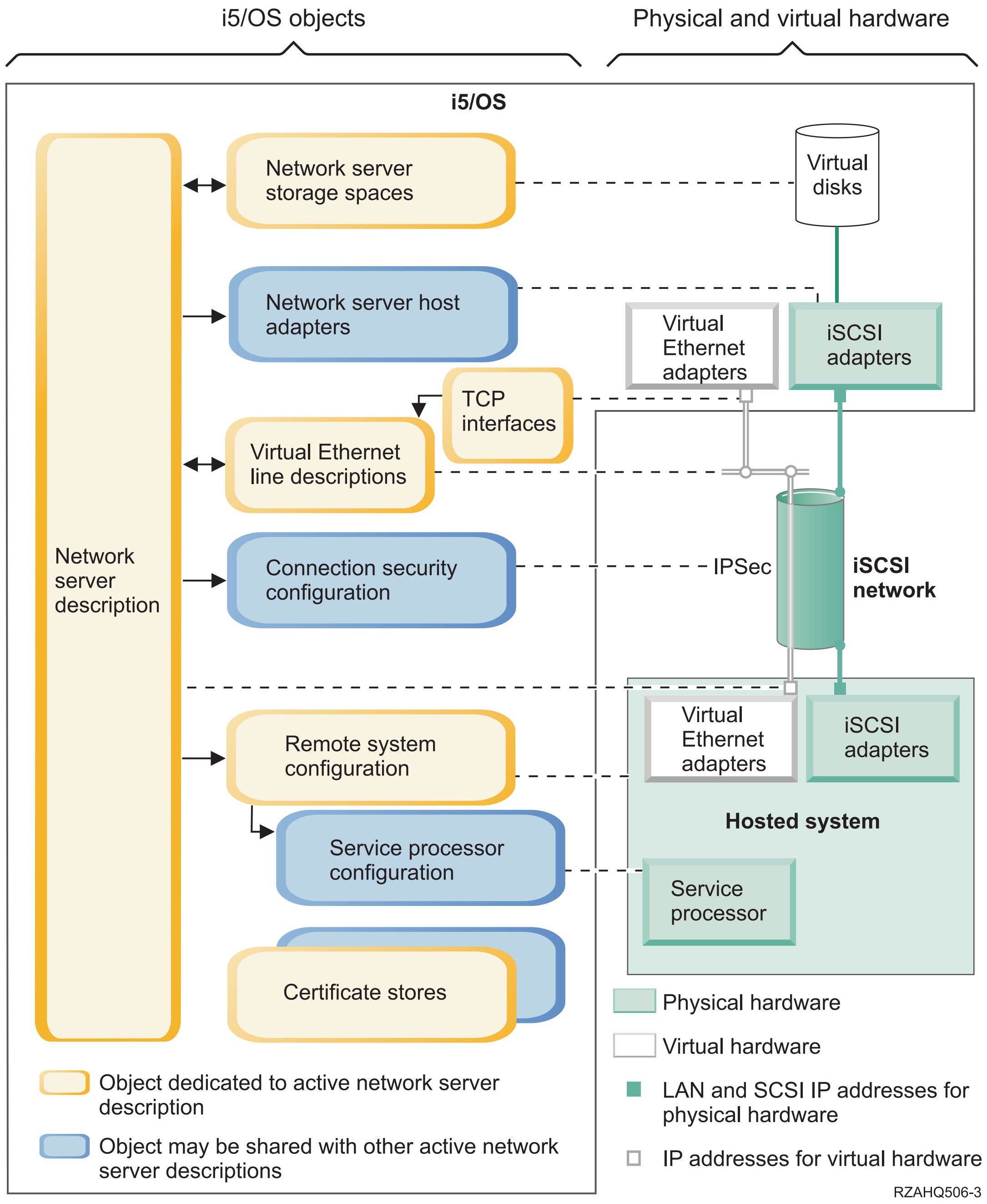

i5/OS objects
Physical and virtual hardware
i5/OS
Network server description
Network server storage spaces
Network server host adapters
TCP interfaces
Virtual Ethernet line descriptions
Connection security configuration
Remote system configuration
Service processor configuration
Certificate stores
Virtual disks
Virtual Ethernet adapters
iSCSI adapters
IPSec
iSCSI network
Virtual Ethernet adapters
iSCSI adapters
Hosted system
Service processor
Object dedicated to active network server description
Object may be shared with other active network server descriptions
Physical hardware
Virtual hardware
LAN and SCSI IP addresses for physical hardware
IP addresses for virtual hardware
RZAHQ506-3

Figure 16. iSCSI configuration objects in i5/OS with network security

Figure 16 shows key i5/OS objects as well as key hardware components that are used for iSCSI attached xSeries or IBM BladeCenter servers when network security is used.

See the following sections that describe the objects in Figure 16:

- "Remote system configuration" on page 47
- "Service processor configuration" on page 47
- "Connection security configuration" on page 47
- "Certificate stores" on page 47
- "Network server description" on page 44
- "Network server storage spaces" on page 45

- “Data flows” on page 45
- “Virtual Ethernet line descriptions” on page 41
- “TCP/IP interfaces” on page 41

Remote system configuration

The remote system network server configuration (NWSCFG type RMTSYS) object shown in Figure 16 on page 46 is the same as described in “Remote system configuration” on page 43 for Figure 15 on page 42, except that it contains challenge handshake authentication protocol (CHAP) configuration values that are used to authenticate the remote system when it initially accesses storage.

Service processor configuration

The service processor network server configuration (NWSCFG type SRVPRC) object shown in Figure 16 on page 46 is the same as described in “Service processor configuration” on page 43 for Figure 15 on page 42, except for the following:

- It contains a service processor user name and password that are used to sign on to the service processor.
- It contains information required to manage an optional SSL certificate that is used to secure the i5/OS to service processor communications.

Connection security configuration

The connection security network server configuration (NWSCFG type CNNSEC) object shown in Figure 16 on page 46 is used to secure the SCSI and virtual Ethernet data flows between i5/OS and the iSCSI attached xSeries or IBM BladeCenter server:

- It identifies a set of IP security (IPSec) rules that are used with the various storage and virtual Ethernet connections.
- You can decide which data flows are secured and which data flows are not secured. You can choose to secure none, some, or all of the storage or virtual Ethernet connections. For example, you can choose to secure just the storage (SCSI) data flows or just one of the virtual Ethernet connections.
- You identify which SCSI and virtual Ethernet data flows are secured by specifying the appropriate security rules on the storage paths and virtual Ethernet paths parameters of the NWSD.
- When using IPSec, the SCSI and virtual Ethernet data flows between i5/OS and the iSCSI attached integrated server are encrypted and have an additional layer of encapsulation (tunneling) within the normal Ethernet network protocols.

Certificate stores

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

- **The i5/OS system certificate store.** If you manually import certificates to the hosted system’s service processor from an external source, this certificate store is where the corresponding trusted root CA certificates are stored. The system certificate store is shared by many i5/OS applications.
- **A certificate store that is associated with the service processor configuration.** This certificate store is created automatically for you if you configure SSL for the service processor connection using the **Automatically set up user and generate certificate** option. For more information, see “Automatic SSL initialization” on page 130. The certificates in this certificate store are used only when communicating with hosted systems that use the corresponding service processor configuration. This certificate store is shared if multiple hosted systems (for example, IBM BladeCenter blades) are using the same service processor configuration. Certificates are placed in this certificate store if you:
  - Use the service processor configuration option to generate a certificate.
  - Synchronize a certificate from the hosted system’s service processor to the corresponding service processor configuration.
- **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.

High availability concepts

iSeries and xSeries integration and storage virtualization provide innovative options that can enable you to enhance the reliability and recoverability of your Windows server environment. Hosted systems can provide increased availability with one or more of the following technologies.

Hot spare hardware

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. With hosted systems, there are two ways to use hot spare hardware to minimize downtime that is caused by hardware failures:

1. Hosted system hardware, including Integrated xSeries Servers, xSeries servers that are attached via an Integrated xSeries Adapter, and xSeries or IBM BladeCenter servers that are attached via an iSCSI host bus adapter, can be hot spared. If the hardware that is used to run the hosted system fails, you can quickly switch the hosted system's disk images to compatible spare hardware and restart the hosted system. For more information, see "Hot spare between server hardware" on page 156.
2. For iSCSI attached servers, the iSeries target iSCSI host bus adapters (iSCSI HBA) can be hot spared. If an iSCSI HBA that a hosted system is using fails, you can quickly switch the hosted system to use a spare iSCSI HBA and restart the hosted system. For more information, see "Hot spare between iSCSI local host adapters" on page 132.

iSCSI multipath

A hosted system can use redundant iSCSI data paths to access virtual disks hosted by i5/OS. This is accomplished by defining a multipath group of two or more iSCSI HBAs and then specifying that a given virtual disk should be accessed using a group, rather than a single iSCSI HBA. With this configuration, the data on the virtual disk can be accessed using any of the iSCSI HBAs in the group. For more information, see "Advanced iSCSI support" on page 20.

Microsoft Windows Cluster Service (MSCS)

Hosted servers can use MSCS to provide real-time application failover in the case of hosted system hardware or software failures. User-initiated failovers can be used to take a server offline so that maintenance or backups can be performed while the application continues to run on the other server(s) in the cluster. For more information, see "Windows Cluster Service" on page 98.

Security concepts

For procedures to implement the security concepts described in this section, see "Configure security between i5/OS and hosted systems" on page 128. There are several types of security to consider.

- "Security for IXSs and IXA attached systems"
- "Security for iSCSI attached systems" on page 49

Security for IXSs and IXA attached systems

Storage data and virtual Ethernet communications for IXSs and IXA attached systems flow over physically secure iSeries system buses and HSL cables.

Security for iSCSI attached systems

iSCSI technology leverages the low cost and familiarity of Ethernet and IP networking. The flexibility of Ethernet and IP networking allows iSCSI attached systems to share hardware, extend the range, and increase bandwidth by adding hardware. However, this familiarity and flexibility leads to a requirement for appropriate network security.

Each of the different types of networks used by iSCSI attached systems has its own security considerations.

Service processor connection security
Service processor security can involve one or more of the following mechanisms.

- Service processor password
- Secure Sockets Layer (SSL)
- Network isolation and physical security

iSCSI network security
There are two types of iSCSI network traffic to consider.

- Storage security can involve one or more of the following mechanisms.
  - Network isolation, physical security, and security gateways
  - Challenge Handshake Authentication Protocol (CHAP)
  - IP Security (IPSec)
  - Firewalls
- Virtual Ethernet security can involve one or more of the following mechanisms.
  - Network isolation, physical security, and security gateways
  - IP Security (IPSec)
  - Firewalls
  - In addition, when user enrollment or remote command submission send sensitive data over the point to point virtual Ethernet, these applications use a Secure Sockets Layer (SSL) connection between i5/OS and Windows. For more information about user enrollment, see “User and group concepts” on page 51.

Network isolation and physical security
Network isolation minimizes the risk of data being accessed by unauthorized devices and data being modified as 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/network. When configuring a VLAN switch, treat an iSCSI HBA that is installed in your iSeries server as a VLAN-unaware device.

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

Service processor password
This password is managed by i5/OS and is used when your iSeries server starts a conversation with the hosted system’s service processor. 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.

Service processor Secure Sockets Layer (SSL)
You can enable this type of SSL only if you have the appropriate type of service processor hardware. If enabled, SSL encrypts traffic on the service processor connection and ensures that the service processor is

authentic. Authentication is based on a digital certificate from the service processor that is installed in i5/OS either manually or automatically. This certificate is distinct from the digital certificates used for the SSL connection between i5/OS and Windows.

Secure Sockets Layer (SSL) connection between i5/OS and Windows
The Windows environment on iSeries 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. These certificates are distinct from the digital certificates used for service processor SSL. 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.

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

IP Security (IPSec)
IPSec encrypts storage and virtual Ethernet traffic on the iSCSI network. A related protocol, Internet Key Exchange (IKE), ensures that the communicating IP endpoints are authentic.

Two conditions are required to enable IPSec:

1. Both the iSeries and hosted system must have special iSCSI HBAs with high-speed IPSec support.
2. You must configure a pre-shared key. i5/OS can generate appropriate pre-shared keys. If multiple iSCSI HBAs are involved in the iSeries or hosted system, you can assign different pre-shared keys to different IP address pairs. All other details of IPSec and IKE are handled automatically. IPSec support in i5/OS TCP/IP and Windows TCP/IP are not involved.

IPSec HBAs provide a filter function that blocks communication with IP addresses that are not configured. IPSec HBAs perform this filtering even if IPSec encryption is not enabled by supplying a pre-shared key.

When used for virtual Ethernet, IPSec is not applied directly to the virtual Ethernet endpoints, but rather to the iSCSI HBAs that form the tunnel through the iSCSI network. Consequently, when multiple iSCSI attached Windows servers communicate with each other over virtual Ethernet, each server's IPSec configuration is independent of the others. For example, it is possible for a server to enable IPSec and communicate with other Windows servers that are using physical security instead of IPSec. Servers do not have to use the same IPSec pre-shared key to communicate with each other.

Firewalls
A firewall can be used between a shared network and the iSeries server to protect the iSeries from unwanted network traffic. Similarly, a firewall can be used between a shared network and a hosted system to protect the hosted 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 actually 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 "Configure a firewall" on page 131 for information about optionally controlling UDP port selection.
  - MAC and IP headers for the virtual Ethernet adapter.

IPSec HBAs provide a firewall-like function that blocks communication with IP addresses that are not configured, even if IPSec is not enabled by supplying a pre-shared key.

User and group concepts

One of the main advantages of using Windows environment on iSeries 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. This section will explain the function in more detail.

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

- **AS400_Permanent_Users** Users in this group cannot be removed from the Windows environment by the iSeries server. 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 environment. Membership in this group is controlled from the Windows environment, 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 "Types of user configurations" on page 53.

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 "Enterprise Identity Mapping (EIM)" on page 180.

Enrolling existing Windows user profiles

You can also enroll a user who already exists in the Windows environment. The password for the user must be the same on i5/OS as for the already existing Windows user or group. See "Password considerations" on page 55.

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" on page 54. 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 on a local integrated Windows server or 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 environment 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 environment, you automatically create and enroll those users in the Windows environment as well.

Enrolling to multiple domains

You may enroll users and groups to multiple domains, but typically this is unnecessary. In most Windows environments, 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 occuring on each member server. Use the Propagate Domain User (PRPDMNUSR) parameter in the Change Network Server Despcription (CHGNWD) or Create Network Server Description (CRTNWSD) commands. See “The QAS400NT user” on page 183 for more information.

Types of user configurations

It is helpful to think of integrated Windows users as fitting into three basic types:

- **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 180.
- **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 “Enterprise Identity Mapping (EIM)” on page 180.

- **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 1. 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 iSeries Navigator provides with their 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 iSeries Navigator to manually define EIM i5/OS target associations and Windows source associations.

User enrollment templates

A user enrollment template is a tool to help you enroll users from i5/OS to the Windows environment more efficiently. 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 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.

For a detailed procedure see "Create user templates" on page 178.

Password considerations

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 iSeries Security Reference .
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 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.

Chapter 5. Install and configure Windows environment on iSeries

Setting up Windows environment on iSeries involves installing hardware and two separate pieces of software: IBM i5/OS Integrated Server Support and the Windows 2000 Server or Windows Server 2003 operating system from Microsoft.

To install and configure Windows environment on iSeries, do the following steps:

1. Check the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/). Ensure that you are aware of late breaking news and information.
2. Check for late breaking news and information for the hardware you are installing.
   - IXA install read me first (www.ibm.com/systems/i/bladecenter/ixa/readme/)
   - iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/)
   - IXS install read me first (www.ibm.com/systems/i/bladecenter/ixs/readme/)
3. Check to make sure you have the correct hardware and software.
   a. “Hardware requirements.”
   b. “Software requirements” on page 59.
4. For IXS or IXA attached servers, install hardware, if needed. See Install iSeries Features. Choose your model of iSeries server. Select **PCI Adapter** for an IXS, **Integrated xSeries Adapter** for an IXA. If you are installing an iSCSI HBA you will be directed to install your hardware in step 6b.
5. Install the IBM iSeries Integrated Server Support.
   a. “Prepare for the installation of integrated Windows servers” on page 60
   b. “Install IBM i5/OS Integrated Server Support” on page 64
6. Install Microsoft Windows 2000 Server or Windows Server 2003 to the integrated server.
   a. “Plan for the installation of Windows server” on page 65
   b. “Install Windows 2000 Server or Windows Server 2003” on page 89
7. Now that you have completed the installation, configure the integrated Windows Server.
   a. “Code fixes” on page 106. These code fixes will correct any errors discovered in the licensed program since its release.
   b. Chapter 6, “Manage virtual Ethernet and external networks,” on page 111
   c. “Set an integrated Windows server to automatically vary on with TCP/IP” on page 106

Hardware requirements

To run integrated Windows servers, you need the following hardware:

1. One of the following Integrated xSeries Servers (IXSs) or Integrated xSeries Adapters (IXAs).

Description	Feature code	Type-model
iSCSI host bus adapter (copper)	5783[4]	573B-002
iSCSI host bus adapter (fiber)	5784[4]	573C-002

Description	Feature code	Type-model
2.0 GHz Integrated xSeries Server	4811 4812 4813	4812-001
2.0 GHz Integrated xSeries Server	4710	2892-002
2.0 GHz Integrated xSeries Server	4810	2892-002
1.6 GHz Integrated xSeries Server	2792	2892-001
1.6 GHz Integrated xSeries Server	2892	2892-001
1.0 GHz Integrated xSeries Server	2799	2890-003
1.0 GHz Integrated xSeries Server	2899	2890-003
850 MHz Integrated xSeries Server	2791	2890-002
850 MHz Integrated xSeries Server	2891	2890-002
700 MHz Integrated xSeries Server	2790	2890-001
700 MHz Integrated xSeries Server	2890	2890-001
Integrated xSeries Adapter model 100	0092 [1,2]	2689-001
Integrated xSeries Adapter model 200	0092 [1,3]	2689-002

Notes:

1. The IXA requires an xSeries server. The xSeries server may have additional requirements, see the System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/) web site for details.

2. The hardware is ordered through AAS or WTAAS as machine type 1519-100.

3. The hardware is ordered through AAS or WTAAS as machine type 1519-200.

4. The iSCSI HBA requires an xSeries or BladeCenter server. The xSeries or BladeCenter server may have additional requirements. See the System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/) web site for details.

Note: If you have integrated server hardware that is not listed in the above table, see the System i integration with BladeCenter and System x web site for specifications.

For information about how to install hardware, see the “Install iSeries features” topic. For a description of IXSs, IXAs, and iSCSI HBAs, see “Hardware concepts” on page 13.

2. An iSeries server with sufficient free disk space, including 100 MB for the code of the IBM i5/OS Integrated Server Support, and 2047 MB to be used for the Windows system drive or network server storage space.
3. For IXSs, one or more approved LAN ports or PCI adapters:

Description	Feature Code	Supported by IXS hardware type 4812	Supported by IXS hardware type 2892	Supported by IXS hardware type 2890
iSeries 1000/100/10 Mbps Ethernet Adapter (copper UTP)	5701		X	
iSeries Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	5700		X	

Description	Feature Code	Supported by IXS hardware type 4812	Supported by IXS hardware type 2892	Supported by IXS hardware type 2890
iSeries Gigabit (1000/100/10 Mbps) Ethernet Adapter (copper UTP)	2760			X
iSeries Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	2743			X
iSeries 2892 10/100 Mbps Ethernet port	2892		X	
IBM iSeries 10/100 Mbps Ethernet Adapter	2838			X
High-speed 100/16/4 Mbps Token-ring PCI Adapter	2744		X	X
iSeries 4812 1000/100/10 Mbps Ethernet port	4812	X		

4. An SVGA compatible monitor, a mouse, and a keyboard. There is only a single keyboard/mouse port in an IXS, so you will also need a keyboard/mouse Y-cable to be able to attach both at the same time. If you have several integrated servers and plan to administer only one at a time, consider switching one set of I/O hardware between integrated servers.
5. At least 128 MB of random access memory (RAM), or at least 256 MB of RAM if you are using Windows Server 2003. This memory is installed in the integrated server and must be ordered separately.
6. A PC with Microsoft Windows and iSeries Access (which includes iSeries navigator) installed.

   Note: iSeries navigator is preferred for most Windows environment on iSeries configuration tasks.

For additional hardware requirements, see

- "Memory requirements" on page 61
- "Networking concepts" on page 28

Software requirements

You need this software:

1. i5/OS 5722-SS1 Version 5 Release 4.

   To check your release level:

   a. On the i5/OS command line, type `Go LICPGM` and press Enter.

   b. Type `10` in the option field to look at installed products.

   c. Look for 5722SS1. The release shown beside that is your version. (On some releases, you may need to press F11 before the version number appears.)
2. IBM i5/OS Integrated Server Support (5722-SS1 Option 29) V5R4. See "Install IBM i5/OS Integrated Server Support" on page 64.
3. IBM iSeries Navigator, which is included with IBM iSeries Access for Windows (5722-XE1).

   Notes:

   a. When installing iSeries Navigator on a Windows PC, do a full install or do a custom install and select the optional Integrated Server Administration component.

   b. iSeries navigator is preferred for most Windows environment on iSeries configuration tasks.
4. TCP/IP Connectivity Utilities for i5/OS V5R4 (5722-TC1).
5. For IXS and IXA attached servers, you need Microsoft Windows 2000 Server or Windows Server 2003. For iSCSI attached servers you need Windows Server 2003 media that includes Service Pack 1. For more information about integrating Service Pack 1 with your Windows Server 2003 installation media, see Integrating a service pack with Windows Server 2003 on the Integration with BladeCenter and System x Web site.
6. Any required Microsoft Windows service packs. For the latest information about available service packs that IBM has tested with i5/OS Integrated Server Support, refer to the Applications topic on the System i integration with BladeCenter and System x Web site.

For iSCSI servers, you also need this software:

1. IBM Director Server 5.20 or greater must be installed on the i5/OS partition that will host your integrated server.

   Notes:

   a. IBM Director might have additional software requirements.
   b. The component of IBM Director Server that is required for integrated servers might be referred to as a management server in the IBM Systems Software Information Center. No other components of Director are required.
   c. You do not need to install any components of IBM Director on the integrated Windows server.
   d. IBM Director 5.10.3 is supported for existing integrated servers if the most recent PTFs are installed.

   For information about installing IBM Director Server, see Installing IBM Director Server on i5/OS in the IBM Systems Software Information Center.
2. IBM i5/OS Digital Certificate Manager (5722-SS1 option 34) V5R4
3. IBM HTTP Server for iSeries (5722-DG1)

For additional information about the installation of required software, see the iSeries Software Installation manual .

Prepare for the installation of integrated Windows servers

The installation will go smoothly if you perform some preliminary tasks.

1. Verify that you have the necessary authority to perform the installation. You must have *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority on i5/OS. *SECADM special authority is required to perform step 8 of this checklist. For information about special authorities, refer to the iSeries Security Reference .
2. Verify "Memory requirements" on page 61.
3. "Configure i5/OS TCP/IP for integrated Windows servers" on page 62.
4. Decide how many integrated Windows servers and subnets you need for your particular business.

   If you are installing an iSCSI attached server, each iSCSI HBA for iSeries requires two fixed IP addresses and each hosted xSeries system or IBM BladeCenter requires at least two IP addresses for iSCSI. For more information about IP address requirements, see "Networking concepts" on page 28.

   If your organization uses fixed IP addresses (organizations that use DHCP may configure the integrated Windows server to be assigned an IP address automatically just like any standard PC server), obtain TCP/IP addresses from your network administrator. These include:

   - IP addresses for all external TCP/IP ports
   - Subnet mask

- Your domain name or workgroup name
- IP address for your Domain Name System (DNS) server, if you have one
- IP address of the default gateway for your local area network (LAN), if you have one

If you are running TCP/IP on your iSeries system, the last two items in the above list have already been supplied to the system. Specify *SYS for those parameters while performing the Install Windows server (INSWNTSVR) command.

5. Enable NetServer™ and set up a user profile, so you can perform maintenance tasks on your integrated server. Refer to “Enable iSeries NetServer” on page 63 and “Plan for a Windows user with authorities to access iSeries NetServer” on page 63.
6. It is possible to eliminate the need for a physical CD-ROM during installation. For example, to avoid the delay and expense of shipping the CD-ROM to a remote site if you need to reinstall a server, or to slipstream a Microsoft service pack or hotfix into your install source to avoid virus infections (MS Knowledge base article 828930).
   a. If you want to store the installation image on a CD, Integrating a service pack with Windows Server 2003 on the System i Integration with BladeCenter and System x Web site.
   b. If you want to use IFS to access to installation image, see Creating a Windows Server install CD image in IFS on the System i Integration with BladeCenter and System x Web site.

   Note: Contents of the installation CD may be subject to licenses from their respective authors and distributors. Compliance with these licenses is your responsibility. By offering this function, IBM takes no responsibility for compliance with or enforcement of any CD license agreement.
7. You can customize the installation by using a configuration file to change the default values in the Windows unattended install setup script file (unattend.txt). See Chapter 15, “Network server description configuration files,” on page 243.
8. If the server will be installed on an external xSeries or IBM BladeCenter server using an iSCSI HBA, make sure that the i5/OS QRETSVRSEC system is set to 1. You can do this with the Work with System Values (WRKSYSVAL) command.
9. If you use logical partitions on your iSeries server, recall that you need to install IBM i5/OS Integrated xSeries Server Support only on the logical partition that you will use to vary on the server. There is no requirement to install the licensed program on all the logical partitions. For example, one logical partition might have the i5/OS Integrated xSeries Server Support and one or more integrated Windows servers installed while another logical partition has neither i5/OS Integrated xSeries Server Support nor any integrated servers installed.
10. If the server will be installed on an external xSeries server using an Integrated xSeries Adapter, refer to the following links:
    - IXA install read me first
    - Install iSeries Features
11. If the server will be installed on an Integrated xSeries Server, see IXS install read me first .
12. If the server will be installed on an external xSeries or IBM BladeCenter server using an iSCSI HBA, make sure that you are following the installation process on the iSCSI install read me first web page.

Memory requirements

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 Performance Capabilities Reference Guide for the minimum memory requirements for IXS, IXA and iSCSI attached xSeries servers.

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

Time synchronization

To keep the time on i5/OS and the Windows environment synchronized, do the following steps:

1. Select *YES for synchronize date and time in the Install Windows server (INSWNTSVR) command or the CHGNWSD command. Selecting *YES will synchronize the time between i5/OS and the integrated Windows server every 30 minutes. Selecting *NO will synchronize the time only when the server is started.
2. Ensure that the iSeries 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. For more information, see "Complete the server installation" on page 95.

If you have problems with time synchronization, check the i5/OS system value for LOCALE to make sure it is set properly.

Note: Time synchronization should be set to *NO for Windows active domain servers and domain member servers. Since Windows Active Directory has its own time synchronization facility, setting time synchronization to *YES will cause a conflict.

Configure i5/OS TCP/IP for integrated Windows servers

When you install the Windows operating system on your integrated server, you have the option of using values that you specified in the i5/OS TCP/IP configuration as default values to configure your integrated server. 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 iSeries Navigator installed, you can use it to configure your TCP/IP connections. The iSeries Navigator online help tells you how to configure TCP/IP. If you do not have iSeries 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.

iSeries Access for Windows on integrated Windows servers

IBM iSeries Access for Windows allows you to connect a personal computer (PC) to an iSeries server over a local area network (LAN), a twinaxial connection, or a remote link. 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 iSeries 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 iSeries Access for Windows on your integrated server. This enables you to write server applications that call the ODBC device driver to access DB2 for iSeries.

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

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

Additional information sources:

- You can read a comparison of iSeries Access for Windows with iSeries NetServer.

Enable iSeries NetServer

iSeries 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 iSeries user profile with the same password, or you must have a guest NetServer user profile configured.

If you plan to use iSeries NetServer only to perform maintenance tasks, you can set it up without iSeries Navigator. In that case, you can use the quickstart method found in the “Configure iSeries server for NetServer”topic. If you want the full capabilities of iSeries NetServer, you need iSeries Navigator, which requires setting up iSeries Access (see “iSeries Access for Windows on integrated Windows servers”) on a PC that you use for administration.

Once you have set up iSeries NetServer, you need to set up a Windows user with access to iSeries NetServer or you can set up an iSeries NetServer guest user profile. See “Plan for a Windows user with authorities to access iSeries NetServer.”

Plan for a Windows user with authorities to access iSeries 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 iSeries NetServer.

Before you can apply code fixes and system upgrades to the Integrated Server Support code 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 iSeries NetServer. You can use one of the following methods to use this account.

- Sign onto Windows with an account that has a corresponding iSeries 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 “Enroll a single i5/OS user to the Windows environment using iSeries Navigator” on page 177.
- If you prefer not to create a user profile, you can also use a guest user profile that is configured for iSeries NetServer. See “Create a guest user profile for iSeries NetServer”

Once you have set up your iSeries NetServer user profile, return to “Enable iSeries NetServer” on page 63 or “Prepare for the installation of integrated Windows servers” on page 60.

Create a guest user profile for iSeries NetServer

You must have *SECADM special authority to perform this task.

If you have iSeries Navigator on your system, you can use the graphical interface to set up a guest user profile for iSeries NetServer with no special authorities and no password.

If you do not have iSeries Navigator, follow these steps to set up a guest user profile for iSeries 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 iSeries Security Reference 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 iSeries NetServer, enter the following command:
   ```
   ENDTCPSVR SERVER(*NETSVR)
   ```
4. To restart iSeries NetServer, enter the following command:
   ```
   STRTCPSVR SERVER(*NETSVR)
   ```

Install IBM i5/OS Integrated Server Support

To install IBM i5/OS Integrated Server Support, perform these steps on iSeries:

1. If you are upgrading IBM iSeries Integration for Windows Server from V5R2 or V5R3, refer to this topic, “Upgrade the IBM iSeries Integration for Windows Server licensed program” on page 96. Perform the steps under ″Preparing to Upgrade″ and then return here.
2. Insert the i5/OS CD containing 5722-SS1 option 29.
3. Type `GO LICPGM` and press Enter.
4. Choose option `11` from the `Work with Licensed Programs` menu; then press Enter.
5. Page down the list of licensed programs until you see the description `Integrated Server Support`.
6. Enter a `1` in the `Option` field beside the description.
7. Press enter.
8. Enter the name of the `Installation device` in which you inserted the i5/OS CD.
9. Press Enter, and the system installs the integration software.
10. After installing IBM i5/OS Integrated Server Support, install the latest cumulative program temporary fix (PTF) package from IBM. Note that there should be no users on your iSeries when installing 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.

11. 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 Fixes in the **Get Started with iSeries** topic.
12. If you are upgrading IBM iSeries Integration for Windows Server from V5R2 or V5R3, go to "Upgrade the IBM iSeries Integration for Windows Server licensed program" on page 96. Perform the steps under "After upgrading i5/OS" and return here.
13. If you are upgrading i5/OS Integrated Server Support from a prior release, you need to upgrade existing integrated Windows servers to the new level. See "Upgrade the integrated server side of IBM i5/OS Integrated Server Support" on page 97.

Plan for the installation of Windows server

It is recommended that you make the first integrated Windows server on your network a domain controller and name it carefully. (To change its name, you must first change its role.) Domain controllers contain the master security database. Any domain controller can make changes which are then replicated to all other domain controllers.

If you are installing an iSCSI attached server you should also see "Plan for iSCSI hardware installation."

Before you install Windows 2000 Server or Windows Server 2003, you need to complete and save the command generated by the "Windows server installation advisor". Alternatively, you may fill out the "Installation worksheet for i5/OS parameters" on page 68.

See "Install Windows 2000 Server or Windows Server 2003" on page 89 to continue.

Plan for iSCSI hardware installation

You should configure your iSCSI hardware before beginning the Windows server installation.

- "Plan the boot mode for your hosted system"
- "Create a service processor configuration and a remote system configuration" on page 66
- "Plan your service processor connection" on page 67
- "Configure the service processor discovery method on your iSeries server" on page 67

Plan the boot mode for your hosted system

The boot mode determines how IP and storage information required to boot Windows is delivered to an iSCSI HBA in the hosted system.

Dynamically delivered to the remote system via DHCP
This is the default mode. A DHCP server on the iSeries server automatically provides configuration information via the configured NWSH adapters. See "Diskless booting over iSCSI" on page 22.

- Multiple NWSDs can use the hosted system at different times.
- This mode can be used on switched networks and on routed networks connected by a DHCP relay.
- When IPSec is enabled, DHCP traffic is allowed to pass between the iSCSI HBAs

Manually configured on the remote system

- Only one NWSD can use the hosted system.
- This setting works on networks without DHCP relay.
- When IPSec is enabled between the iSCSI HBAs, DHCP traffic is blocked on the iSCSI network.

Create a service processor configuration and a remote system configuration

Before installing the server, you can optionally create a service processor configuration and a remote system configuration so that their names can be provided as parameters to the Install Windows Server (INSWNTSVR) command. This procedure can be performed before the hosted system hardware is set up, and is optional because INSWNTSVR can generate these objects when given all of the same information as parameters. It is recommended that you create the service processor configuration and the remote system configuration before you run the INSWNTSVR command whenever any of the following conditions are true:

- You have never installed an iSCSI attached server before and you want as much guidance as possible.
- You prefer using a graphical interface whenever possible.
- The remote system serial number or iSCSI HBA labels will be less accessible later.

To create a service processor configuration and remote system configuration, do the following steps.

1. If you have not already created a service processor configuration to use with the new server, create one now. You will be able to change this object later.
   a. Expand **Integrated Server Administration**.
   b. Expand **iSCSI Connections**.
   c. Right-click **Service Processors**.
   d. Select **New Service Processor Configuration**.
   e. On the **General** tab:
      - Enter the **Name** and **Description**.
      - Specify the enclosure **Serial number** to identify the service processor on the network. Look at the system enclosure to determine this value.
      - Select the **Object authority**. You can use the default value **Change**.

   f. On the **Security** tab, specify **Do not use a certificate (requires physical security)**.
   g. Click **OK**.
2. If you have not already created a remote system configuration, create one now.
   a. Expand **Integrated Server Administration**.
   b. Expand **iSCSI Connections**.
   c. Right-click **Remote Systems**.
   d. Select **New Remote System Configuration**.
   e. On the **General** tab:
      - Enter the **Name** and **Description**.
      - For **Service processor configuration**, select the existing or new service processor configuration from step 1.
      - Specify the **Remote system identity**.

        Note: To specify Remote system identity for a IBM BladeCenter blade, select the **Use the following values option** and specify the IBM BladeCenter blade serial number. For other servers, leave the **Use enclosure identity** option selected.
      - Select the **Object authority**. You can use the default value **Change**.

   f. On the **Network Interfaces** tab, do the following steps for each iSCSI HBA port that you will use in the hosted system.
      1) Click **Add...**

2) In the **Network Interface Properties** panel, specify at least one **adapter (MAC) address** from a label on the iSCSI HBA. To determine whether to specify an address for the **Remote SCSI interface** and the **Remote LAN Interface**, see “iSCSI network” on page 29. If you are not sure, specify an address for both. Each address consists of 12 hexadecimal characters.

   - For the **Remote SCSI interface**, look for the word ‘iSCSI’ on the label and specify the corresponding address.
   - For the **Remote LAN interface**, look for the word ‘TOE’ on the label and specify the corresponding address.

   Note: For iSCSI HBAs with two ports, the label shows four addresses. Each port has an iSCSI address and a TOE address.

3) For each adapter (MAC) address that you specify, also enter an **Internet address** and **Subnet mask** that is appropriate for your iSCSI network. Leave the **Gateway** field blank if your iSCSI network has no gateway.

4) Click **OK** on the **Network Interface Properties** .

g. On the **Boot parameters** tab:

   - Configure a boot mode. See “Plan the boot mode for your hosted system” on page 65. In most cases, this will be the default option **Dynamically delivered to remote system via DHCP**. For more information, see “Diskless booting over iSCSI” on page 22. Ignore the **More than one iSCSI interface in remote system** checkbox.

h. On the **CHAP authentication** tab:

   - Select the CHAP option you will use. For more information, see “Security for iSCSI attached systems” on page 49.

i. If you want to configure additional information for this object, configure it now.

j. Click **OK**.

Plan your service processor connection

If you created a new service processor configuration to use with the new server, you must determine what methods are supported by your service processor for each of the following, and which supported methods you want to use.

- Configuration method
- Static or dynamic IP addressing
- Discovery method
- Security method

You will need this information in the next steps when you prepare the hardware and change the service processor configuration. To decide which methods you will use, see “Service processor connection” on page 29 and “Service processor discovery configuration” on page 143, but don’t perform the configuration steps yet.

Configure the service processor discovery method on your iSeries server

Configure a service processor discovery method. At this time, skip any steps that must be done at the hosted system because these steps will be performed later as part of the hardware preparation. For more information, see “Service processor discovery methods” on page 144.

Network server descriptions

Network server descriptions (NWSDs) represent an integrated Windows server on iSeries. The Install Windows server (INSWNTSVR) command automatically creates an NWSD for each integrated server that you install. The NWSD typically has the same name as the server. When you perform an action on the NWSD, you also take action on the server. For example, varying the NWSD on starts the server, and varying the NWSD off shuts down the server.

Installation worksheet for i5/OS parameters

Prior to installing Windows 2000 Server or Windows Server 2003, complete either the Windows server installation advisor or this installation worksheet.

This worksheet will help you to install and configure your system.

Note: Parameters that are marked **Full** are used for a full install. Fields that are marked as **Basic** apply to a basic install.

Field	Description and Instructions	Value
Network server description (NWSD) Full, Basic	Defines the operating characteristics and communications connections of the network server that controls the integrated Windows server. See "Network server descriptions" on page 67. 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. The network server description name is also the computer name and TCP/IP host name of the integrated server.	
Install type (INSTYPE) Full, Basic	Specifies the type of install to perform. Choose one of the following: ***FULL** Required when installing on an internal Integrated xSeries(R) Server (IXS) and is optional when installing on an external xSeries server attached with an Integrated xSeries Adapter (IXA) or iSCSI HBA . ***BASIC** Optional install type when installing on an externally attached xSeries server attached with an IXA or iSCSI HBA. With this option, the first part of the install process is controlled by the i5/OS Install Windows server INSWNTSVR command. Then the install is completed by the xSeries install process using the ServerGuide™ CD.	
Resource name (RSRCNAME) Full, Basic	Identifies the Windows server hardware. For iSCSI attached xSeries and IBM BladeCenter servers, specify a resource name of *ISCSI. For both IXS and IXA attached xSeries servers, enter the File Server IOA resource name. To determine the name, enter `DSPHDWRSC *CMN` (Display Communication Hardware Resources) at the i5/OS command line. The resource name will appear as LINxx where xx is a number. "Tip: Find resource names when you have multiple integrated servers" on page 88	

Field	Description and Instructions	Value
TCP/IP port configuration (TCPPORTCFG) Full	Specify the Windows TCP/IP configuration values that are specific to each locally controlled adapter port. Otherwise, skip this step and use the default value *NONE. **Note:** Only adapters that are directly managed by the iSeries and logically controlled by the IXS can be configured using the TCPPORTCFG parameter. LAN adapters that are attached with an IXA or iSCSI HBA and are managed by the xSeries server cannot be configured with this parameter.	• Port 1 – IP address – Subnet mask – Gateway (optional) • Port 2 – IP address – Subnet mask – Gateway (optional) • Port 3 – IP address – Subnet mask – Gateway (optional) • Port 4 – IP address – Subnet mask – Gateway (optional)
Virtual Ethernet port (VRTETHPORT) Full, Basic	Specifies the TCP/IP configuration for the virtual Ethernet networks used by the file server. A matching virtual Ethernet port is required to install the Windows Cluster service. ***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 – *VRTETHx – IP Address – Subnet mask – Associated Port (Optional) • Virtual port 2 – *VRTETHx – IP Address – Subnet mask – Associated Port (Optional) • Virtual port 3 – *VRTETHx – IP Address – Subnet mask – Associated Port (Optional) • Virtual port 4 – *VRTETHx – IP Address – Subnet mask – Associated Port (Optional)
TCP/IP local domain name (TCPDMNNAME) Full	Specifies the TCP/IP local domain name associated with the integrated server. You can specify *SYS to use the same value the i5/OS system uses.	

Field	Description and Instructions	Value
TCP/IP name server system (TCPNAMSVR) Full	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 the i5/OS uses.	
To workgroup (TOWRKGRP) Full	Specifies the name of the Windows server workgroup in which the server participates.	
To domain (TODMN) Full	Specifies the name of the Windows domain in which the server participates.	
Server message queue and library (MSGQ) Full, Basic	Specify the name of the message queue and the library it will be located in. If the message queue does not already exist, the INSWNTSVR command creates it. The message queue is where all event logs and errors associated with this server are sent. You should specify a MSGQ name and library. You can also specify *JOBLOG to send nonsevere errors to the job log of the user administration monitor and severe errors to QSYSOPR. If you specify *NONE, nonsevere errors are not sent to i5/OS, and severe errors are sent to QSYSOPR.	Queue: Library:
Event log (EVTLOG) Full, Basic	Specifies whether or not i5/OS receives event log messages from the integrated server. The choices are all, system, security, application, or none: ***ALL** i5/OS receives all event log messages. ***NONE** No event log messages are received. ***SYS** i5/OS receives system event log messages. ***SEC** i5/OS receives security event log messages. ***APP** i5/OS receives application event log messages. **Note:** If you have the integrated server send its security log to the iSeries (by specifying *ALL or *SEC), be sure to set up the message queue with the correct security.	

Field	Description and Instructions	Value
Installation source and system drive sizes and auxiliary storage pool (ASP) (SVRSTGSIZE) (SVRSTGASP) (STGASPDEV) Full, Basic	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 system drive (drive C) must be large enough to hold the Windows server operating system. 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 i5/OS creates and links the drive as a FAT32 or NTFS network server storage space, depending on the size. For more information about these drives, see "Predefined disk drives for integrated Windows servers" on page 162. **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 iSeries Navigator. For more information about working with independent ASPs, see Independent disk pools. Both the Information Center and iSeries Navigator refer to ASPs as disk pools. To use an independent ASP, the ASP device must be available prior to running the INSWNTSVR command.	Installation source drive: Size: ASP: ASPDEV: System drive: Size: ASP: ASPDEV:

Field	Description and Instructions	Value
License mode (LICMODE) Full	Determines the license mode to install Microsoft Windows server. **Element 1 License type:** ***PERSEAT** Indicates that a client license has been purchased for each computer, device, or user that accesses the 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 is specified. **number-client-licenses:** Specifies the number of client licenses purchased for the server being installed. **Element 3 Windows Terminal Services:** ***TSENABLE** For Windows 2000, install Windows Terminal Services and Terminal Services licensing. ***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.	License type: Client licenses: Terminal services:
Propagate domain user (PRPDMNUSR) Full, Basic	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.	
Shutdown timeout (SHUTDTIMO) Full, Basic	A value which determines how long i5/OS waits to allow programs to end before shutting down the integrated server. The delay can be from 2 to 45 minutes. If you do not specify a value, it will be set to 15 minutes.	Shutdown timeout:

Field	Description and Instructions	Value
Restricted device resources (RSTDEVRSC) Full, Basic	Restricts iSeries 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.	
Time zone Full	(Optional) Records the time zone of the iSeries for use in the Windows server phase of installation. See “Time synchronization” on page 62.	
Virtual Ethernet point to point (VRTPTPPORT) Full, Basic	A local area network (see “Networking concepts” on page 28) 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:
Configuration file (CFGFILE) Full, Basic	During the installation, creates and specifies a customized NWSD (see Chapter 15, “Network server description configuration files,” on page 243). The default is *NONE. To specify a configuration file that you have created, substitute the name of the file and the library where it is stored (*LIBL, *CURLIB, or the name of the library).	

Installation worksheet for additional internet SCSI (iSCSI) parameters

Field	Description and Instructions	Value
Activation timer (ACTTMR)	Specifies the amount of time in seconds that the system will wait for the connection to be established to the remote server's service processor and to power on the remote server. The default value is 120. Specify a value in seconds ranging from 30 through 1800.	Activation timer:
Communications message queue (CMNMSGQ)	Specifies the name of a message queue to receive communications status messages. **Qualifier 1:** • ***SYSOPR** Causes messages to be placed in the system operator message queue. • ***name*** Specify the name of a message queue to receive communications status messages. **Qualifier 2:** • ***LIBL** All libraries in the job's library list are searched until the first match is found • ***CURLIB** The current library for the job is searched. If no library is specified as the current library for the job, the QGPL library is used. • ***library-name*** Specify the name of the library to be used	Message queue: Library:
Storage path (STGPTH)	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.	NWSH name:

Field	Description and Instructions	Value
Virtual Ethernet path (VRTETHPTH)	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) 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.	Virtual Ethernet path: Port: NWSH name:
Shutdown TCP port (SHUTDPORT)	Do not use this parameter.	
Virtual Ethernet control port (VRTETHCTLP)	Specifies the TCP port to use for virtual Ethernet control. **Note:** This is an advanced parameter that may be useful when there is a firewall in the iSCSI network. **8800** Use the TCP port number of 8800. **integer** Specifies the port number identifying the port that is to be used for virtual Ethernet control. Valid values range from 1024 through 65,535.	
Remote system NWSCFG (RMTNWSCFG)	Specifies the remote system network server configuration to use with this server. **Note:** It may be preferable or even necessary to create the remote system configuration before you run the INSWNTSVR command. See “Create a service processor configuration and a remote system configuration” on page 66. ***DFT** Use the system generated default remote system network server configuration name of ’nwsdnameRM’ where nwsdname is the name of the network server description. **name** Specify the name of an existing remote system network server configuration.	

Field	Description and Instructions	Value
Service processor NWSCFG (SPNWSCFG)	Specifies the service processor network server configuration to use with this server. **Note:** It may be preferable or even necessary to create the service professor configuration before you run the INSWNTSVR command. See "Create a service processor configuration and a remote system configuration" on page 66. ***DFT** Use the system generated default service processor network server configuration name of 'nwsdnameSP' where nwsdname is the name of the network server description. **name** Specify the name of an existing service processor network server configuration.	
Connection security NWSCFG (CNNNWSCFG)	Specifies the connection security network server configuration to use with this server. ***DFT** Use the system generated default connection security network server configuration name of 'nwsdnameCN' where nwsdname is the name of the network server description. **name** Specify the name of an existing connection security network server configuration.	
Default IP security rule (DFTSECRULE)	Specifies the default IP Security (IPSec) rule used between the hosting and remote system. **Note:** This parameter is ignored if you specified an existing connection security configuration in the CNNNWSCFG parameter ***NONE** IP Security rules are not configured. ***GEN** The system will automatically generate a random pre-shared key. **pre-shared-key** Specify the pre-shared key. A pre-shared key is a nontrivial string up to 32 characters long.	
IP security rule (IPSECRULE)	Specify the relative entry of the IP security rules (IPSECRULE) parameter, defined in the existing connection security network server configuration that will be used as the initial IP security setting between the hosting and remote system. ***DFTSECRULE** Use the value specified on the Default IP security rule (DFTSECRULE) parameter. ***NONE** Remote interface will not use any security rule. **1-16** Remote interface will use security rule specified.	

Field	Description and Instructions	Value
Initialize service processor (INZSP)	Specifies how the remote system's service processor is secured. **Note:** You cannot specify *SYNC if the service processor configuration already exists. *MANUAL, *AUTO, and *NONE are only used if the service processor configuration does not exist. ***MANUAL** This is the most secure method. You must manually configure the user name, password and certificate for the service processor. Certificate management is required. This method is appropriate to protect your service processor password when you connect to it over public networks. ***AUTO** You do not need to manually configure parameters on the remote system's service processor. The service processor of the remote system will automatically generate a certificate. The connection is secure once initialized. This option is appropriate if you connect to the service processor over a network that is physically secure or is protected by a firewall. ***SYNC** This network server configuration will synchronize the user, password, and self-signed certificate with the service processor. ***NONE** There is no security for the service processor password. Do not use this unless you connect to the service processor over a physically secure network.	
Enable unicast (ENBUNICAST)	Unicast is a transmission method where packets are sent directly to the specified Service processor name (SPNAME) or Service processor address (SPINTNETA) parameter. The system identification for the Enclosure identifier (EID) parameter is automatically retrieved if *AUTO is specified and the system hardware supports it. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter ***NO** Disable unicast ***YES** Enable unicast.	

Field	Description and Instructions	Value
Enclosure identifier (EID)	Specifies the identifying serial number, type and model of the enclosure containing the service processor. They are required to locate the remote system on the network when ENBUNICAST(*NO) is specified. Look for these values on the label of the system. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter ***AUTO** Automatically retrieve the identifier when ENBUNICAST(*YES) is specified. **Element 1: Serial number** Specify the remote system's machine serial number using only alphanumeric characters without dashs. **Element 2: Manufacturer type and model** Specify the remote system's machine type and model in the form ttttmmm where tttt is the machine type and mmm is the machine model number.	
Service processor name (SPNAME)	Specifies the remote system's service processor host name. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter ***SPINTNETA** The remote system is identified by the value specified for the Service processor address (SPINTNETA) parameter. **host-name:** Specify the remote system's service processor host name.	
Service processor address (SPINTNETA)	Specify the remote system's service processor internet address. Internet addresses are expressed in the decimal form nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter **internet-address:** Specify the internet address of the service processor.	

Field	Description and Instructions	Value
SP authentication (SPAUT)	Specifies the service processor user name and password. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter ***DFT** The default service processor userid and password are used. **Element 1: User name** Specify the remote system's service processor user name. **Element 2: User Password** Specify remote system's service processor password. Password must be at least 5 characters in length and contain at least one alphabetic character and one numeric or symbolic character.	Name: Password:

Field	Description and Instructions	Value
SP certificate identifier (SPCERTID)	The SP certificate identifier specifies one of three possible fields that identifies the service processor's certificate. This parameter is specified to provide additional validation that the certificate is from the service processor. The contents of the selected field must exactly match the value of the field that was entered when the certificate was generated or requested from a certificate authority. **Note:** This parameter is ignored if you specified an existing service processor configuration in the SPNWSCFG parameter. **Single values:** ***NONE** Service processor certificate is not configured. **Element 1: Component** ***COMMONNAME** Selects the certificates common name specified when the certificate was generated or requested from a certificate authority. On the Remote Supervisor Adapter II this correlates to the ″ASM Domain Name″ field used to generate a self-signed certificate or generate a certificate signing request. ***EMAIL** Selects the certificate's e-mail address specified when the certificate was generated or requested from a certificate authority. On the Remote Supervisor Adapter II this correlates to the **Email address** field used to generate a self-signed certificate or generate a certificate signing request. ***ORGUNIT** Selects the certificate's organizational unit specified when the certificate was generated or requested from a certificate authority. On the Remote Supervisor Adapter II this correlates to the **Organizational Unit** field used to generate a self-signed certificate or generate a certificate signing request. **Element 2: Compare value** **compare-value** Specify the certificates component compare value. Specify no more than 255 characters of text, enclosed in apostrophes.	Component: Compare value:

Field	Description and Instructions	Value
Remote system identifier (RMTSYSID)	Specifies the identifying serial number, type and model of the remote system. When specified, they are used to locate the remote system on the network. Look for these values on the label of the remote system. **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. **Single values:** ***EID** Use the service processor enclosure identifier. **Element 1: Serial number** **serial-number** Specify the remote system's machine serial number. **Element 2: Manufacturer type and model** **type-model** Specify the remote system's machine type and model in the form ttttmmm where tttt is the machine type and mmm is the machine model number.	Serial number: Manufacturer type and model:
Delivery method (DELIVERY)	Specifies how the parameters necessary to configure the remote system are delivered. **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. ***DYNAMIC** Parameters are dynamically delivered to the remote system using DHCP. ***MANUAL** Parameters are manually configured on the remote system using the BIOS utilities (System BIOS or Adapter BIOS - CTRL-Q).	
CHAP authentication (CHAPAUT)	Specifies the Challenge Handshake Authentication Protocol (CHAP) for the host system iSCSI target to authenticate the remote system initiator node. **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. **Single values:** ***NONE** CHAP authentication is not enabled. **Element 1: CHAP name** Specify the CHAP name. **Element 2: CHAP secret** Specify the secret you want to use for the Challenge Handshake Authentication Protocol as a value up to 24-characters long.	CHAP name: CHAP secret:

Field	Description and Instructions	Value
Boot device ID (BOOTDEVID)	Specifies the PCI Function Address (Bus/Device/Function) of the iSCSI adapter in the remote system that will be used to boot from. This information can be accessed using the BIOS utilities (System BIOS or Adapter BIOS - CTRL-Q). **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. **Single values:** ***SINGLE** The single iSCSI adapter is used on the remote system Note: Remote systems with more than one iSCSI adapter installed in the server are required to specify which adapter will be used to boot from. **Element 1: Bus number** Specify the bus number of the remote system's iSCSI adapter that will be used to boot. **Element 2: Device number** Specify the device number of the remote system's iSCSI adapter that will be used to boot. **Element 3: Function** **function-number** Specify the function number of the remote system's iSCSI adapter that will be used to boot.	Bus number: Device: Function:

Field	Description and Instructions	Value
Dynamic boot options (DYNBOOTOPT)	This is an advanced function. This parameter is used to configure the internal DHCP Server that is part of the iSCSI Target Host Bus Adapter firmware and its required to provide IP address and diskless boot parameters for the remote iSCSI Initiator. **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. **Element 1:** **Vendor ID** The client and server are pre-configured to a fixed vendor ID. Network administrators can configure clients to define their own idetifying values to convey hardware, operating system or other identifying information. DHCP option 60 described in the IETF RFC 2132 is used for this function. ***DFT** The default vendor ID will be used. **vendor-id** Vendor ID of the remote system's iSCSI adapter that will be used. **Element 2:** **Alternate client ID** Used by clients to specify their unique identifier to the server. Each client's identifier must be unique among all other client identifiers used on the effective DHCP network to which the client is attached (that is, the client's local subnet and any remote subnets reachable using DHCP relay). Vendors and system administrators are responsible for choosing client identifiers that meet this requirement for uniqueness. DHCP option 61 described in the IETF RFC 2132 is used for this function. ***ADPT** The default Client ID consists of the adapter address for the remote system's iSCSI adapter. This value will be used to identify the remote system. **client-id** Specify the Client ID of the remote system's iSCSI adapter that will be used to boot.	Vendor ID: Alternate client ID:

Field	Description and Instructions	Value
Remote interfaces (RMTIFC)	Specifies the remote system interfaces. This information is used to identify and configure the remote system's interfaces. Each adapter port has two functions to support a SCSI and a LAN interface. **Note:** This parameter is ignored if you specified an existing remote system configuration in the RMTNWSCFG parameter. **Element 1: SCSI interface** **Element 1: Adapter address** Specify the 12-character hexadecimal adapter address for the remote system's SCSI interface. **Element 2: Internet address** **internet-address** for the remote system's SCSI interface. **Element 3: Subnet mask** **subnet-mask** for the remote system's SCSI interface. **Element 4: Gateway address** **gateway-address** for the remote system's SCSI interface. **Element 5: iSCSI qualified name** ***GEN** The system will automatically generate the iSCSI qualified name. **iqn-name** iSCSI qualified name for the remote system's SCSI interface.	SCSI interface • Adapter address: • Internet address: • Subnet mask: • Gateway address (Optional): • iSCSI qualified name:
Remote interfaces (RMTIFC) continued	**Element 2: LAN interface** **Element 1: Adapter-address** 12-character hexadecimal adapter address for the remote system's LAN or TCP Offload Engine (TOE) interface. **Element 2: Internet address** for the remote system's LAN interface. **Element 3: Subnet mask** for the remote system's LAN interface. **Element 4: Gateway address** for the remote system's LAN interface.	LAN interface • Adapter-address: • Internet address: • Subnet mask: • Gateway address (Optional):

Windows Cluster Service information

Notes:

1. Fill in this work sheet only when installing a clustered integrated server and your hardware model supports Windows Cluster service. (Integrated Netfinity Servers do not support Windows Cluster service.)

2. Network adapters are referred to as ports in i5/OS.

Item	Description and Instructions	Value
Cluster name	Specifies the name of the cluster. Administrators will use this name for connections to the cluster. The cluster name must be different from the domain name, from all computer names on the domain, and from other cluster names on the domain. The cluster name is also used to create the network server storage space that will be used as the Windows cluster quorum resource. ***NONE:** Do not form or join a Windows Cluster. **cluster-name:** Specify the name of the cluster.	

Item	Description and Instructions	Value
Cluster configuration: (Elements 1 - 4)	Specifies the parameters required to configure a new Windows Cluster. **Notes:** This parameter is used to verify the i5/OS cluster configuration. The Microsoft configuration wizards are used to install the Cluster service. This parameter is only required when forming a new Windows cluster using the Cluster name (CLU) parameter. **Element 1: Cluster domain name** Specifies the domain to which the cluster belongs. If the cluster already exists, the cluster will be joined, otherwise, the cluster will be formed. If forming a cluster, the Cluster configuration (CLUCFG) parameter must be specified. **cluster-domain-name:** Specify the domain name to which the cluster belongs when forming a new cluster. **Element 2: Quorum resource size** Specifies the size in megabytes of the storage space used as the Windows quorum resource. ***CALC** Specifies that the size should be calculated to be the default value based on the Windows server version (WNTVER) parameter. **quorum-size** Specifies the Windows quorum resource size in megabytes. The size must be at least 550 megabytes but no larger than 1024000 megabytes. **Element 3: Quorum resource ASP** Specifies the auxiliary storage pool for the storage space used as the Windows quorum resource. Specify one of the following values: **1:** The storage space is created in auxiliary storage pool 1, the system auxiliary storage pool (ASP). **quorum-ASP:** Specify a value ranging from 2 through 255 for the ASP identifier. Valid values depend on how many ASPs are defined on the system. **Element 4: Quorum ASP device** Specifies the independent auxiliary storage pool device name for the storage space used as the Windows quorum resource. **Note:** You cannot specify both a Quorum resource ASP and a Quorum ASP device value.	Cluster domain name: Quorum resource size: Quorum resource ASP: Quorum ASP device:

Item	Description and Instructions	Value
Cluster configuration: (Elements 5-7)	**Element 5: Cluster connection port** Specifies the connection port used for the Cluster service communication. ***VRTETH*x*:** The network server virtual Ethernet port *x* is configured, where *x* has a value of 0 through 9. **Note:** The virtual Ethernet port must be configured to match this value.**Element 6: Cluster Internet Address** Specifies the Internet address for the cluster. **IP address:** Specify the cluster internet address in the form, xxx.yyy.zzz.nnn, where xxx, yyy, zzz, and nnn are decimal numbers ranging from 0 through 255. **Note:** The Internet address selected must be unique across all NWSD objects and the i5/OS TCP/IP configuration. **Element 7: Cluster Subnet Mask** **subnet-mask:** Specifies the subnet mask for the cluster in the form, nnn.nnn.nnn.nnn, where nnn is a decimal number ranging from 0 through 255.	Connection port: Cluster Internet Address: Cluster Subnet mask:

Comparison of FAT, FAT32, and NTFS file systems

Windows 2000 Server or Windows Server 2003 allow you to choose between NTFS and FAT32 file systems. IBM i5/OS Integrated Server Support installs your system drives using an appropriate file system that depends on the hardware resource capabilities, Windows version and intended use. The installation command converts FAT32 drives to NTFS unless CVTNTFS(*NO) is specified.

Note: **Do not** convert the **D** drive to NTFS. It must remain FAT.

You do have the option of converting the C drive. Here are some comparisons that might help you decide:

FAT	FAT32	NTFS
Volume from floppy diskette size up to 4 GB	Volumes from 512 MB to 2 terabytes	Volume 10 MB to 2 TB
Maximum file size 2 GB	Maximum file size 4 GB	File size limited by size of volume
Does not support Windows 2000 or Windows Server 2003 Active Directory	Does not support Windows 2000 or Windows Server 2003 Active Directory	Required to use Windows 2000 or Windows Server 2003 Active Directory or shared cluster drives
Allows access to files on the hard disk with PC-DOS.	Allows access to files on the hard disk with PC-DOS.	Does not allow access to files on the hard disk with PC-DOS.
Allows you to customize your server with NWSD configuration files	Allows you to customize your server with NWSD configuration files.	Cannot use NWSD configuration files.
Allows you to use the NWSD dump tool (QFPDMPLS) to retrieve files from the disk for service	Allows you to use the NWSD dump tool to retrieve files from the disk for service	Cannot use the dump tool to retrieve files from the disk

Tip: Find resource names when you have multiple integrated servers

You can have multiple integrated servers of the same type installed on your iSeries. If so, you may not be able to tell them apart on the Display Communication Resources display.

To find out which integrated server a resource name refers to, follow these steps:

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 Network Server Host Adapter. This is the resource to be used when creating an NWSH object. The NWSH object name is used when installing the NWSD.
3. Look at the Card Position under the Physical Location heading.
4. Look at the labels on the slots of your iSeries. 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 xSeries Server hardware to which the resource name refers.

Go back to "Installation worksheet for i5/OS parameters" on page 68.

Supported language versions

These languages are supported on the Language version parameter (LNGVER) of the Install Windows server (INSWNTSVR) command:

LNGVER	National Language
*PRIMARY	Uses the language version of the primary language that is installed on iSeries
2911	Slovenian
2922	Portuguese
2923	Dutch
2924	English upper/lowercase
2925	Finnish
2926	Danish
2928	French
2929	German
2931	Spanish
2932	Italian
2933	Norwegian
2937	Swedish
2938	English uppercase DBCS
2939	German MNCS
2940	French MNCS
2942	Italian MNCS
2950	English uppercase
2962	Japanse DBCS
2963	Dutch MNCS
2966	Belgian French
2975	Czech
2976	Hungarian

LNGVER	National Language
2978	Polish
2979	Russian
2980	Brazilian Portuguese
2981	Canadian French MNCS
2984	English upper/lowercase DBCS
2986	Korean DBCS
2987	Chinese, Traditional
2989	Chinese, Simplified
2994	Slovakian
2996	Portuguese MNCS

IBM i5/OS Integrated Server Support supports Windows Multi-Language User Interface.

Install Windows 2000 Server or Windows Server 2003

You will need the following:

- A CD that contains the Windows 2000 Server or Windows Server 2003 software (or an image of the CD).
- Your Windows license key (printed on the back of the installation CD jewel case or Certificate document).
- A completed and printed “Installation worksheet for i5/OS parameters” on page 68 or the command string generated by the installation advisor.

Notes:

1. Microsoft documentation tells you to disable disk mirroring and disconnect any uninterruptible power supply before installing or upgrading Windows server. Be aware that this does not apply to disk mirroring or an uninterruptible power supply that you have on your iSeries.
2. If you have an Integrated xSeries Server, an Integrated xSeries Adapter, or an iSCSI HBA that is not listed in the “Hardware requirements” on page 57 section, see the System i integration with BladeCenter and System x Web site for installation instructions.

Do the following steps:

1. Prepare the integrated xSeries hardware. For more information, see the following links.
   - IXA install read me first (www.ibm.com/systems/i/bladecenter/ixa/readme/)
   - iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/)
   - IXS install read me first (www.ibm.com/systems/i/bladecenter/ixs/readme/)
2. If you are installing an iSCSI attached server, see “Prepare iSCSI hardware for Windows installation” on page 90
3. “Start the installation from the i5/OS console” on page 90.
4. “Continue the installation from the integrated Windows server console” on page 94.
5. “Complete the server installation” on page 95.

If you encounter any error messages during the installation, see “Respond to error messages during installation” on page 105.

Prepare iSCSI hardware for Windows installation

For iSCSI attached servers, there are some additional things to configure after you prepare the hardware.

- “Initialize service processor security”
- “Create and start a network server host adapter”

Initialize service processor security

If you created a new service processor configuration for a new service processor, you should change the security settings from the service processor’s default user name and password to a new user name and password that you select.

Select the procedure from the following list that corresponds to the security method that you decided to use.

- For a service processor password without SSL, use the procedure described in “Service processor password” on page 131.
- For a service processor password with SSL, use the procedure described in “Configure service processor SSL” on page 130.

Create and start a network server host adapter

You must configure a target iSCSI HBA in your iSeries server before installing Windows on an iSCSI attached server. This configuration is called a network server host adapter (NWSH) device.

An NWSH device can be used by more then one active server. If your new server will use an existing NWSH device, verify that the existing NWSH device is started.

To create and start (vary on) a new NWSH device, do the following steps.

1. Identify the NWSH hardware resources as follows using iSeries Navigator:
   a. Expand **Configuration and Service —> Hardware —> Communications**.
   b. Note the resource name for any resource with the description Network Server Host Adapter.
   c. If you want to use a CL command use WRKHDWRSC TYPE(*CMN).
2. Create an NWSH device. See “Create a network server host adapter object” on page 117.
3. Start the NWSH device. See “Start a network server host adapter” on page 119.

Start the installation from the i5/OS console

If you are installing an iSCSI attached server, you should be following the process in the iSCSI install read me first. IBM Director server should be running on your iSeries server. For information about starting Director Server, see “Verify that IBM Director Server is installed and running” on page 142.

To install Windows 2000 Server or Windows Server 2003 on iSeries, 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. When performing an installation type of *FULL, place the installation CD in the iSeries server optical drive (unless you plan to use an image of the installation CD).

   When performing an Install type of *BASIC, place the ServerGuide CD in the attached xSeries server CD-ROM drive.
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 "Continue the installation from the integrated Windows server console" on page 94.

- 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 i5/OS parameters" on page 68 in each of the following fields:

3. In the Network server description field (see "Network server descriptions" on page 67 for more information), type the server name from the "Installation worksheet for i5/OS parameters" on page 68 and press `Enter`.
4. In the `Install type field`, type the value (*FULL or *BASIC) that you filled out in the "Installation worksheet for i5/OS parameters" on page 68.
5. In the `Resource Name` field, type the information that you filled out in the "Installation worksheet for i5/OS parameters" on page 68.
6. Choose the `Windows server version` you want to install; press Enter.

   Note: Windows Server 2003 is required for iSCSI attached servers.
7. 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 i5/OS parameters" on page 68. Otherwise, skip this step and use the default value *NONE.
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 i5/OS parameters" on page 68.
11. Type the values from the "Installation worksheet for i5/OS parameters" on page 68 in these fields:
    - TCP/IP local domain name
    - TCP/IP name server system
    - Server message queue
    - Library
12. In the `Event log` field, specify which event log messages you want i5/OS to receive from the server.
13. In the fields for the `Server storage spaces`, type the values from the "Installation worksheet for i5/OS parameters" on page 68:
    - 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.
    - 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.
    - For system drives up to 32 GB, in the Convert to NTFS field, you can specify *NO to leave the integrated server's system drive formatted with the file allocation table (FAT32) file system. Otherwise, use the default of `*YES` to convert the system drive to the New Technology File System (NTFS) during the installation. For information that might help you decide, see "Comparison of FAT, FAT32, and NTFS file systems" on page 87. The INSWNTSVR command automatically converts system drives larger than 32 GB to NTFS if necessary.

14. **Optional:** Specify either a Windows workgroup or domain in the corresponding To workgroup or To domain parameters.
15. **Optional:** Specify the name of the user who holds the Windows server license you are installing in the Full Name field.
16. **Optional:** Specify the name of the organization that holds the Windows server license you are installing, in the Organization field.
17. 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 "Supported language versions" on page 88.
18. In the Synchronize date and time field, specify *YES to have i5/OS synchronize the date and time with the integrated server every 30 minutes. If you want i5/OS to synchronize the date and time with the integrated server only when you vary it on, type *NO.
19. 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.
20. In the Windows license key field, specify the CD key that Microsoft has provided, including the dash. In most cases, you can find this CD key printed on the back of the Windows installation CD jewel case.
21. In the License type field, specify the type of Windows server license that you purchased.
22. If you specified *PERSERVER in the License type field, then in the Client licenses field, specify the number of client licenses that you purchased.
23. Enter the Terminal services options to install in the Terminal services field.
24. In the Restricted device resources field, type the value from the "Installation worksheet for i5/OS parameters" on page 68.
25. In the Shutdown timeout field, specify the integrated server's shutdown time-out value in minutes. This is used to limit the amount of time that the integrated server's operating system is given to shut down before the server is varied off.
26. If you are installing an IXA attached or IXS server, continue to step 34 on page 93 and fill out additional parameters. If you are installing an ISCSI attached server, type the values for the iSCSI parameters from the "Installation worksheet for i5/OS parameters" on page 68 in the following fields:
    - Activation timer
    - Communications message queue
27. 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 43.
28. 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.
29. **Optional:** Specify the Shutdown TCP port and the Virtual Ethernet control port.
30. Enter an existing network server configuration name for the following fields or select the default values.
    - Remote system NWSCFG
    - Service processor NWSCFG
    - Connection security NWSCFG

    Press Enter.
31. Enter the IP Security (IPSec) rule to use:
    - For an existing Connection security NWSCFG:

    a. Specify the configured security rule to use the IP security rule field.
    b. Press Enter.
  - For a defaulted Connection security NWSCFG:
    a. Specify the default IP Security (IPSec) rule to use in the Default IP security rule field
    b. Press Enter.

32. If prompted, enter service processor configuration information from the "Installation worksheet for i5/OS parameters" on page 68 in these fields, when using the defaulted Service processor NWSCFG name:
    - In the Initialize service processor field:
      – a. When initializing the service processor is any value other than *NONE, enter a Component and Compare value for the SP certificate identifier 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.
33. If prompted, enter remote system configuration information from the "Installation worksheet for i5/OS parameters" on page 68 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 CHAP authentication field, enter the Challenge Handshake Authentication Protocol (CHAP) values used to authenticate the remote system.
    - In the Boot device ID field, identify the iSCSI adapter used to boot the remote system. Use the default value *SINGLE if there is only one iSCSI boot device in the remote system.
    - 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
34. Filling out additional parameters allows you to do the following things:

- 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.)
- Use your own IP addresses for the point to point virtual Ethernet.
- Use an NWSD configuration file. See Chapter 15, “Network server description configuration files,” on page 243.
- Configure a new or existing Windows Cluster configuration.

Provide any other information that seems relevant for your needs and press Enter.

The integrated Windows server starts to install. The second stage of the installation process is “Continue the installation from the integrated Windows server console.” The process will take approximately 1 hour, depending on your hardware configuration.

Continue the installation from the integrated Windows server console

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 “Prepare for the installation of integrated Windows servers” on page 60 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 “Respond to error messages during installation” on page 105.
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 “Time synchronization” on page 62.
   b. 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.

To complete the installation of Windows server when using ServerGuide, perform these tasks:

- Insert the ServerGuide CD in the local optical drive of the HSL attached server. (The IXA attached xSeries server.)
- Respond **G** to the message NTA100C ″Insert ServerGuide CD-ROM into &2 optical device. (C G)″
- Follow the ServerGuide Wizard through the install process.

See “Complete the server installation” on page 95.

Complete the server installation

Perform a few final tasks after installing Windows 2000 Server or Windows Server 2003 on i5/OS to verify that it is correctly installed and ready.

1. It is recommended to install the latest supported Microsoft service pack. Refer to the Microsoft Service packs page for the latest supported service pack list on the Microsoft service packs page of the System i integration with BladeCenter and system x Web site and to run Windows Update.
2. If you want the integrated Windows server to automatically vary on when you start TCP/IP, see “Set an integrated Windows server to automatically vary on with TCP/IP” on page 106.
3. If the QRETSVRSEC system value was not already enabled for an iSCSI attached server install, change the QRETSVRSEC system value on i5/OS to ensure that i5/OS keeps passwords (this avoids delays when users sign on):
   - On the i5/OS command line, enter the command:
     ```
     WRKSYSVAL SYSVAL(QRETSVRSEC)
     ```
   - To change the value, enter a `2` in the `Option` field and press Enter.
   - Change the value of `Retain server security data` to `1`.
4. 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.
5. You can create additional disk drives for applications and data, rather than storing these items on the system drive. See “Add disk drives to integrated Windows servers” on page 164 for more information.

   Note: When working with storage in the Windows operating system, there is an option to convert a basic disk to a dynamic disk. This is not related to dynamically linking storage in i5/OS operating system. If you plan on using the DISKPART command line utility in Windows, either do not change the disk from basic to dynamic, or specify sizes that will not cause volumes to be misaligned as listed in the iSCSI Disk I/O section of System i Performance Capabilities Reference . If you already have a dynamic disk, you can create and link additional disks to extend a spanned volume instead of using the DISKPART utility.
6. 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 Chapter 6, “Manage virtual Ethernet and external networks,” on page 111 for more information.
7. You may want to enroll some of your i5/OS users to the Windows server or domain. See Chapter 11, “Administer integrated Windows server users from i5/OS,” on page 177 for more information.
8. 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.)
9. You can customize your servers by creating your own NWSD configuration file. See Chapter 15, “Network server description configuration files,” on page 243.
10. If you want Windows clustering, see “Windows Cluster Service” on page 98.
11. If your server is installed with Windows Server 2003 and has Active Directory installed (for example, it is a domain controller), see “Enabling Kerberos with a Windows Server 2003 Active Directory Server” on page 104.
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 “Time synchronization” on page 62.
    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. If you are using a 2892-002 or 4812-001 IXS hardware type with Microsoft Windows 2000 Server, you should install special video device drivers to take advantage of the ATI Radeon video chip which is on the 2892-002 and 4812-001 IXS. See “Install the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 104.
14. If you are using a 2892-002 or 4812-001 IXS hardware type with Microsoft Windows Server 2003, you should adjust the hardware acceleration settings to achieve optimal performance. See “Adjust hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 105.

For iSCSI attached servers you can also do the following steps:

1. You can configure your server to use additional iSCSI HBAs to improve performance or availability. See “Configuring multipath I/O” on page 138 and “Manage iSCSI HBA usage” on page 133 for more information.
2. If your iSCSI network supports large frame sizes, you may be able to improve your virtual Ethernet performance. See “Maximum transmission unit (MTU) considerations” on page 139 for more information.

Upgrade the IBM iSeries Integration for Windows Server licensed program

If you are upgrading i5/OS and IBM iSeries Integration for Windows Server to V5R4, you need the CD containing 5722-SS1. If you also plan to install new Integrated xSeries Server hardware, make sure you complete this software installation first. As you follow the upgrade procedure in the iSeries Software Installation manual , take these additional steps:

Preparing to upgrade:

1. Ensure that you have the latest code fixes installed on all your existing integrated Windows servers, as well as on your i5/OS. See “Code fixes” on page 106.
2. Ensure that you have a system backup available that includes the storage allocated to your integrated servers.
3. As a precaution, record the associated resources for your hardware:
   a. On the i5/OS command line, type `WRKCFGSTS *NWS` and press Enter.
   b. Type 8 in the option column next to the network server description. The Work with Network Server Descriptions display appears.
   c. Type `5` in the option column next to the network server description.
   d. Page down until you see the field `Resource name` and record the value for this network server (for example, LIN05).
   e. Press F12 twice to back out of this command.
   f. On the i5/OS command line, type `WRKHDWRSC TYPE(*CMN)` and press Enter.
   g. Type `7` (Display resource detail) in the option column next to the resource name that you identified in step 3 d. The type column has the CCIN number for the Integrated xSeries Server hardware, and the text description should be `File Server IOP` or `File Server IOA`.
   h. If you have multiple Integrated xSeries Servers of the same type installed on your iSeries, you may be able to identify the correct one by card position:
      1) look at the `Card Position` under the `Physical Location` heading.
      2) Look at the labels on the slots of your iSeries. 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 xSeries Server to which the resource name refers.
   i. Record the information that appears in the `Type-model` and `Serial number` fields.
   j. Press F12 twice to back out of the command.
4. Vary off all of your integrated servers. See “Start and stop an integrated server” on page 149.

To install the new version of i5/OS on your iSeries, return to the procedure in the iSeries Software Installation manual .

After upgrading i5/OS, complete these additional steps:

1. Start the integrated server (see "Start and stop an integrated server" on page 149) and verify that it has the same resource name:
   a. On the i5/OS command line, type `WRKHDWRSC TYPE(*CMN)` and press Enter.
   b. Type `7` (Display resource detail) in the option column next to the resource name that you identified in step 3d on page 96. Verify that the information that appears in the `Type-model` and `Serial number` fields match what you recorded for this resource.
   c. If these fields do not match what you recorded, do this:
      1) Press F12 to back out to the previous display.
      2) Use option 7 to display the resource details for other resource names in the list until you find the one whose `Type-model` and `Serial number` match those your recorded. Note the resource name that i5/OS now associates with this Integrated xSeries Server hardware. Press F12 to back out of this command.
      3) On the i5/OS command line, type `WRKNWSD` and press Enter. The Work with Network Server Descriptions display appears.
      4) Type `2` (change) in the option column next to the network server description and press Enter. The Change Network Server Description display appears.
      5) Change the resource name to the new correct resource name for this network server.
2. Install IBM i5/OS Integrated Server Support on your existing integrated servers. See "Install IBM i5/OS Integrated Server Support" on page 64.

Upgrade the integrated server side of IBM i5/OS Integrated Server Support

IBM i5/OS Integrated Server Support is the software which couples together the iSeries and its integrated Windows servers. Think of it as a translation program. Half of the program runs on the iSeries to translate from the Windows language to the i5/OS language, and the other half runs on the integrated servers to translate from the i5/OS language to the Windows language.

New versions of IBM i5/OS Integrated Server Support are installed to i5/OS. Then the integrated server part of the licensed program needs to be copied over to the integrated server and installed.

You need to upgrade your existing integrated Windows servers' licensed program when you install:

- A new version of IBM i5/OS Integrated Server Support.
- A new version of Windows server from Microsoft.

New version of IBM i5/OS Integrated Server Support

When you install a new version of IBM i5/OS Integrated Server Support, you need to upgrade all your existing integrated servers to that level. If you have multiple integrated servers, you might want to upgrade those servers remotely from i5/OS.

This procedure requires that you have the same userid and password on the integrated Windows servers and i5/OS.

To upgrade an integrated server, follow these steps:

1. End any applications that are running.
2. Ensure that no users are logged on to the integrated server.

Attention: The integrated server automatically restarts after completion of the installation, so if you skip steps 1 and 2, you risk data loss.

3. From the **Start** menu, choose **Programs**, then **IBM iSeries**, then **Integration for Windows Server**, then **Software Level**.

   Note: When a new level of the licensed program is available for installation, logging on to an integrated server as an administrator causes Software Level to start automatically.

4. If you are upgrading from V5R3 or later, select the option to **Synchronize**. Otherwise, select the option to **Install Release from iSeries**.
5. Follow the user interface instructions to complete the installation.
6. **Tip:** Afterward, back up the predefined installation and system drives for this server. See "Back up predefined disk drives for integrated Windows servers" on page 188 for information about backing up these drives. Since it is safer to back up all storage spaces for the server at the same time, you should also back up the associated user-created storage (described in "Back up user-defined disk drives for an integrated Windows server" on page 189).

New version of Windows Server

To upgrade your servers from Windows NT 4.0 to Windows 2000, see Upgrade your server from Windows NT 4.0 to Windows 2000 Server in the V5R3 iSeries Information Center.

Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware

IPCS or INS servers (type 2850 and 6617) must be reinstalled on newer hardware or migrated to 2890 IXS hardware before installing V5R4. See the Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware topic in the V5R3 iSeries information center.

Migrate to iSCSI attached servers

Migrating to an iSCSI attached server is not supported. All iSCSI attached servers require new installations.

Windows Cluster Service

Windows cluster service links individual servers so they can perform common tasks. Should any one server stop functioning, a process called failover automatically shifts its workload to another server to provide continuous service. In addition to failover, some forms of clustering also employ load balancing, which enables the computational workload to be distributed across a network of linked computers.

Windows 2000 Advanced Server supports a two-node cluster while Windows Server 2003 Enterprise Edition supports eight-node clusters. Datacenter versions of Windows are not supported.

Windows Cluster Service support is supported for integrated Windows servers running either Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition.

Notes:

1. Windows clustered network server nodes must reside within a single iSeries partition in order to be clustered.
2. iSCSI attached xSeries cannot be clustered with IXS/IXA attached servers.

Although the traditional Windows clustered server solution requires a shared physical SCSI or Fibre Channel device, the integrated Windows server solution uses a virtual Fibre Channel bus to share the virtual disk devices between the nodes of a cluster.

In addition, the new support for virtual Ethernet enables high-performance, secure communication for the internal node-to-node communication between clustered nodes.

Detailed checklists for planning and creating a server cluster are available in the online Microsoft help for Server clusters and should be referred to prior to installing and configuring a Windows Cluster server. Additional information, including step-by-step guides to installing Cluster service, is available on the Microsoft Web site .

For more information about support for Windows Cluster service, see the following topics:

"Install Windows Cluster service"
Find out how to install and configure Windows Cluster service on an integrated Windows server.

"Install Windows Cluster service on an existing server" on page 100
Find out how to create clusters on an existing integrated Windows server.

Cluster support on an iSCSI attached server

For information about iSeries support for Microsoft Cluster Service (MSCS) on an iSCSI attached server see MSCS on an iSCSI attached server on the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/windows/iscsiclusters.html).

Install Windows Cluster service

Before installing the Cluster service, read all Microsoft checklists for installing server clusters to help you avoid future problems in planning and installation.

Note: During installation of Cluster service on the first node, vary off all other nodes participating in the cluster before you start Windows.

In the Server clusters information, any references to a shared SCSI or Fibre Channel device refers to the virtual Fibre Channel implementation used to access the shared network server storage spaces.

To install and run Windows Cluster service, complete the following tasks:

1. Install Windows Cluster service on the Integrated xSeries server
   - "Install Windows Cluster service on a new integrated Windows server"
   - "Install Windows Cluster service on an existing server" on page 100
2. "Install Windows Cluster service on Windows" on page 102

Install Windows Cluster service on a new integrated Windows server

The easiest way to install and configure the Windows Cluster server is to do so when you first configure an integrated server. Use the Install Windows server (INSWNTSVR) command with the following parameters that specify the cluster configuration information:

- Cluster name (CLU) parameter
- Cluster configuration (CLUCFG) parameter

For more information about installing the integrated server, see "Install Windows 2000 Server or Windows Server 2003" on page 89.

After you run the INSWNTSVR command (and the integrated Windows server install completes) and before you install the Windows Clustering service on the Windows side, you must perform additional configuration steps on the integrated server console. For more information, see "Prepare Windows before installing Windows Cluster service" on page 101.

Cluster name:

The Cluster name (CLU) parameter provides the name that the cluster will be known by. This is used by administrators to connect to the cluster and represents the group of independent network server nodes which will work together as a single system. The name entered for the cluster name is also used as the name of the network server storage space that is created and will serve as the quorum resource for the cluster.

Cluster configuration:

The Cluster configuration parameter (CLUCFG) is used to define the cluster and configure the quorum resource network server storage space. Additionally, this information is used to validate that any secondary nodes have the correct i5/OS configuration necessary to create the virtual cluster connections for the shared storage devices and the virtual Ethernet port that will be used for the private clustering interconnect. The cluster configuration value of *CLU will retrieve the cluster configuration from the existing quorum resource network server storage space specified on the CLU parameter,

Note: The clustering connection port requires configuration of a matching virtual Ethernet port. For more information about configuring a virtual Ethernet port, see “Configure virtual Ethernet networks” on page 111.

Install Windows Cluster service on an existing server

You can install Windows Cluster service on an existing Windows 2000 Advanced Server or a Windows Server 2003 Enterprise Edition server.

Ensure that the server’s Integrated Server Support level is synchronized with i5/OS. See “Upgrade the integrated server side of IBM i5/OS Integrated Server Support” on page 97. This ensures the availability of all server functions required to install the Windows Cluster service.

To install Windows Cluster service on an existing server, perform the following tasks:

- Create a storage space (quorum resource)
- Configure the virtual Ethernet connection port
- Link the quorum resource drive to the network server description

After you complete the steps above and before you install the Windows Clustering service on the integrated Windows server side, you must perform some additional configuration steps on the integrated Windows server console. For more information, see “Prepare Windows before installing Windows Cluster service” on page 101.

Create a storage space (quorum resource):

The first step is to create a storage space to use as the quorum resource. To create a storage space, use the Create NWS Storage space (CRTNWSSTG) CL command and specify the special format *NTFSQR.

The name of the network server storage space should match the name of the cluster you are creating. The recommended size is 550 MB or larger. The command prompts for the following cluster information, which you need to provide:

- Cluster domain name
- Virtual Ethernet connection port
- IP Address for the Windows cluster
- Subnet mask for the Windows cluster

Configure the virtual Ethernet connection port:

The next step is to configure the virtual Ethernet connection port that you want to use for the private cluster communication. See “Configure virtual Ethernet networks” on page 111. The virtual Ethernet port that you use must match the connection port you specify with the quorum resource network server storage space.

Link the quorum resource drive to the network server description:

Link the quorum resource storage space to the network server by using the Add Server Storage Link (ADDNWSSTGL) command, using ACCESS(*SHRUPD), DYNAMIC(*YES) and DRVSEQNBR(*QR).

Note: During installation of Cluster service on the first node, all other nodes must be varied off before starting the integrated server. Additional shared storage devices can be created and linked at this time. All shared storage spaces must be *NTFS and linked with ACCESS(*SHRUPD).

Prepare Windows before installing Windows Cluster service

After you install the integrated server, you need to prepare the server to install the Windows Cluster service.

To prepare Windows before you install the Windows Cluster service, perform the following tasks:

1. Format the quorum resource
2. Configure the private network adapter

When you complete these steps, Windows is ready for you to install the Windows Cluster service. For more information, see “Install Windows Cluster service on Windows” on page 102.

Format the quorum resource:

The first step to prepare Windows for a Windows Cluster installation is to format the quorum resource as NTFS. Formatting the quorum resource is not only required to install the Windows Cluster service, it is also the first step when installing the first node of a cluster. For more information, see “Format integrated server disk drives” on page 166.

For IXS or IXA attached servers, the quorum resource appears as an unformatted disk drive that typically has a logical device driver letter of E. The location of the quorum resource is bus number 1, target identifier 0 and Logical Unit Number (LUN) 0.

You should format the volume and label it using the same name as the cluster, which is also the name of the quorum resource network server storage space name. Also format any other shared storage spaces at this time. It is also recommended that you assign a fixed drive letter to the quorum resource drive and any other shared storage drives.

Note: The drive letter assigned to all storage spaces on the shared storage bus must be the same on all nodes of the cluster.

Configure the private network adapter:

Next, configure the private network adapter for use by the Windows Cluster service by completing the following steps on the first node in your cluster:

1. On the integrated Windows server console, right-click **My Network Places** and select **Properties**.
2. Right-click the **Local Area Connection 2** icon.

   Note: Which network adapter is private and which is public depends on how you configured the server. This information assumes the following:

   - The first network adapter (Local Area Connection) is connected to the public network by using a physical LAN adapter under the Integrated Windows server

- The second network adapter (Local Area Connection 2) is the virtual Ethernet adapter configured as the cluster configuration connection port that you want to use as the private cluster network
- The third network adapter (Local Area Connection 3) is the virtual Ethernet point to point connection to i5/OS and should not be enabled for any clustering use

The number and order of network adapters may not be the same, depending on the physical and virtual configuration of the server and the network.

3. Click **Status** to display the **Local Area Connection 2 Status** window, which shows the connection status, as well as the speed of connection.
4. In the **Local Area Connection 2 Status** window, click **Properties**.
5. In the **Properties** dialog box, make sure that the contents of the **Connect using** field contains `IBM iSeries Virtual Ethernet x`, where `x` matches the *VRTETHx that you specified for the cluster configuration connection port.
6. Click **Close**, then click **Close** again.

For clarity, you should rename your Local Area Network Icons. For example, you might want to change the name of Local Area Connection 2 to something like Private Cluster Connection.

Install Windows Cluster service on Windows

The actual installation of the Windows Cluster service depends on the version of Windows installed during the Windows environment for iSeries installation. For the most part, refer to the Microsoft documentation for instructions on installing the Windows Cluster service. This information highlights specific steps required to install the Windows Cluster service on an Integrated Windows server.

- "Install Windows Cluster service on Windows 2000 Server"
- "Install Windows Cluster service on Windows Server 2003" on page 103

Note: Make sure that Windows Cluster service is installed and running on one server before starting Windows on another server in the cluster. Starting the operating system on multiple servers before the Windows Cluster service is running on one server can damage the cluster storage. After you configure the first server, you can simultaneously install the remaining servers.

Install Windows Cluster service on Windows 2000 Server: Use the Cluster Service Configuration wizard to install the Windows Cluster service. You supply the wizard with all the initial cluster configuration information.

To install Windows Cluster service, perform the following tasks:

1. Start the Cluster Service Configuration wizard
2. Use the wizard to configure the cluster service

Start the Cluster Service Configuration wizard:

To start the Cluster Service Configuration wizard, complete the following steps:

1. From the Windows **Start** menu, click **Settings**, then click **Control Panel**.
2. In the **Control Panel** window, double-click **Add/Remove Programs.**
3. In the **Add/Remove Programs** window, click **Add/Remove Windows Components**.
4. In the **Windows Components Wizard** dialog box, select **Cluster Service**, then click **Next**.

Configure the Windows Cluster service:

After you have started the Cluster Service Configuration wizard, it prompts you through the installation of the Windows Cluster service. You supply the wizard with all the initial cluster configuration information, which is required in order to create the cluster.

When prompted for the quorum resource, select the drive that you formatted and labeled. Although this drive is typically the E: drive for a new installation, the Disk Manager may have fixed another letter to the drive.

Network connections require special consideration:

Note: The order in which the Cluster Service Configuration wizard presents the network configuration information may vary.

- Uncheck the box **Enable this network for cluster use** for the `IBM iSeries virtual Ethernet Point to point` (typically Local Area Connection 3)
- Select the option **Internal cluster communications only** for the `IBM iSeries virtual Ethernet x`where `x` matches the `*VRTETHx` specified on the cluster configuration connection port (typically Local Area Connection 2)
- Configure the remaining network connections according to their need

Specify the `IBM iSeries virtual Ethernet x` adapter (typically Local Area Connection 2) as the primary network for the Internal Cluster Communication.

Install Windows Cluster service on Windows Server 2003: Use the Cluster Administrator to install Windows Cluster service on Windows Server 2003 and to join an existing cluster. Both installing the cluster service and joining an existing cluster require you to open the Cluster Administrator. Open the **Cluster Administrator** from the Windows **Start** menu by selecting **All Programs**, then **Administrative Tools**, then **Cluster Administrator**.

Install and configure the Windows Cluster service by completing the following steps.

1. Open the **Cluster Administrator**.
2. In the **Open Connection to Cluster** dialog box that appears, in **Action**, select **Create new cluster**.
3. Click **OK** to display the New Server Cluster wizard, which prompts you through the installation of the Cluster service for the first node.
4. Click **Next**.
5. Type the **Domain** (defaulted) and **Cluster name**.
6. Type the **Computer name** (defaulted).
7. Type the **IP Address** for the cluster management
8. Type the **Cluster Service Account User name**, **Password** and **Domain**.
9. Verify the **Proposed Cluster Configuration**.

Join an existing cluster:

Join an existing cluster by completing the following steps:

1. Open the **Cluster Administrator**.
2. In the **Open Connection to Cluster** dialog box, in **Action**, select **Add nodes to cluster**.
3. Then in **Cluster or server name**, either type the name of an existing cluster, select a name from the list, or click **Browse** to search for an available cluster.
4. Click **OK** to display the Add Server Cluster wizard.
5. Select one or more computer names to add to the cluster, the click **Add**.
6. Enter the domain account password for the cluster service.
7. After Cluster service has finished installing, use the Cluster Administrator to locate and select the cluster that you just created.
8. Expand **Cluster Configuration**, **Network Interfaces**. This will open in the right panel with a list of all **Local Area Connections**.

9. Type the network name (Local Area Connection x) for the virtual `IBM iSeries virtual Ethernet x`where x matches the `*VRTETHx` specified on the Cluster configuration connection port. You need to identify this network later, so remember the name.
10. Identify the network name (Local Area Connection x) for the virtual `IBM iSeries virtual Ethernet point to point`. You need to identify this network later, so remember the name.
11. In the **Cluster Administrator** window, expand **Cluster Configuration**, **Networks**.
12. Right-click the network name (Local Area Connection x) for the virtual `IBM iSeries virtual Ethernet x`and select **Properties**.
13. Select the option **Internal cluster communications only** for this network.
14. Right-click the network name (Local Area Connection x) for the virtual `IBM iSeries virtual Ethernet point to point`and select **Properties**.
15. Uncheck the box **Enable this network for cluster use** for this network.

Configure the remaining network connections according to their need.

Enabling Kerberos with a Windows Server 2003 Active Directory Server

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. Additional information, including information about installing the service pack or the hot fix, is available 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.

Install the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server

The 2892-002 and 4812-001 Integrated xSeries Server include an ATI Radeon 7000M video chip. The required drivers are not included in the Microsoft Windows 2000 Server distribution CD. You will need to install the ATI video display driver on the integrated Windows server to take full advantage of the ATI video chip's capabilities.

Your system must have DirectX 8.1, or later, installed before you can install the ATI video drivers.

To install the ATI video driver for Windows 2000, follow these steps:

1. Install DirectX version 8.1 or later. Windows 2000 ships with DirectX 7.0 but DirectX version 8.1 or later is required for the ATI video drivers and must be installed before installing the ATI video drivers. Microsoft maintains a website for DirectX information and downloads. Visit `http://www.microsoft.com/directx`.
2. Install the ATI video driver:
   a. Close all programs.
   b. Click the **Start** button and select the **Run** menu item.
   c. Click the **Browse** button.
   d. Browse to the `%SystemDrive%\WSV` directory where `atidrvr.exe` is located.
   e. Select `atidrvr.exe` and click OK to run the program.
   f. Follow the installation instructions on the screen.
3. Optionally, the Advanced ATI Control Panel tabs can be installed.
   a. Close all programs.
   b. Click the **Start** button and select the **Run** menu item.
   c. Click the **Browse** button.
   d. Browse to the `%SystemDrive%\WSV` directory where `aticp.exe` is located.
   e. Select `aticp.exe` and click OK to run the program.
   f. Follow the installation instructions on the screen.

Adjust hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server

If you are installing Windows Server 2003 on a 2892-002 or 4812-001 IXS, some additional setup is required for optimal video performance. To adjust performance, do the following steps:

1. From the Windows **Start** menu, click **Settings -> Control Panel -> Display**.
2. On the **Display Properties** panel, click the **Settings** tab.
3. Click **Advanced**.
4. Click the **Troubleshoot** tab.
5. Adjust the **Hardware Acceleration** slider as wanted
6. Click **Apply**.
7. Click **OK**.
8. Click **OK** again to accept the change.

Respond to error messages during installation

The integrated Windows server phase of the installation flags missing information that you did not provide during the i5/OS phase of the installation, then allows you to supply the information. This section contains some examples of those error messages and how to respond.

Error (Installing Server)

You may not have specified a value in the `To workgroup` or `To domain` fields of the `Install Windows Server` display on i5/OS. If not, then you will see the following error message:

```
Error (Installing Server)

A setup parameter specified by your system administrator or
computer manufacturer is missing or invalid.  Setup must therefore
ask you to provide this information now.

Once you have furnished the required information, unattended Setup
operation will continue.
```

```
You may wish to inform your system administrator or computer
manufacturer that the "JoinWorkgroup" value is missing or invalid.
```

Click **OK**.

The installation program then prompts you to make the computer a member of a workgroup or domain.

Set an integrated Windows server to automatically vary on with TCP/IP

You can set an integrated server to automatically vary on when you start TCP/IP. 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: Beginning in V5R1, 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.

   Note: 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.

Code fixes

IBM iSeries Integrated Server Support code fixes provide the most current and error-free code possible without requiring you to wait for the next software release. They update the iSeries Integrated Server Support code that enables Microsoft Windows server to run on the integrated server and are separate from the service packs for Windows itself, which you must get from Microsoft.

Read about the "Types of code fixes" on page 107.

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 dependant on the level of code on the i5/OS side.

When you use the integration software to synchronize an integrated server, there are potentially four actions which you may cause to occur 'under the covers'.

1. If i5/OS has been upgraded to a new release, for example, from V5R3 to V5R4, the software for the new release will replace that of the old release.

2. If a new IBM iSeries Integrated Server Support service pack has been installed on i5/OS, it will be copied over to the integrated server.
3. If an IBM iSeries 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.

There are three ways to perform a synchronization

- "Synchronize the integration software level using the integrated Windows server console."
- "Synchronize the integration software level using iSeries Navigator" on page 108.
- "Synchronize the integration software level using a remote command" on page 108.

If you have problems performing a synchronization, see "IBM iSeries Integrated Server Support snap-in program" on page 219.

Types of code fixes

There are four types of code fixes

1. Code fixes applied to the i5/OS integration code, referred to as **regular program temporary fixes (PTFs)**.
   - To apply them all you have to do is install them to i5/OS.
   - These code fixes are available from IBM Support or from the internet at http://www.ibm.com/servers/eserver/iseries/integratedxseries (take the Service & support link on the left navigation bar) .
2. Code fixes which are copied to the integrated server's drives and run on the integrated server, referred to as **service pack PTFs**.
   - The IBM iSeries Integrated Server Support licensed program has an integrated server part which is copied over from the i5/OS side. When you apply an i5/OS Cumulative PTF package, it may contain an Integrated Server Support service pack which can be applied to the integrated server. You do this by synchronizing the integrated server.
   - These code fixes are also available from IBM Support or online at http://www.ibm.com/servers/eserver/iseries/integratedxseries/ (take the Service & support link on the left navigation bar) .
3. Code fixes applied to Microsoft Windows server itself, referred to as **service packs**.
   - These come from Microsoft. You can download them from their Windows Update web site.
   - Do not apply any code fixes from Microsoft which might change portions of Windows server used by IBM iSeries Integrated Server Support. For example, do not download any SCSI storage device drivers or LAN device drivers from Windows Update.
   - Other areas are generally safe, for example, USB device drivers may be downloaded from Windows Update at your own risk.
4. Hotfixes applied to Microsoft Windows server itself and applied using Windows Update.

Synchronize the integration software level using the integrated Windows server console

To use the iSeries Integrated Server Support snap-in to synchronize the software level, you must be a Windows system administrator. 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.

Synchronize the integration software level using iSeries Navigator

| 1. In iSeries 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.

To find out which levels of software are installed on i5/OS and the integrated server follow this procedure:

| 1. In iSeries 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.

Synchronize the integration software level using a remote command

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 "Run integrated Windows server commands remotely" on page 153.

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

Error Code	Error
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.

Chapter 6. Manage virtual Ethernet and external networks

This section contains procedures to help you create and understand virtual Ethernet and external networks described in "Networking concepts" on page 28.

- "Configure IP address, gateway and MTU values"
- "Configure virtual Ethernet networks"
- "Configure inter-partition virtual Ethernet networks" on page 112
- "Explore point to point virtual Ethernet networks" on page 113
- "External networks" on page 114
- "Remove network adapters" on page 115

Configure IP address, gateway and MTU values

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. See "Point to point virtual Ethernet IP address conflicts" on page 233.
- 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. See "Change remote system configuration properties" on page 122.
- 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.

Configure virtual Ethernet networks

This section will describe how to configure a virtual Ethernet network between integrated servers. (Note that if you are installing an integrated server from scratch, the installation command (INSWNTSVR) can configure virtual Ethernet networks for you.) For information about how to extend virtual Ethernet networks to other iSeries logical partitions, see "Configure inter-partition virtual Ethernet networks" on page 112. The procedure consists of the following basic steps

1. Configure a virtual Ethernet port and line description for the integrated server. Using iSeries Navigator:
   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.

Note: On iSCSI attached servers, use an IP address that is on a different subnet than the IP addresses in the network server host adapter and remote system configuration.

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 the procedure for all the integrated servers you want to connect to the network, specifying the same virtual Ethernet port for each one.
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.

Configure inter-partition virtual Ethernet networks

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 networks are configured differently on iSeries systems with the Hardware Management Console (HMC) than on other systems. In an iSeries HMC system, 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 with an eServer i5 and Configure Inter-partition virtual Ethernet networks 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 as described in step 1 on page 111 of the “Configure virtual Ethernet networks” on page 111 article if one has not already been created for the port of interest (0 through 9). Select an associated port name (Cmnxx) for the appropriate 268C resource.
3. Continue with step 2 of the “Configure virtual Ethernet networks” on page 111 article (in all i5/OS partitions that control a participating integrated server), and step 3 of “Configure virtual Ethernet networks” on page 111.

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 by pinging between connected integrated servers and partitions.

Inter-partition networks without the Hardware Management Console

In a system other than an iSeries HMC system, inter-partition connections exist between partitions using the same network number, and integrated servers are connected only if their controlling i5/OS partitions are connected. Network numbers 0-9 are pertinent to integrated servers. For example, if an i5/OS partition is configured for inter-partition communication on networks 1 and 5, then integrated servers controlled by that partition can participate in inter-partition communication on virtual Ethernet ports 1 and 5. The configuration procedure consists of the following steps:

1. Configure the network number that you want each partition to connect to. Refer to Logical Partition concepts and iSeries Navigator online help information. Keep in mind that integrated servers are connected only if their controlling i5/OS partitions are connected.
2. Configure a virtual Ethernet port and line description as described if one has not already been created for the port you want to use (0 through 9). See Step 1 of “Configure virtual Ethernet networks” on page 111. Leave the associated port name set to **None**.
3. Continue with step 2 in “Configure virtual Ethernet networks” on page 111 (in all i5/OS partitions that control a participating integrated server), and step 3 in “Configure virtual Ethernet networks” on page 111.
4. If you want a partition to fully participate, you will need to appropriately configure the protocol(s) within the partition. In each i5/OS partition that you want to participate, use the WRKHDWRSC *CMN command to find the name of the appropriate port of hardware type 268C, which was automatically created. See Step 1 in “Configure virtual Ethernet networks” on page 111. Then create an Ethernet line description on the 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 by pinging between connected integrated servers and partitions.

Explore point to point virtual Ethernet networks

Each integrated server has a point to point virtual Ethernet network connection with the iSeries, which allows the iSeries to control the integrated server. Here you can learn how to view or change these connections, although they are automatically configured during installation.

View point to point 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.

View point to point Ethernet connections from the integrated Windows server console

1. At the console of your integrated server, click **Start —> Settings —> Control Panel**. Then select **Network and Dial-up Connections**.
2. One of the icons will be named **virtual Ethernet point to point**. Double-click it.
3. Click **Properties** in the dialog box which appears.
4. Double-click **Internet Protocol (TCP/IP)** in the next dialog box.
5. 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's IP address augmented by one so as to be even instead of odd.
6. 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.
7. At the C:\> command prompt which appears, enter the command ping followed by the i5/OS IP address which you remember from the last step. For example `ping 192.168.3.1`. The command should return `Reply from ....`. That's good. The ping command sends a packet of data to a certain internet address and times how long it takes to make a round trip.
8. (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, `ping '192.168.3.2'`. Congratulations! If all went correctly we have proved that you have a properly functioning point to point virtual Ethernet network.

External networks

You can install a new network adapter card in an open PCI slot. If you do this, you need to configure the new adapter on the integrated Windows server.

Refer to the Install iSeries Features topic for information about installing a new network adapter card. Choose your model of iSeries and find the instructions labeled **Install PCI Card and Integrated xSeries Adapter Card**.

To set up a new network adapter, see "Install network adapter device drivers and add adapter address information to an integrated Windows server" on page 115.

To create a virtual Ethernet connection, see "Configure virtual Ethernet networks" on page 111.

To remove a network adapter, see "Remove network adapters" on page 115.

Install network adapter device drivers and add adapter address information to an integrated Windows server

Here you can install adapter device drivers and add adapter address information for the new adapters on an integrated Windows server.

The adapters and device drivers under Windows 2000 Server and Windows Server 2003 support Plug-n-Play. Once an adapter has been physically installed, reboot the integrated server by varying it on for the adapters to become available. Remember to configure the IP address for every adapter (connection).

If you are upgrading your Integrated xSeries Server from Windows NT 4.0 to Windows 2000 Server, remove the old adapter before adding the new one. See “Remove network adapters.”

Windows 2000 Server or Windows Server 2003 recognizes the new adapter. To configure the IP address for a given adapter:

1. Right-click **My Network Places**; then click **Properties** from the pull-down menu.
2. Double-click the correct adapter (Local Area Connection) to configure the IP address.
3. Click the **Properties** button.
4. Select the **Internet Protocol (TCP/IP)**, then click the **Properties** button.
5. If it is not already selected, click the **Use the following IP address** radio button.
6. In the **IP Address** field, specify the IP address.
7. In the **Subnet Mask** field, specify the subnet mask.
8. In the **Default Gateway** field, specify the default gateway address.
9. Click **OK, OK, and Close** to complete the IP address setting.

   Note: If Windows indicates that the IP address is already configured for another adapter, but you cannot find an adapter already using the address, Windows is probably aware of a previous hardware environment that used the address. To display a LAN adapter from a previous hardware environment so that you can free the IP address, see the Microsoft Knowledge Base article Q241257 Device Manager Does Not Display Devices Not Currently Present in Windows 2000 .

Remove network adapters

Before you remove a network adapter card from an integrated Windows server, you need to uninstall it from within Windows.

To uninstall network adapters from an integrated server, follow these steps.

1. Click **Start**, then **Settings**, then **Control Panel**.
2. Start the **Add/Remove Hardware** wizard and click **Next** on the opening panel.
3. Click on **Uninstall/unplug a device**.
4. On the **Choose a remove task** panel, click **Next** to take the default (Uninstall a device).
5. Select the device from the list that you want to uninstall (for example, IBM PCI Token-ring adapter).
6. Click **Yes** to confirm that you want to remove the adapter.
7. Because Windows 2000 Server and Windows Server 2003 are Plug and Play operating systems, you must either physically remove the adapter from i5/OS or disable it before restarting the server. If you restart the integrated server with the adapter still plugged in, the operating system will detect it as new hardware and reinstall the device driver. If you want to disable the adapter rather than remove it, follow these steps:
   a. From the **Control Panel**, select **Network and Dial-up Connections**.

    b. Select the LAN adapter.
    c. Right-click and select **Disable**.

8. Restart the server to complete the procedure.

Chapter 7. Administer connections to iSCSI attached servers

The following sections will guide you through some tasks performed on iSCSI HBA integrated servers.

- "Work with iSCSI configuration objects"
- "Configure security between i5/OS and hosted systems" on page 128
- "Manage iSCSI host bus adapters" on page 132
- "Remote server discovery and management" on page 142

Work with iSCSI configuration objects

i5/OS objects are used to configure and manage the iSCSI HBA for iSeries, the remote xSeries or IBM BladeCenter system, the remote system's service processor and the security attributes of the iSCSI network. See the following sections for details.

- "Manage network server host adapters"
- "Manage remote system network server configurations" on page 120
- "Manage service processor network server configurations" on page 123
- "Manage connection security network server configurations" on page 125

Manage network server host adapters

Network server host adapter (NWSH) objects are used to configure the iSeries target iSCSI host bus adapter (iSCSI HBA). 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 43.

The following tasks can be performed on NWSH objects:

- "Create a network server host adapter object"
- "Create a network server host adapter object based on another one" on page 118
- "Display network server host adapter properties" on page 118
- "Change network server host adapter properties" on page 119
- "Start a network server host adapter" on page 119
- "Stop a network server host adapter" on page 119
- "Delete a network server host adapter" on page 120

Create a network server host adapter object

A network server host adapter (NWSH) object must be created for each iSeries target iSCSI host bus adapter (iSCSI HBA).

Note: If you are using the iSCSI Network Planning Guide, you should use the network planning worksheets to help you do the following task.

To create a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Right-click **Local Host Adapters**.
4. Select **New Network Server Host Adapter**.

5. On the **General** tab:
   - Enter the NWSH device **Name** and **Description**.
   - Select the **Hardware resource**. For information on determining the hardware resource for your iSCSI HBA, see "Prepare for the operating system install" on the iSCSI install read me first web page.
   - Select the **Object authority**. You can use the default value **Change**.
6. On the **Local Interfaces** tab, enter information to define the SCSI and LAN interface attributes for the iSCSI HBA.
7. 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 CRTDEVNWSH or WRKDEVD.

Create a network server host adapter object based on another one

You can copy an existing network server host adapter (NWSH) object when creating a new one. 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 iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local 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.

Display network server host adapter properties

A network server host adapter (NWSH) object contains configuration information for an iSeries target iSCSI host bus adapter (iSCSI HBA).

To display the attributes of a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.

4. Right-click a local 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.

Change network server host adapter properties

A network server host adapter (NWSH) object contains configuration information for an iSeries target iSCSI host bus adapter (iSCSI HBA).

To change the attributes of a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.
4. Right-click a local 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.

Start a network server host adapter

In order for an integrated server to use an iSeries target iSCSI host bus adapter (iSCSI HBA) for storage or virtual Ethernet data flows, the corresponding network server host adapter (NWSH) object must be started (varied on). Make sure that you have cabled the iSeries target iSCSI host bus adapter to the iSCSI network. See the iSCSI Host Bus Adapter for IBM xSeries and BladeCenter iSCSI HBA topic in the IBM Systems Hardware Information Center.

To start a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.
4. Right-click a local 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 Chapter 14, “Troubleshoot integrated Windows servers,” on page 205 or the iSCSI troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html) web page.

Stop a network server host adapter

Stopping (varying off) a network server host adapter (NWSH) object will make the corresponding iSeries 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 “Start and stop an integrated Windows server using iSeries Navigator” on page 149 for more information.

To stop a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.
4. Right-click a local 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.

Delete a network server host adapter

To delete a network server host adapter using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **iSCSI Connections**.
3. Select **Local Host Adapters**.
4. Right-click a local 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.

Manage remote system network server configurations

Remote system network server configuration (NWSCFG subtype RMTSYS) objects are used to configure attributes of an iSCSI attached remote xSeries or IBM BladeCenter blade server. The remote system configuration is used to identify the specific xSeries or IBM BladeCenter hardware that the integrated server will run on. It also defines how the remote system boots and communicates with the iSeries system. For more information, see “Remote system configuration” on page 43.

The following tasks can be performed on remote system configuration objects:

- “Create a remote system configuration object”
- “Create a remote system configuration object based on another one” on page 121
- “Display remote system configuration properties” on page 121
- “Change remote system configuration properties” on page 122
- “Display remote system status” on page 122
- “Delete a remote system configuration object” on page 122

Create a remote system configuration object

A remote system network server configuration (NWSCFG subtype RMTSYS) object must be created for each xSeries or IBM BladeCenter server 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 network planning worksheets to help you do the following task.

To create a remote system configuration using iSeries 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 **Network 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.

Create a remote system configuration object based on another one

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 iSeries 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.

Display remote system configuration properties

A remote system network server configuration (NWSCFG subtype RMTSYS) object contains configuration information for an IBM xSeries or BladeCenter server that will be used to run an iSCSI attached integrated server.

To display the attributes of a remote system configuration using iSeries 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.

Change remote system configuration properties

A remote system network server configuration (NWSCFG subtype RMTSYS) object contains configuration information for an xSeries or IBM BladeCenter server that will be used to run an iSCSI attached integrated server.

To change the attributes of a remote system configuration using iSeries 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.

Display remote system status

You can display the xSeries or IBM BladeCenter server hardware status. For example, this may help you determine if it is available for use by an iSCSI attached integrated server.

To display the status of a remote system using iSeries 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 **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.

Delete a remote system configuration object

To delete a remote system configuration using iSeries 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 **Delete**.
6. Click **Delete** on the confirmation panel.

If you want to use CL commands, see DLTNWSCFG or WRKNWSCFG.

Manage service processor network server configurations

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 xSeries or IBM BladeCenter server. 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.

The following tasks can be performed on service processor configuration objects:

- “Create a service processor configuration object”
- “Create a service processor configuration object based on another one”
- “Display service processor configuration properties” on page 124
- “Change service processor configuration properties” on page 124
- “Initialize a service processor” on page 124
- “Delete a service processor configuration object” on page 125

Create 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 xSeries or IBM BladeCenter 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 iSeries 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.

Create 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 iSeries 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.

Display 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 xSeries or IBM BladeCenter server that is used to run an iSCSI attached integrated server.

To change the attributes of a service processor configuration using iSeries 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.

Change 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 IBM xSeries or BladeCenter that is used to run an iSCSI attached integrated server.

To change the attributes of a service processor configuration using iSeries 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.

Initialize a service processor

A service processor network server configuration (NWSCFG subtype SRVPRC) object contains configuration information for a service processor or Management Module of an xSeries or IBM BladeCenter 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 may also want to regenerate or synchronize the user, password, and certificate 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 iSeries 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:
   - **Initialize a new service processor**
   - **Regenerate service processor certificate**
   - **Synchronize certificate from 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.

Delete a service processor configuration object

To delete a service processor configuration using iSeries 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.

Manage connection security network server configurations

Connection security network server configuration (NWSCFG subtype CNNSEC) objects are used to define the IP security (IPSec) rules that are used to secure the storage and virtual Ethernet data flows over the iSCSI network between the iSeries and xSeries or IBM BladeCenter blade servers. For more information, see “Connection security configuration” on page 47.

Note: If the iSCSI HBA hardware on either the iSeries or xSeries/Center side of the iSCSI connection does not support IPSec, then IPSec cannot be used to secure the data flows over the iSCSI network. If the iSCSI HBA hardware does not support IPSec, then a connection security object still needs to be created, but no IP security rules should be defined.

The following tasks can be performed on connection security configuration objects:

- “Create a connection security configuration object” on page 126
- “Create a connection security configuration object based on another one” on page 126
- “Display connection security configuration properties” on page 127
- “Change connection security configuration properties” on page 127
- “Delete a connection security object” on page 127

Create a connection security configuration object

A connection security network server configuration (NWSCFG subtype CNNSEC) object must be created to define the IP security (IPSec) rules that are used to secure the storage and virtual Ethernet data flows over the iSCSI network between the iSeries and xSeries or IBM BladeCenter blade servers.

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. If the iSCSI HBA hardware on either the iSeries or xSeries or IBM BladeCenter side of the iSCSI connection does not support IPSec, then IPSec cannot be used to secure the data flows over the iSCSI network. If the iSCSI HBA hardware does not support IPSec, then a connection security object still needs to be created, but do not define any IP security rules.

To create a connection security configuration using iSeries 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. On the **IP Security Rules** tab:
   - If your iSCSI HBA hardware supports IPSec, define the IP security rules that will be used to secure the storage and virtual Ethernet data flows over the iSCSI network.
   - Otherwise, do not define any IP security rules.
7. Click **OK**.

If you want to use CL commands, see CRTNWSCFG or WRKNWSCFG.

Create 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 iSeries 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.

Display connection security configuration properties

A connection security network server configuration (NWSCFG subtype CNNSEC) object contains IP security (IPSec) rules that are used to secure the storage and virtual Ethernet data flows over the iSCSI network between the iSeries and xSeries or IBM BladeCenter blade servers.

To display the attributes of a connection security configuration using iSeries Navigator, follow these steps:

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.

Change connection security configuration properties

A connection security network server configuration (NWSCFG subtype CNNSEC) object contains IP security (IPSec) rules that are used to secure the storage and virtual Ethernet data flows over the iSCSI network between the iSeries and xSeries or IBM BladeCenter blade servers.

Note: If the iSCSI HBA hardware on either the iSeries or xSeries/IBM BladeCenter side of the iSCSI connection does not support IPSec, then IPSec cannot be used to secure the data flows over the iSCSI network. If the iSCSI HBA hardware does not support IPSec, then do not define any IP security rules.

To change the attributes of a connection security configuration using iSeries Navigator, follow these steps:

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.

Delete a connection security object

To delete a connection security configuration using iSeries Navigator, follow these steps:

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.

Configure security between i5/OS and hosted systems

See "Security for iSCSI attached systems" on page 49 to determine which of the following security actions are appropriate for your environment:

- "Configure CHAP"
- "Configure IPSec"
- "Configure service processor SSL" on page 130
- "Service processor password" on page 131
- "Configure a firewall" on page 131

Configure CHAP

Note: You must have security administrator (*SECADM) special authority to create, change, or display CHAP information.

To configure CHAP, or to change CHAP credentials, do the following steps:

1. With the server shut down (NWSD varied off), use the procedure described in "Change remote system configuration properties" on page 122 to change the properties of the remote system configuration for the server. Go to the **CHAP Authentication** tab.
   - To enable CHAP, select the **Use the following values for CHAP authentication** option and specify a **CHAP name** and select the **Generate CHAP secret once** option.
   - To disable CHAP, select the **Do not use CHAP** option.
2. Use the procedure described in "Display remote system configuration properties" on page 121 to display the properties of the remote system configuration for the server.
   - On the **CHAP Authentication tab**, note the **CHAP name** and **CHAP secret**.
   - On the **Boot Parameters** tab, note the boot parameter delivery method.
3. This step is required if the boot parameter delivery method is **Manually configured on remote system** or **Dynamically delivered to remote system via CHAP**. Upon the next server start (NWSD vary on), watch the hosted system's console for a prompt to press CTRL-Q. Immediately on seeing the prompt, press `CTRL-Q`. In the CTRL-Q utility, select the adapter that is configured to boot the hosted OS. Enter the CHAP name and secret from the remote system configuration properties into the CHAP name and secret fields of the CTRL-Q target security configuration panel. Do not enter this information into the CTRL-Q initiator configuration panel.

   Note: Any non-boot iSCSI HBAs in the hosted system are automatically configured from the i5/OS configuration.

Configure IPSec

Note: An iSCSI HBA for iSeries with IPSec support is required in order to use IPSec to secure the data flows over the iSCSI network. If the iSCSI HBA hardware does not support IPSec, then a connection security object still needs to be created but you should not define any IP security rules.

To configure IPSec, or to change IPSec credentials, do the following steps:

1. This step is required if you haven't already generated the first pre-shared key. You can also perform this step at any time to change the pre-shared key: With the server shut down (NWSD varied off), use the procedure described in "Change connection security configuration properties" on page 127 to change the properties of the connection security configuration for the server.
   - Go to the **IP Security Rules** tab.
   - Click the **Add** button and select the **Generate pre-shared key once** option.

- Click **OK** to add the new IP security rule to the table and click **OK** again to save the connection security configuration and cause the pre-shared key to be generated.

  Note: You must have security administrator (*SECADM) special authority to create, change, or display a pre-shared key.

2. Use the procedure described in "Display connection security configuration properties" on page 127 to display the properties of the connection security configuration for the server.
   - Go to the **IP Security Rules** tab.
   - Note the first row in the table value, which contains a random pre-shared key generated by i5/OS. This information will be used in step 5.
3. Using iSeries Navigator:
   - Select **Integrated Server Administration** -> **Servers**.
   - Right-click the integrated server and select **Properties**.
   - Go to the **iSCSI Security** tab.
   - For the **Default IP security rule**, select **1**, then click **OK** to save the change. This tells i5/OS to do the following things: wherever a **Default** value appears for an IP security rule in the server properties, use the first value in the connection security configuration (specified by the server's **Connection security configuration** value on the **iSCSI Security** tab of the server properties).
4. This step is required only if you don't want IPSec enabled on all of the server's NWSD's connections, or if remote interface rules in the server properties have been changed from the Default value.

   Using iSeries Navigator:
   - Select **Integrated Server Administration** -> **Servers**.
   - Right-click the integrated server and select **Properties**.
   - Go to the **Storage Paths** tab.
   - Each **Remote Interface IP Security Rule** corresponds to an iSCSI HBA pair consisting of an iSCSI HBA for iSeries port and a hosted system iSCSI HBA port.

     Repeat the following for all of the **Remote Interface IP Security Rule** columns on the **Storage Paths** and the **Virtual Ethernet Paths** tabs.

     Note: Any NWSH used more than once in an NWSD must have identical sets of Remote Interface IP Security Rule values in each of the storage or virtual Ethernet paths that reference it.

     Set each Remote Interface IP Security Rule to either None or Default, whichever is appropriate for the way you are using that particular iSCSI HBA port pair:
     - Use **None** if you want network traffic to flow in the clear between the iSCSI HBA ports, regardless of the ability of either iSCSI HBA to support IPSec.
     - Use **Default** if the corresponding iSCSI HBA for iSeries supports IPSec, and you want to allow only encrypted traffic (or no traffic if the hosted system's iSCSI HBA port does not support IPSec).
5. This step is required only if the Delivery method in the remote system configuration is **Manually configured on remote system** or **Dynamically delivered to remote system via CHAP**: Upon the next server start (NWSD vary on), watch the hosted system's console for a prompt to press CTRL-Q. Immediately on seeing the prompt, press CTRL-Q. In the CTRL-Q utility, select the adapter that is configured to boot the hosted OS. Enter the pre-shared key from the connection security configuration properties into the pre-shared key of the target security configuration panel. See "Diskless booting over iSCSI" on page 22 more information about the CTRL-Q utility.

   Note: Any non-boot iSCSI HBAs in the hosted system are automatically configured from the i5/OS configuration.

Configure service processor SSL

SSL and a service processor password work together to secure system management traffic between an iSeries system LAN adapter and hosted system's service processors.

You can use either of the following methods to initialize the service processor SSL connection.

- "Automatic SSL initialization"
- "Manual SSL initialization"

For information about the service processor password, see "Service processor password" on page 131.

Automatic SSL initialization

To initialize SSL automatically, do the following steps:

1. If the connection between the service processor and the iSeries uses a shared network, consider temporarily connecting the service processor and the iSeries with an isolated network. If you do not, the automatic method is slightly less secure than the manual methods during the short time it takes for the Initialize task in step 3 to run.
2. Use the procedure described in "Change service processor configuration properties" on page 124 to change the properties of the service processor configuration for the server. Go to the **Security** tab and select the **Automatically set up user and generate certificate** option. Press OK to save the change.
3. Use the procedure described in "Initialize a service processor" on page 124 to initialize the service processor:
   a. Specify the **Initialize a new service processor** option.

      Note: Use the **Synchronize certificate from service processor** option if this is an additional service processor configuration used for the same service processor that has already been previously initialized for use with another integrated server.

   b. Specify the **User** and **Password** values.
   c. Press **Initialize** to perform the operation.

      Note: The service processor automatically generates a self-signed certificate, which is stored by i5/OS. The certificate is stored in the integrated file system directory /QIBM/UserData/Director/classes/com/ibm/sysmgt/app/iide/ with a file name that matches the name of the service processor configuration. This file will have a 'kdb' extension.

Manual SSL initialization

To initialize SSL manually using a certificate signed by a trusted Certificate Authority, do the following steps:

1. Use the web interface of the service processor to request an SSL certificate from a trusted Certificate Authority. For the detailed procedure, refer to the IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide (www.ibm.com/pc/support/site.wss/). Under **Browse**, select **Servers**, Family: **xSeries 236**, **publications**.

   Note: The certificate for the Certificate Authority must be in the i5/OS *SYSTEM certificate store.

2. Upon receipt of the new certificate from the Certificate Authority, use the web interface of the service processor to import the certificate into the service processor.
3. Use the procedure described in "Change service processor configuration properties" on page 124 to change the properties of the service processor configuration for the server. Go to the Security tab and do the following steps:
   a. Select the **Manually set up user and certificate** option.
   b. For the **Component** option, select either **Common name**, **E-mail address**, or **Organizational unit**.

   c. For the **Compare value**, specify the corresponding information in the new certificate. This allows SSL to distinguish your certificates from other certificates signed by trusted Certificate Authorities in the i5/OS *SYSTEM certificate store. For example, you can specify the e-mail address that you used to receive a certificate from a well-known Certificate Authority.
   d. Press **OK** to save the change.
4. Change the password and complete initialization. See "Service processor password."

To disable SSL, use the above procedure, but select the **Do not use a certificate (requires physical security)** option.

Service processor password

To change the service processor password, use the procedure described in "Initialize a service processor" on page 124.

1. Select the **Change service processor user ID and password** option.
2. Specify the new **User**, **Password**, and **Confirm new password values**.
3. Press **Initialize** to perform the operation.

Configure a firewall

If there is a firewall between the iSeries and the iSCSI network, 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 "Display remote system configuration properties" on page 121 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, TCP port, and UDP ports:** Use the procedure described in "Display network server host adapter properties" on page 118 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 iSeries 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 iSeries Navigator:

  1. Expand **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 value for **Virtual Ethernet control port**.

If IPSec is used, there are additional considerations for firewalls between an iSCSI HBA and the iSCSI network:

- **Allow IPSec:** This option is not available on all firewalls.
- Only IP addresses should be considered when configuring firewalls. TCP and UDP ports are encrypted by IPSec, and therefore the firewall cannot act on this information.

Manage iSCSI host bus adapters

Use the following tasks to manage iSCSI host bus adapters (HBAs) and Network server host adapters (NWSHs).

- "Hot spare between iSCSI local host adapters"
- "Manage iSCSI HBA usage" on page 133
- "Configuring multipath I/O" on page 138
- "Maximum transmission unit (MTU) considerations" on page 139
- "Integrated DHCP server" on page 141

Hot spare between iSCSI local host adapters

The iSeries iSCSI local host adapter hardware provides hot spare capabilities to enhance the reliability and recoverability of the Windows server environment. If the iSCSI local host adapter that a Windows server is using fails, you can quickly and easily switch the server to use another ″hot spare″ iSCSI local host adapter. 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, "Hot spare between server hardware" on page 156.

To hot spare iSCSI local host adapter hardware using iSeries 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:
   - Right-click the NWSH and select **Properties**.
   - Select the **General** tab and select a new value for the **Hardware resource** prompt.
   - 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.

Manage iSCSI HBA usage

You can attach several hosted systems (xSeries systems or IBM BladeCenter blades) to the iSeries using a single iSeries iSCSI host bus adapter (iSCSI HBA). You can also attach a single hosted system to the iSeries using several iSCSI HBA for iSeries. There are also a couple of ways of configuring a hosted system to use more than one iSCSI HBA for iSeries. Combinations of these techniques can be used as well.

See the following sections for information about several common configurations:
- "Share an iSCSI HBA among multiple hosted servers"
- "Spreading workload over multiple iSCSI HBAs" on page 134
- "Using multiple iSCSI HBAs for redundancy" on page 135
- "Manage iSCSI HBA allocation at the Windows side of the iSCSI network" on page 136

Share an iSCSI HBA among multiple hosted servers

A single iSCSI HBA for iSeries may 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 HBA for iSeries 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 HBA can support. Each active server storage path will use a file server resource in the network server host adapter (NWSH) object that corresponds to the iSCSI HBA. Likewise, each active server virtual Ethernet path will use a virtual Ethernet resource in the NWSH object. There is a limit to the number of file server and virtual Ethernet resources supported by a particular NWSH, which limits how many active servers can use the NWSH.

To see the NWSH file server and virtual Ethernet resource limits using iSeries Navigator, follow these steps:
1. 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 on the **Resource Usage** tab.
7. 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.
8. 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 less defined practical limit to the number of servers that an iSCSI HBA can support. The practical limit is determined by the available iSCSI HBA bandwidth and the workload that is being run through the iSCSI HBA. The practical limit will most likely limit how many hosted systems the iSCSI HBA can support before the file server and virtual Ethernet resource limits described above are reached. The practical limits will depend on your particular server configurations and workloads.

Spreading workload over multiple iSCSI HBAs

Servers that require high bandwidth may require more than one iSCSI HBA for iSeries to handle the workload. You can segment this even further by identifying which virtual disks and virtual Ethernet LANs require high bandwidth and which ones do not. For example, you can dedicate an iSCSI HBA to a disk that needs high bandwidth and share another iSCSI HBA 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 HBAs 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 using iSeries Navigator, first shut down the server (see “Start and stop an integrated server” on page 149), then follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **Servers**.
3. Right-click a server from the list available.
4. Select **Properties**.
5. Click on the **Storage Paths** tab.
6. Click the **Add** button to define a new storage path.
7. Select the network server host adapter (NWSH) that corresponds to the iSCSI HBA that you want to use for the storage path.
8. Click **OK** to add the storage path to the server properties panel.
9. 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.
10. Click **OK** on the server properties panel 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 in order to use the new storage path. First unlink the disk (see “Unlink integrated Windows server disk drives” on page 168). Then link the disk to the server again (see “Link a disk drive to an integrated server” on page 165), using the new storage path number that was added above.

To define additional virtual Ethernet paths using iSeries Navigator, first shut down the server (see “Start and stop an integrated server” on page 149), then follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **Servers**.
3. Right-click a server from the list available.
4. Select **Properties**.
5. Click on 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. Click **OK** on the server properties panel to save the changes in the NWSD.

If you want to use a CL command, see the VRTETHPTH keyword on the CHGNWSD command.

Using multiple iSCSI HBAs for redundancy

Even if the bandwidth requirements of a server do not indicate that more than one iSCSI HBA for iSeries is needed, you may want to use multiple iSCSI HBAs to provide fault tolerance and redundancy. This will reduce the likelihood of server failures that are caused by a failure of an iSCSI HBA or one of the network components (switches, cables, and so on.) that connect the iSeries to the hosted system. Redundancy is provided by the iSCSI ability to do multipath I/O (see “Advanced iSCSI support” on page 20). To take advantage of multipath I/O, you create a multipath group that identifies two or more iSCSI HBAs. Then you define which virtual disks will use the multipath group. You can optionally use the multipath group as the default path when linking disk drives.

To define a multipath group using iSeries Navigator, first shut down the server (see “Start and stop an integrated server” on page 149), then follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **Servers**.
3. Right-click a server from the list available.
4. Select **Properties**.
5. Click on the **Storage Paths** tab.
6. Define at least two storage paths (use the **Add** button, if necessary).
7. Below the storage paths table, click the **Properties** button for the multi-path group.
8. Use the checkboxes to identify two or more of 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. **Optional:** Select the multi-path group as the default path for disk drives.
11. Click **OK** on the server properties panel to save the changes in the NWSD.

If you want to use a CL command, see the MLTPTHGRP and DFTSTGPTH keywords on the CHGNWSD command.

Now that the multipath group is defined, you need to re-link one or more of the server’s virtual disks in order to use the multipath group. First unlink the disk (see “Unlink integrated Windows server disk drives” on page 168). Then link the disk to the server again (see “Link a disk drive to an integrated server” on page 165), specifying either the multipath group explicitly or specifying the default path (if the default path for disk drives was defined to use the multipath group).

Manage iSCSI HBA allocation at the Windows side of the iSCSI network

An iSCSI attached integrated Windows server can use multiple physical iSCSI HBA ports. An iSCSI HBA 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 HBA port for the Windows server.

IP addresses

iSCSI HBA ports can have a SCSI IP address, a LAN IP address, or both types of address. A port with a SCSI IP address can carry storage traffic. A port with a LAN IP address can carry virtual Ethernet traffic.

Boot storage configuration

You select the iSCSI HBA port used to boot Windows with the CTRL-Q utility. After Windows Server has started, the selected iSCSI HBA port will continue to provide a connection to the i5/OS storage path that corresponds to the system drive.

Automatic allocation of iSCSI HBA ports to virtual Ethernet and non-boot storage paths

IBM i5/OS Integrated Server Support includes several applications for Microsoft Windows that automatically read the i5/OS objects that contain the server configuration information. These programs automatically allocate the iSCSI HBA 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 Windows Server.
- You restart the **IBM iSeries Virtual Ethernet Manager service** from **Control Panel→ Administrative Tools→ Services**.
- You run the command **qvndvimr /restart** at a Windows command prompt.
- A connection fails. In this case, the affected virtual Ethernet connections are automatically assigned to a different iSCSI HBA port at the hosted system if one is available. Virtual Ethernet will not use the failed connection again until the cause of the failure is corrected and one of the 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 iSeries Manager** service from **Control Panel→Administrative Tools→Services**.
- You run the command **lvmaster /restart** at a Windows command prompt.

Manual allocation of storage to a physical iSCSI HBA port

You can manually allocate storage to a physical iSCSI HBA port. You must have a Windows server with multiple iSCSI HBA ports and an iSeries system with multiple iSCSI HBAs. This task affects iSCSI HBA usage at both sides of the iSCSI network.

Run the qvnimap command at the integrated server console to generate a Storage Device Connection table. Look for all rows in the table that show a physical connection to the desired iSCSI HBA 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. For more information about linking disks, see “Link a disk drive to an integrated server” on page 165.

Manual allocation of a virtual Ethernet adapter to a physical HBA port

If you want to override automatic allocation for virtual Ethernet, you can manually allocate an iSCSI HBA port. Do these steps at the integrated server console.

1. Navigate to the **Network Connections** window.
2. Double-click the **IBM iSeries 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. Enter the IP address of the iSCSI HBA port in Windows 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 HBA allocation. For more information, see "Use the qvnimap command to view iSCSI HBA allocation" and "Display information about virtual Ethernet adapters" on page 138.

Use the qvnimap command to view iSCSI HBA allocation

You can use the qvnimap command to display how iSCSI HBAs are being used for a particular Windows server. Make sure you have administrator rights 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 types of connection tables, one for storage devices and one for virtual Ethernet networks. In connection tables, an ***X*** represents a physical connection that is used by the storage device and path or is used by the virtual Ethernet described to the left of the ***X***. The two endpoints of the physical connection are the initiator port identified above the ***X***, and the target NWSH identified to the immediate left of the ***X***. By looking for all occurrences of ***X*** 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 will appear in the drive column. If a storage space is being used to provide multiple drives, there will be 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 things:

- Initiator iSCSI HBA ports, identified by names such as P1 and P2
- Windows-side Virtual Ethernet port, identified by names such as VRTETHPTP and VRTETH0
- Target iSCSI HBAs, identified by NWSH name

If you do not have administrator rights on the Windows server, you might see some incorrect or missing information such as the following things:

- "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

There are errors that might appear in the output of the qvnimap command.

Table 2. Errors that might occur when you run the qvnimap command and some possible solutions

Condition	Possible causes
RMTIFC MAC address not found	• Incorrect MAC address in the remote system configuration object • Corresponding SCSI or LAN driver disabled or not installed

Table 2. Errors that might occur when you run the qvnimap command and some possible solutions (continued)

Condition	Possible causes
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, this might be caused by one of the following things: • A physical port, network, or network server host adapter (NWSH) problem • The target and initiator on 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

Display 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.

Configuring 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.

For information about multipath I/O and the multipath group, "Advanced iSCSI support" on page 20

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 Web page.

Do these steps to configure multipath I/O.

1. "Configuring the Windows operating system for multipath I/O"
2. "Configuring the integrated server for multipath I/O" on page 139

Configuring the Windows operating system for multipath I/O

Do these steps to install the Microsoft Software Initiator service on the integrated server.

1. Install the i5/OS PTFs listed on the i5/OS PTFs (www.ibm.com/systems/i/bladecenter/ptfs.html) Web page.
2. Synchronize the Windows server and restart the Windows operating system. See "Code fixes" on page 106.
3. Download and install the Microsoft iSCSI Software Initiator. For information about versions of the software that have been tested with iSCSI-attached servers, see the iSCSI install read me first Web page.
   a. Go to the Microsoft Download Center (www.microsoft.com/downloads/) Web site.
   b. Search for **iSCSI initiator**.
   c. Install **Virtual Port Driver**, **Initiator Service**, and **Microsoft MPIO Multipathing Support for iSCSI**. Do not select the option for **Software Initiator**.

      Note: Do not manually configure the installed Microsoft components. The iSeries Manager service automatically configures these components.
   d. Restart the Windows operating system.

The iSeries Manager service is aware of the target storage configured in i5/OS and provides the optimal multipath configuration.

Configuring the integrated server for multipath I/O

To configure your integrated server to use a multipath group, do these steps.

1. Shut down the server. See “Start and stop an integrated server” on page 149
2. Expand **Integrated Server Administration**.
3. Expand **Servers**.
4. Right-click a server from the list available.
5. Select **Properties**.
6. Click on the **Storage Paths** tab.
7. 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**.
8. Below the storage paths table, click the **Properties** button for the multi-path group.
9. Use the checkboxes to identify the defined storage paths to be members of the multi-path group.
10. Click **OK** to update the multi-path group information on the server properties panel.
11. Select the multi-path group as the default path for disk drives.
12. Click **OK** on the server properties panel to save the changes in the NWSD.
13. 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 “Unlink integrated Windows server disk drives” on page 168.
   b. Link the disk to the server. Specify either the multipath group or the default path. See “Link a disk drive to an integrated server” on page 165.

If you want to use a CL command, see the STGPTH, MLTPTHGRP and DFTSTGPTH keywords on the Change Network Server Description (CHGNWSD) command.

Maximum transmission unit (MTU) considerations

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. This setting affects the frame size used by both storage and virtual Ethernet over the iSCSI network. 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. The MTU setting can affect performance, especially virtual Ethernet performance. For information to help you decide which MTU value to use, see “iSCSI network” on page 29.

Note: MTU prompts in the Install Windows Server (INSWNTSVR) command have no effect except for external LAN adapters used on IXS.

Virtual Ethernet has additional MTU configuration capabilities. See the following topics for information about virtual Ethernet MTU configuration:

- “Configuring virtual Ethernet for maximum performance on iSCSI networks that support frames larger than 1500 bytes”
- “Configuring virtual Ethernet for iSCSI networks that have a maximum frame size that is less than 1500 bytes”
- “Configuring virtual Ethernet to support unusual non-TCP applications that do not negotiate MTU”

Configuring virtual Ethernet for maximum performance on iSCSI networks that support frames larger than 1500 bytes

For information on configuring the virtual Ethernet frame size for your iSCSI HBAs, see the iSCSI HBA document.

Related configuration items listed below should be left at their default values:

- For Windows virtual Ethernet adapters, Maximum Frame Size defaults to Auto. Auto causes virtual Ethernet to calculate a maximum frame size based on the Ethernet Frame Size of the iSCSI HBA port used. See “Manage iSCSI HBA allocation at the Windows side of the iSCSI network” on page 136 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**.

Configuring 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 iSeries Virtual Ethernet x** adapter that will use a 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 iSCSI network’s maximum frame size.

Configuring virtual Ethernet to support unusual non-TCP applications that do not negotiate MTU

Note: To avoid impacts to normal applications that negotiate MTU, before performing this procedure you may want to define a separate virtual Ethernet network or separate IP addresses for the application that does not negotiate MTU.

1. Do one of the following.
   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 most constrained iSCSI network’s maximum frame size.
   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 is as large as possible without exceeding the most constrained iSCSI network’s maximum frame size.
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. Using iSeries 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** tab, 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.

Integrated DHCP server

The iSeries iSCSI attached server solution provides an integrated DHCP server. The server is used to deploy boot parameters to the hosted system iSCSI HBA when the Dynamically delivered to the remote system via DHCP option is specified in the i5/OS remote system configuration object and AUTO or DHCP mode is specified in the hosted server iSCSI HBA.

The integrated DHCP server is not a general purpose server. It is intended to exclusively deploy boot parameters to the hosted server iSCSI HBA. The server is automatically configured with the parameters provided in the remote system configuration when an network server description (NWSD) is varied on.

The DHCP server will only respond to the hosted server's iSCSI HBA DHCP client. All of the iSCSI HBA DHCP client requests use an IBM defined vendor id. The server is programmed to respond to requests that use the default vendor id. Any other requests from other devices in the network will be ignored by the DHCP server.

Providing the MAC addresses of the hosted server iSCSI HBAs in the remote system configuration object is very important. In addition to the vendor id previously described, the integrated DHCP server uses the MAC address to properly deploy boot parameters. MAC address is part of the specific scope required to ensure proper parameter deployment.

The scope provided by the vendor id and MAC address can be changed. While this is considered an advanced function, provisions have been put in place to allow the advanced and sophisticated users to more specifically configure this setting, when required. The default vendor id can be configured to other values. Configuration screens are available in the hosted server iSCSI HBA adapter CTRL-Q set up utility and the corresponding remote system configuration object. This advanced function is compliant with the RFC 2132 specification. For more details on advanced configurations see iSCSI install read me first

When an incoming DHCP request is received by the integrated DHCP server and all of the required scope is matched, the integrated DHCP server provides to the DHCP client 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 initiator is the iSCSI HBA in the hosted server that will be 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 hosted system iSCSI HBA.

Both of these sets of IP addresses and IQNs are in the iSeries 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 44.

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 iSeries software objects, eliminating the need to manually configure a server when boot parameters (IP addresses and IQNs) change.

Remote server discovery and management

IBM Director and information from the i5/OS remote system configuration and service processor configuration objects are used to locate and manage attached servers. See the following information.

- “Verify that IBM Director Server is installed and running”
- “Configure remote server and service processor discovery”
  - “Service processor discovery configuration” on page 143
  - “Dynamic IP addressing (DHCP)” on page 144
  - “Service processor discovery methods” on page 144
- “Use the Management Module or RSA II web interface” on page 146

Verify that IBM Director Server is installed and running

IBM Director Server must be installed and running on the i5/OS partition that is connected to your integrated server. Director is used for power control and some management functions for your integrated xSeries or blade hardware.

If you have not installed IBM Director Server, see “Software requirements” on page 59.

If you are using iSeries 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 the “IBM Director Troubleshooting” on page 222 topic and the iSCSI troubleshooting web page (www.ibm.com/systems/i/bladecenter/troubleshooting.html) for more information.

Configure remote server and service processor discovery

i5/OS uses IBM Director Server to locate and identify remote servers on a local area network (LAN) by communicating with the service processor of the remote server. Remote systems are identified by information stored in the remote system configuration and the service processor configuration objects on the iSeries server.

This is a different connection than the connection between the iSeries 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 an iSeries server LAN adapter.

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.

See the following information:

- “Remote server and service processor discovery concepts” on page 23
- “Service processor discovery configuration” on page 143
- “Dynamic IP addressing (DHCP)” on page 144
- “Service processor discovery methods” on page 144
- “Use the Management Module or RSA II web interface” on page 146

Service processor discovery configuration

The service processor IP information must be configured to match the i5/OS configuration. The configuration options depend on the type of service processor. For information about identifying the type of service processor in your xSeries server, 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 xSeries 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 "Discovery by IP address" on page 144.
- The BMC supports security using a password. See "Service processor password" on page 131.

Remote Supervisor Adapter II (RSA II)

The RSA II service processor is available in some xSeries 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 "Use the Management Module or RSA II web interface" on page 146.
- 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 IP addressing (DHCP)" on page 144. 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.
  - "Service Location Protocol (SLP) using multicast addressing" on page 146.
  - "Discovery by IP address" on page 144.
  - "Discovery by host name" on page 145.
- The RSA II supports the following security methods:
  - Password. For the configuration procedure, see "Service processor password" on page 131.
  - SSL and password. See "Configure service processor SSL" on page 130.
- 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/pc/support/site.wss/). 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/pc/support/site.wss/). Under **Browse**, select **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue**. Select **Publications**.

Management Module

The Management Module is available in IBM BladeCenter servers.

- To configure the Management Module, see "Use the Management Module or RSA II web interface" on page 146.
- 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 IP addressing (DHCP)." This is the factory default.
  - Static IP address information.
- The Management Module supports the following discovery methods. Use the one that is the most appropriate for your network.
  - "Service Location Protocol (SLP) using multicast addressing" on page 146
  - "Discovery by IP address."
  - "Discovery by host name" on page 145
- IBM BladeCenter servers have additional considerations for discovery. The remote system identity in the remote system configuration must always be set to the serial number of the IBM BladeCenter server, which can be found on a label on the server. For information about changing the remote system configuration, see "Change remote system configuration properties" on page 122. The enclosure identity in the service processor configuration may be set to the IBM BladeCenter enclosure (chassis) serial number. The Management Module service processor in the IBM BladeCenter must be discovered before any server blades can be discovered. Parameters in the service processor configuration will determine the method of discovery of the Management Module. For information about changing these properties, see "Change service processor configuration properties" on page 124. After the Management Module is discovered, IBM Director will gather information about the server blades contained in the enclosure. The remote system identity will be used to perform the second phase of discovery to discover the individual server blade.
- Management Module supports the following security methods:
  - Password. For more information, see "Service processor password" on page 131.
  - SSL and password. See "Configure service processor SSL" on page 130.
- See the IBM BladeCenter Systems Management Redpaper (www.redbooks.ibm.com/abstracts/redp3582.html) for more information about IBM eServer BladeCenter Systems Management.

Dynamic IP addressing (DHCP)

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.

Service processor discovery methods

There are several methods of service processor discovery.

- "Discovery by IP address"
- "Discovery by host name" on page 145
- "Service Location Protocol (SLP) using multicast addressing" on page 146

Discovery by IP address: This method of discovery uses unicast addressing. To configure discovery by IP address, perform the following steps.

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 "Use the Management Module or RSA II web interface" on page 146.
2. On the iSeries server, 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 "Change service processor configuration properties" on page 124.

3. Using the procedure described in "Change remote system configuration properties" on page 122, ensure that the remote system identity is set correctly:
   - For a stand-alone server, select the **Use enclosure identity from the service processor configuration** option.
   - For a IBM BladeCenter blade, select the **Use the following values** option and specify the blade serial number.

Advantages:

- This discovery method is very simple if the service processor's IP address is known and configured into the service processor.

Disadvantages:

- The IP address must be configured into the 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 hosted 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 "Use the Management Module or RSA II web interface" on page 146.
   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 iSeries server, 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 "Change service processor configuration properties" on page 124.
3. Using the procedure described in "Change remote system configuration properties" on page 122, ensure that the remote system identity is set correctly:
   - For a stand-alone server, select the **Use enclosure identity from the service processor configuration** option.
   - For an IBM BladeCenter blade, select the **Use the following values** option and specify the blade serial number.

Advantages:

- If a DNS server is available, a specific IP address need not be maintained in the i5/OS remote system configuration.

Disadvantages:

- 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.

Service Location Protocol (SLP) using multicast addressing: If you are not using the service processor host name or internet address to discover the server on the network, then multicast addressing with Service Location Protocol (SLP) is used. To configure SLP discovery, you must configure your iSeries server. Do the following steps.

1. Using the procedure described in "Change service processor configuration properties" on page 124:
   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 "Change remote system configuration properties" on page 122, 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.

The service processor advertises itself with a SLP packet sent on the network using multicast addressing. This packet includes attributes such as the serial number, type, and model of the remote server. IBM Director receives this packet and saves information about the server. The serial number from the service processor configuration enclosure identifier or the remote system configuration remote system identifier are mapped to the attributes learned from the SLP discovery process to identify a specific remote server.

Advantages:

- 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.

Disadvantages:

- SLP is only supported by the Remote Supervisor Adapter II service processor and the IBM BladeCenter Management Module service processor. It is not supported by Baseboard Management Controller (BMC) service processors.
- Routers and switches located between the service processor and the iSeries LAN adapter must be configured to support multicast addressing. If not properly configured, routers will not propagate multicast packets. Consult your router documentation to determine how to configure it to allow multicast addressing. The Service Location Protocol uses IP address 239.255.255.253 and port number 427. This information may be required to configure routers to support multicast SLP packets.

Use the Management Module or RSA II web interface

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, the i5/OS objects will contain the old user name and password and you will not be able to connect to the service processor. See “Initialize a service processor” on page 124.

Use the method in “Initialize a service processor” on page 124 to change the user name and password or the Initialize NWS Configuration (INZNWSCFG) command with the *CHGSPAUT option. This will keep the i5/OS objects synchronized with the service processor’s user name and password.

For information about using the web interface to the service processor, see the following links:

- Chapter 2 of the IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User’s Guide - Servers (www.ibm.com/pc/support/site.wss/). Under **Browse**, select **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue**. Select **Publications**
- IBM xSeries and BladeCenter Server Management, SG24-6495

Connect to the an RSA II or IBM BladeCenter Management Module with a web browser

1. **Optional:** If you need to connect the browser to the RSA II through a router, first configure the RSA II’s IP address using the BIOS interface.
2. First enter the RSA II or Management Module IP address or host name in the web browser’s address (url) area.
3. A prompt for the RSA II or Management Module user name and password should be displayed. 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 will not be able to 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.

Once connected to the RSA II/Management Module’s web interface the following tasks can be accomplished:

- 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.

Chapter 8. Administer integrated Windows servers

The following sections will guide you through some common, everyday tasks performed on the integrated server.

Start and stop an integrated server

An integrated Windows server has no power button; its state is controlled by the iSeries. Normally you start and shut down integrated servers from iSeries Navigator or the character-based interface. You can partially shut down an integrated server using its own **Start —> Shut Down** menu, but you cannot start it again without using iSeries Navigator or the character-based interface.

Ensure that integrated servers are varied off before shutting down your iSeries, otherwise, data corruption can occur. Some commands used to shutdown the iSeries will initiate a shutdown in attached integrated servers and wait a certain amount of time for them to power down before shutting down the iSeries. Other commands will shut down the iSeries immediately.

If you use the power off/on scheduling program QEZPWROFFP, you will need to configure it to work with your integrated server.

The following sections describe the start and shut down methods:

Start and stop an integrated Windows server using iSeries Navigator

1. To stop an integrated server in iSeries Navigator, select **Integrated Server Administration -> Servers**.
2. Right-click the server you want to stop and select **Shut Down**. If you want to shutdown all integrated servers, right-click the Integrated xSeries Servers icon in the left navigation and select **Shut Down All**. The status changes to **Shutting down...**, **Partially shut down**, and eventually **Shutdown**.
3. To start an integrated server, right-click it and select **Start**. The status changes to **Starting** and eventually **Started**.

Start and stop an integrated Windows server using the character-based interface

1. To stop an integrated server using the character-based interface type the command `WRKCFGSTS *NWS`.
2. Find the integrated server to stop and enter `2` to cause a *vary off*.
3. The status changes from **ACTIVE** to **SHUTDOWN** to **VARIED OFF**. You can push **F5** to update the screen.

   Note: For iSCSI attached servers the status changes from **ACTIVE** to **VARIED OFF**.
4. To start the integrated server use the same command `WRKCFGSTS *NWS`, and type `1` to *vary on* or start the integrated server.
5. To restart an integrated server you must manually vary it off and then back on. There is no command to automatically restart an integrated server from the character-based interface.

Shutdown an integrated server from the Windows server console

To shut down an integrated Windows server from its own console you select **Start —> Shut Down** from the Windows start menu. However, this method is not recommended because it only causes an integrated server to partially shut down. The Windows operating system stops, leaving the screen *It is now safe to turn off your computer*, but to completely power down and restart you must *vary off* the server using iSeries Navigator or the character-based interface.

As opposed to shutting down, **restarting** an integrated server from its own console is one of the most efficient ways to do so.

Follow these steps

1. From the **Start** menu, choose **Shut down**.
2. Select **Restart** from the drop-down menu and click **Ok**.

Note: For iSCSI attached servers, when the server is Shutdown from the Windows server console the NWSD will not be varied off. The NWSD will transition from ACTIVE to VARIED ON. The server status can be queried using iSeries Navigator or using the Work with Network Server Status (WRKNWSSTS). The status is retrieved every time the command is issued. The Windows server will not automatically report its state.

How to safely shutdown your iSeries when integrated Windows servers are present

The easiest way to ensure your integrated servers will be shut-down safely is to always manually shut them down before shutting down the iSeries. You may grow tired of this tedious task, however. 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.

Note: The CL command `PWRDWNSYS *IMMED` is not recommended. This will power down the iSeries immediately, without attempting to shut down any integrated servers.

Table 3.

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 iSeries continues to power down.

Table 3. (continued)

Issue the CL command `pwrdwnsys *immed`.	The iSeries 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.

Connect to the 4812 IXS virtual serial console

The virtual serial console provides Windows console functions for a Windows Server 2003 server that is running on a 4812 Integrated xSeries Server (IXS). See “Windows console” on page 24 for more information about Windows consoles. This console connection can be used before configuring TCP/IP on the server.

Any Telnet client can be used as the virtual serial console. Multiple Telnet clients can share access to the same virtual serial console. To connect to a console, use Telnet to connect to port 2301 of the i5/OS partition that is sharing its resources. TCP/IP must be configured and running on the i5/OS logical partition.

To connect to a virtual serial console using the IBM Personal Communications client, do the following steps:

1. Click **Start** -> **Programs** -> **IBM Personal Communications** -> **Start or Configure Session**.
2. On the Customize Communication dialog box, select **ASCII** in the **Type of Host** field.
3. Click **Link Parameters**.
4. On the TelnetASCII dialog box, type the host name or the IP address of the i5/OS partition, where you want to connect, in the **Primary Host Name or IP Address** field.
5. Type `2301` in the **Primary Port Number** field.
6. Click **OK**.
7. Click **OK**. The session dialog box opens.
8. On the i5/OS Virtual Consoles menu, select **Integrated xSeries Server Consoles**.
9. On the Integrated xSeries Server Consoles dialog box, select the hardware resource name for the 4812 IOA that you want to connect as the console. To determine the 4812 IOA hardware resource name, display the Network Server Description (NWSD) for the server and use the value of the Resource name parameter.
10. Type the i5/OS service tools ID and password to connect to the Integrated xSeries Server virtual console.

To connect to the virtual serial console using Telnet from a DOS command prompt, follow these steps:

1. On the Command Prompt dialog box, type `telnet` *`partitionname`* `2301`. Where *`partitionname`* is the name of the i5/OS partition where you want to connect.
2. Press the Enter key.
3. On the i5/OS Virtual Consoles menu, select **Integrated xSeries Server Consoles**.

4. On the Integrated xSeries Server Consoles dialog box, select the hardware resource name for the 4812 IOA that you want to connect as the console. To determine the 4812 IOA hardware resource name, display the Network Server Description (NWSD) for the server and use the value of the Resource name parameter.
5. Type the i5/OS service tools ID and password to connect to the Integrated xSeries Server virtual console.

View or change integrated Windows server configuration information

iSeries Navigator allows you to view and change most integrated server configuration information.

1. In iSeries 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 iSeries Navigator as follows:

1. In iSeries 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**.
   - **Local 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 4.

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
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)

Message logging

Integrated Windows servers log information in different places. If there is a problem, this information may help determine the cause. The following sections describe the message logs.

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 iSeries 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 redbook, Microsoft Windows Server 2003 Integration with iSeries, SG24-6959, has an excellent section concerning integrated server event logs in i5/OS and at the Windows console.

Run 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 iSeries operation through Kerberos enabled applications (like iSeries Navigator single sign-on). See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 155 for more information.
- The i5/OS user profile password, and Windows password must be equivalent. The easiest way to keep them consistent is to use User and Group enrollment.

You may also want to read these “Guidelines for submitting remote commands” on page 154.

To run integrated server commands from iSeries Navigator

1. In iSeries 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 remotely submit integrated Windows server commands, keep these guidelines in mind:

Note: Many of the SBMNWSCMD parameters discussed in this section are not available when running Windows commands by using iSeries Navigator. If you need to use a parameter that iSeries 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 155.
- 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

File level backup operations to an integrated Windows server utilize the iSeries NetClient and Submit Network Server Command (SBMNWSCMD) functions. In i5/OS V5R3 or later, these functions provide limited Kerberos v5 support (also known as iSeries Network Authentication). Thus, there are some considerations to keep in mind if you want to use network authentication with these functions.

1. In order to enable iSeries to use Kerberos authentication, you must configure these things on the iSeries server:
   - iSeries Navigator Security option
   - Network authentication service
   - Enterprise Identity Mapping (EIM)
   - Cryptographic Access Provider (5722-AC2 or AC3)
2. The iSeries NetServer should be configured to use Password/Kerberos v5 authentication and 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 Kerberos with a Windows Server 2003 Active Directory Server” on page 104.
4. Kerberos authentication will only be used when the i5/OS job’s user profile has the LCLPWDMGT attribute set to `*NO`. 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**.

Hot spare between server hardware

iSeries and xSeries integration and storage virtualization provide options that can enable you to enhance the reliability and recoverability of your Windows server environment. If a Windows server fails, you can quickly and easily switch the server’s storage spaces to another hot spare xSeries server without restarting your iSeries server. This may reduce the total number of Intel servers needed to provide increased availability. It also adds flexibility by enabling one spare server to be used to protect multiple production servers.

Note: For iSCSI attached servers, the iSCSI local host adapters can also take advantage of hot spare support. See “Hot spare between iSCSI local host adapters” on page 132.

The procedures for hot sparing an integrated server’s hardware are shown below.

Using iSeries 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:
   - Right-click the server and select **Shut Down**.
   - 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 change one of the following:
      - For non-iSCSI servers, select the new **Resource name and type**.
      - For iSCSI servers select the new **Remote system configuration name**.

   Click **OK**.
5. To start the integrated server, right-click the server and select **Start**.

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 to change one of the following:
   - For non-iSCSI servers, change the value for the **Resource name (RSRCNAME)** parameter to specify the new IXS or IXA hardware resource name.
   - For iSCSI servers, 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.

Chapter 9. Manage storage

Instead of having their own hard disk drives, integrated Windows servers use i5/OS disk storage for storing client data and sharing network files. i5/OS disk storage allocated to an integrated server is called *network server storage space*. The integrated server equivalent of installing a new hard drive in a PC server is to create a network server storage space in i5/OS and link it to an integrated server. Realizing that integrated server disk storage is managed through i5/OS will influence your decisions about drive sizes, partitioning, and disk volumes. See "i5/OS storage management." You can also read about "Predefined disk drives for integrated Windows servers" on page 162 and "Disk drives for integrated Windows servers" on page 160.

Windows environment for iSeries helps you handle data storage in the following ways:

- By allowing you to use i5/OS to "Administer integrated Windows server disk drives from i5/OS" on page 163.
- By giving you the option to "Use Windows disk management programs with integrated Windows servers" on page 169.

i5/OS storage management

This brief overview of i5/OS storage management concepts is intended for administrators who are more familiar with how Windows servers manage storage. Because i5/OS handles storage management differently than a PC server, some techniques that you need in the PC server world are unnecessary in the Windows environment on iSeries.

i5/OS and disk drives

i5/OS, the operating system that runs on an iSeries, does not need to deal directly with disk drives. Beneath the operating system a level of software (called System Licensed Internal Code (SLIC)) ″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 Windows 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 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 iSeries Navigator. Both the Information Center and iSeries Navigator refer to ASPs as Disk Pools.

Disk protection:

i5/OS disks can be protected in two ways:

- **Cross-site mirroring**
  Cross-site mirroring, using the operating system geographic mirroring function for IASPs, 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. i5/OS 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 models of iSeries, 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, read Backup and Recovery.

Disk drives for integrated Windows servers

Integrated servers do not have their own disk drives. i5/OS creates network server storage spaces within its own file system and integrated servers use them as if they were normal hard disk drives.

For an integrated Windows server to recognize an integrated server disk drive (network server storage space) as a hard disk drive, you must link them together. You must create a disk drive before you can link it. See “Create an integrated server disk drive” on page 164 and “Link a disk drive to an integrated server” on page 165. 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. See “Format integrated server disk drives” on page 166.

Disk drives can be linked to servers in one of the following ways:

1. Fixed (static) disk drive links allow disk drives to be linked to the server using user specified link sequence positions. The order that the server sees the drives is determined by the relative order of the link sequence positions. The server must be varied off when adding a fixed (static) disk drive link.

   Note: Static drive links are not used for iSCSI attached xSeries servers.
2. A cluster quorum resource disk drive link is used to link the cluster quorum resource disk drive to the servers in the cluster.
3. Cluster shared disk drive links allow a disk drive to be shared among clustered integrated servers. A shared drive can only be linked to nodes that share a common quorum resource drive. Drives of this

type are available to all nodes that are joined together by the links of the cluster quorum resource. Each node has access to the shared drives under the control of Windows Cluster services running on each node.

Note: Drives that are linked as shared should be linked to ALL nodes that are clustered together.

4. Dynamic disk drive links allow additional disk drives to be linked to an integrated server using dynamically assigned link sequence positions. 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 a non-iSCSI integrated server is started, it sees the disk drives in the following order:

1. Statically linked disk drives.
2. Cluster quorum resource disk drive.
3. Cluster shared disk drives.
4. Dynamically linked disk drives.

For iSCSI attached servers, the cluster quorum disk appears at the end of the list of disk drives. Dynamically linked disks and cluster shared disks can be intermixed.

Within each of these link type categories, the disks appear in the order of their user specified link sequence positions. When dynamically linking a disk drive to an active server, the new disk drive appears following all other linked disk drives.

The following table shows the iSeries virtual disk drive features supported for various types of server network server descriptions (NWSDs) with i5/OS V5R4 or later.

Disk features supported

Feature	**NWSD type[5] *WINDOWSNT or *IXSVR with OS type *WIN32**	**NWSD type[5] *ISCSI with OS type *WIN32**
Number of fixed (static) links	16	0
Number of dynamic links	16	63[1]
Number of cluster quorum links	1	1
Number of cluster shared links	15	61[1]
Maximum number of virtual disks that can be linked to the server	48 with clustering[2]; 32 otherwise	64 with clustering[2]; 63 otherwise
Maximum capacity per virtual disk	1000 GB	1000 GB
Maximum total virtual disk capacity, assuming 1000 GB per disk	46.9 TB with clustering[2]; 31.3 TB otherwise	62.5 TB with clustering[2]; 61.5 TB otherwise
Can link virtual disks while the server is active?	Yes Exceptions: fixed links	Yes Exceptions: dynamic links 1-2
Can unlink virtual disks while the server is active?	Yes Exceptions: fixed links, disk can not be part of a volume set, disk can not be a volume mounted in a directory	Yes Exceptions: dynamic links 1-2, disk can not be part of a volume set, disk can not be a volume mounted in a directory
Virtual disk format types allowed when linking[3]	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN
Virtual disk access types allowed when linking	Exclusive update, shared update[4]	Exclusive update, shared update[4]

Feature	NWSD type[5] *WINDOWSNT or *IXSVR with OS type *WIN32	NWSD type[5] *ISCSI with OS type *WIN32
Disk links requiring exclusive update address type	All fixed disk links and all dynamic links	All dynamic links
Disk links requiring shared update address type	Cluster quorum link and all cluster shared disk links	Cluster quorum link and all cluster shared disk links

Notes:

1. For iSCSI Windows servers, the dynamic and cluster shared disks use the same sequence position range and can be intermixed. The combined total number of dynamic and cluster shared disk links is 63.
2. Windows server clustering requires use of Microsoft Cluster Service (MSCS) to control access to the shared disks in the cluster.
3. See the Create NWS Storage Space (CRTNWSSTG) command help text for a description of the format types.
4. When multiple servers link a disk using shared update, only one server can actually have write access to the disk at any point in time. For example, on Windows servers, Microsoft Cluster Service (MSCS) is used to control which server in the cluster has write access to the disk.
5. See the Create Network Server Desc (CRTNWSD) command help text for a description of the NWSD types and the associated operating system (OS) types.

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 drive to another to move it to a different disk pool.

After a network server storage space has been created and linked to an integrated server, you must format it from the Windows console. You can choose from between three types of disk formats. You will probably choose NTFS since it is the most efficient and secure format. Partitions formatted with NTFS can be up to 1,024,000 MB. Another format type is FAT-32. Partitions formatted with FAT-32 can be from 512 – 32,000 MB. The oldest format type is FAT. The maximum possible size for a FAT partition is 2,047 MB. The predefined installation source drive partition (D), which must be in FAT format, is therefore limited to 2,047 MB.

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 iSeries NetServer.

The IBM iSeries integrated server support installation process creates several disk drives that are used to install and run integrated Windows servers. See the topic on "Predefined disk drives for integrated Windows servers."

For information about creating drives, see "Create an integrated server disk drive" on page 164

Predefined disk drives for integrated Windows servers

The IBM iSeries Integrated Server Support installation process creates two disk drives (network server storage spaces) for installing and running integrated servers. See "Disk drives for integrated Windows servers" on page 160. By default, i5/OS creates these disk drives in the system disk pool (ASP), but you can choose a different location during the installation. i5/OS also uses these disk drives to load and start the integrated server.

Servers have these predefined disk drives:

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. You can choose to leave the drive as FAT. The C drive is automatically converted to NTFS, if required by the size of the storage space.

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 Chapter 15, “Network server description configuration files,” on page 243. 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” on page 87.

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 iSeries 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: 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.

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.

Administer integrated Windows server disk drives from i5/OS

Administering integrated server disk drives (network server storage spaces) from i5/OS includes these tasks:

- “Access the i5/OS integrated file system from an integrated server”
- “Obtain information about integrated server disk drives”
- “Add disk drives to integrated Windows servers” on page 164
- “Copy a disk drive” on page 166
- “Expand a disk drive” on page 167
- “Expand a system drive” on page 168
- “Unlink integrated Windows server disk drives” on page 168
- “Delete integrated Windows server disk drives” on page 168

Access 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 iSeries Support for Windows Network Neighborhood (iSeries NetServer). This allows you to easily work with file system resources on i5/OS. For information about using iSeries NetServer, see:

- Create an iSeries NetServer file share
- Set up your PC client to use iSeries NetServer
- Access iSeries NetServer file shares with a Windows client

For more information, see “Enable iSeries NetServer” on page 63.

Obtain information about integrated server disk drives

If you want to know what percentage of an integrated server disk drive (network server storage space) is in use or what its format is, you can obtain the information from i5/OS.

To obtain disk drive information, follow these steps:

1. In iSeries 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 iSeries Navigator toolbar

If you want to use the CL command, see Work with Network Server Storage Spaces (WRKNWSSTG).

Add disk drives to integrated Windows servers

Creating and formatting what the integrated server perceives as disk drives for your applications and data involves creating network server storage spaces on i5/OS. For conceptual information about network server storage spaces, see "Disk drives for integrated Windows servers" on page 160. To add an integrated server disk drive (network server storage space), perform these tasks:

1. "Create an integrated server disk drive."
2. "Link a disk drive to an integrated server" on page 165.
3. "Format integrated server disk drives" on page 166.

Create an integrated server disk drive

Creating an integrated server disk drive (network server storage space) is the first step toward adding disk space to an integrated Windows server. The time that you need to create a disk drive is proportional to the size of the drive. After creating the disk drive, you must link (See "Link a disk drive to an integrated server" on page 165) it to the network server description of your integrated server and format it. See "Format integrated server disk drives" on page 166.

To create an integrated server disk drive, follow these steps:

1. In iSeries Navigator, select **Integrated Server Administration**.
2. Right-click the **All Virtual Disks** folder and select **New Disk** or click the appropriate icon on the iSeries Navigator toolbar.
3. Specify a disk drive name and description.
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.
6. Select a disk pool (auxiliary storage pool) to contain the disk.
7. Select the planned file system for the disk.

   Note: When you format the disk from Windows, you can choose a different file system if needed.
8. If you are creating a Windows cluster quorum resource disk, specify the cluster attributes.
9. 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.
10. Click **OK**.

If you want to use the CL command, see CRTNWSSTG.

Notes:

1. To link the new disk drive as a separate operation, see "Link a disk drive to an integrated server" on page 165.
2. Created disks must be partitioned and formatted using Disk Management by Windows or by using the DISKPART command line utility.
3. Creating or starting a server with a disk drive in an independent disk pool (ASP) requires that the disk pool device be available.

Link a disk drive to an integrated server

In order for an integrated Windows server to recognize an integrated server disk drive (network server storage space) as a hard disk drive, you must link the two together. You must create a disk drive before you can link it. See "Create an integrated server disk drive" on page 164. 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. See "Format integrated server disk drives" on page 166.

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 "Start and stop an integrated server" on page 149.
2. In iSeries 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 iSeries 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. If you are not linking a disk drive dynamically, then start your integrated server. See "Start and stop an integrated server" on page 149.

If you want to use the CL command, see ADDNWSSTGL.

If the disk drive is new and has not previously been formatted, refer to "Format integrated server disk drives" on page 166.

Manage disk drives 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.

Format integrated server disk drives

In order to use integrated Windows server disk drives (network server storage spaces), you must format them. Before you can format them, you must first create (see “Create an integrated server disk drive” on page 164) and link (see “Link a disk drive to an integrated server” on page 165) the disk drives, then start the Windows server from i5/OS (see “Start and stop an integrated server” on page 149).

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.

Copy a disk drive

You can create a new integrated Windows server disk drive (network server storage space) by copying data from an existing disk drive.

To copy 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 **New Based On** or click the appropriate icon on the iSeries 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: The DISKPART command line utility can be used 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).

Expand a disk drive

You can expand a virtual disk drive (network server storage space) without copying the disk drive. For information about expanding a boot disk, see “Expand a system drive” on page 168.

Attention:

- For disks that have been changed from basic to dynamic in the Windows operating system, using the DISKPART command line utility after expanding the disk may cause multiple partitions to be created for a volume. This will cause performance degradation on iSCSI attached servers. You should create and link additional disks to extend a spanned volume instead of expanding a dynamic disk and using the DISKPART utility.
- If you use the DISKPART utility, do not change the disk from basic to dynamic to ensure that the volume is contained on a single partition. If you are using dynamic disks, specify sizes that will not cause volumes to be misaligned as listed in the iSCSI Disk I/O section of System i Performance Capabilities Reference .

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 iSeries 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 on-line 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.

Notes:

1. The disk cannot be linked to an active server while it is being expanded. If the server supports dynamic unlinking of disk drives, then the above procedure can be performed while the server is active. In this case, the disk is dynamically unlinked, then expanded and then dynamically relinked to the server again. Therefore, the disk is temporarily unavailable to the active server while the disk is being expanded.
2. The DISKPART command line utility can be used to expand an existing partition in order to utilize any additional free space.

   Note: DISKPART is available by default on Windows Server 2003. It can also be downloaded from the Microsoft web page (www.microsoft.com). Refer to the Microsoft Knowledge base articles for DISKPART for details and limitations.
3. Expansion of an existing network server storage space has some limitations depending on how the storage space was originally allocated.

If you want to use the CL command, see Change Network Storage Space (CHGNWSSTG). Note that when using CHGNWSSTG to expand the disk, the disk cannot be linked to an active server. CHGNWSSTG will not automatically unlink and relink the disk if the server is active.

Expand a system drive

Attention:

1. You should back up your system drive before you expand it. See the Microsoft web page (www.microsoft.com) for more information about using the DISKPART utility.
2. Using the DISKPART command line utility on disks that have been changed from basic to dynamic in Windows may cause multiple partitions to be created for a volume which will cause performance degradation on iSCSI attached servers. To ensure the system drive is contained on a single partition, do not change the system drive from basic to dynamic. If using dynamic disks, specify sizes that will not cause the system drive to be misaligned as listed in the iSCSI Disk I/O section of System i Performance Capabilities Reference

To expand a system drive, do the following steps.

1. Shut down the server. See "Start and stop an integrated server" on page 149.
2. Unlink the system drive disk from the server. See "Unlink integrated Windows server disk drives."
3. Change the size of the disk. See "Expand a disk drive" on page 167.
4. Link the disk to a temporary server network server description as a data disk. See "Link a disk drive to an integrated server" on page 165.
5. Start the temporary server. See "Start and stop an integrated server" on page 149.
6. On the temporary server Windows console, extend the partition of the disk using the DISKPART utility.
7. Shut down the temporary server. See "Start and stop an integrated server" on page 149.
8. Unlink the disk from the temporary server. See "Unlink integrated Windows server disk drives."
9. Link the expanded disk to the original server as the system disk. See "Link a disk drive to an integrated server" on page 165.
10. Start the original server. See "Start and stop an integrated server" on page 149.

Unlink integrated Windows server disk drives

Unlinking integrated server disk drives (network server storage spaces) disconnects them from the integrated server, making them inaccessible to users. For information about when drives can be dynamically unlinked, see "Disk drives for integrated Windows servers" on page 160.

To unlink a disk drive, follow these steps:

1. If you are not unlinking a disk drive dynamically, shut down your integrated server. See "Start and stop an integrated server" on page 149.
2. In iSeries Navigator, select **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.
3. Right-click the disk drive to be unlinked and select **Remove Link**, or select the drive and click the appropriate icon on the iSeries Navigator toolbar.
4. **Optional:** To change the sequence of the drives, click **Compress link sequence**.
5. Click **Remove**.

If you want to use the CL command, see Remove Server Storage Link RMVNWSSTGL.

Delete integrated Windows server disk drives

Deleting a disk drive (network server storage space) destroys the data on the disk drive and frees the iSeries disk storage so that it can be used for other purposes.

Before you can delete a disk drive, you must unlink it from the integrated server. See "Unlink integrated Windows server disk drives" on page 168. Once you have unlinked it, you can delete it.

To delete the disk drive, follow these steps:

1. In iSeries 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 **Delete** or click the appropriate icon on the iSeries Navigator toolbar.
4. Click **Delete** on the confirmation panel.

If you want to use the CL command, see Delete NWS Storage Space DLTNWSSTG.

Delete disk drives when removing an integrated server

When you manually remove an integrated server, you need to delete the disk drives (network server storage spaces) that are associated with the network server description (NWSD) for that server. Also delete user-created disk drives that you own.

The Delete Windows Server (DLTWNTSVR) command is provided to remove objects created by the Install Windows server (INSWNTSVR) command. It removes the network server description (NWSD), line descriptions (LIND), storage spaces (NWSSTG), TCP interfaces, controller descriptions (CTLD), and device descriptions (DEVD). This is the recommended way to permanently remove an integrated server from the system.

You also need to delete any disk drives that i5/OS predefined as the system drive and installation drive for your server.

To find out what disk drives are associated with your server, see the topic "Obtain information about integrated server disk drives" on page 163

Use Windows disk management programs with integrated Windows servers

You can use the Windows Disk Management program to administer your disk drives (network server storage spaces), just as if they were individual physical disk drives. Features such as assigning drive letters, partitioning, and volume set creation are fully functional.

When using Windows disk management programs, consider the following:

- When you link disk drives, you can assign relative sequence positions for the drives or have i5/OS do it automatically.
- Unless you use Windows Disk Management to assign the optical drive letter, the optical drive appears as the next available drive letter after all disk drives on the integrated server. If no user-defined disk drives are linked to your NWSD, the optical drive typically appears as drive E.

Chapter 10. Share devices

One advantage integrated Windows servers have is the ability to use iSeries devices. You can use iSeries optical drives, tape drives, and printers from your Windows server.

Accessing iSeries devices includes these tasks:

- i5/OS and Windows server refer to devices by different names, so you first need to learn the appropriate device descriptions and hardware resource names you plan to use. See “Determine the device description and hardware resource names for iSeries devices.”
- To use an optical drive on an integrated server, vary it on from i5/OS. See “Use iSeries optical drives with integrated Windows servers.”
- See this topic: “Use iSeries tape drives with integrated Windows servers” on page 172 for information about allocating drives to integrated Windows servers, formatting tapes, transferring drives between servers, and transferring drives back to i5/OS.
- Read this topic: “Print from an integrated Windows server to iSeries printers” on page 176.

Determine the device description and hardware resource names for iSeries devices

When you refer to iSeries devices on i5/OS, you need to use their device description name. When you refer to those devices from an integrated Windows server, you need to use their hardware resource name. If the names are different and you use the wrong name, you get the wrong device.

To determine the hardware resource name and see whether it is the same as the device description name, follow these steps:

1. On the i5/OS command line, type `DSPDEVD` *`device_description_name`* and press Enter.
2. The `Resource name` field has the hardware resource name for this device. Check to see if it has the same name as the `Device description` field. If the names are different, you must remember to use the appropriate name depending on whether you are working from the integrated Windows server or from i5/OS.

   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. IBM Integrated Server Support does not support tape libraries. Therefore, if your device has a tape library description, both the tape device and tape library device must be in a varied off state before locking the device on the Windows server.

Use iSeries optical drives with integrated Windows servers

Windows server can use an iSeries optical drive just as it does a local optical drive. The iSeries optical drive appears as a normal local optical drive in the **My Computer** folder on Windows server.

If you have logical partitions on your iSeries, 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.

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. At the i5/OS command line, type `WRKCFGSTS *DEV *OPT` and press Enter.
2. In the `Opt` column next to the correct optical device, typically OPT01, type 1 to vary on the optical drive.

3. Press Enter and the optical drive varies on.

To lock an optical drive, follow the steps below:

1. Click **Start**, then **Programs,** then **IBM iSeries,** then **IBM iSeries Integrated Server Support.**
2. Expand **IBM iSeries 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 iSeries optical drive from an integrated Windows server, see "Optical device problems" on page 210.

| **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

Return control of an optical device from an integrated server to iSeries

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 iSeries optical drive from an integrated server to iSeries, follow these steps:

1. Click **Start,** then **Programs,** then **IBM iSeries,** then **IBM iSeries Integrated Server Support**.
2. Expand **IBM iSeries Integrated Server Support**.
3. Expand the network server description name.
4. Select **iSeries Devices**.
5. Select the device that you want to unlock.
6. Right-click and select **All Tasks,** then **Unlock Device**.

Use iSeries tape drives with integrated Windows servers

iSeries 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 "Supported iSeries tape drives" on page 175.

Because multiple integrated servers in the same iSeries system 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 iSeries, the tape drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions.

To use an iSeries tape drive from an integrated server you must perform the following tasks:

- "Format a tape on i5/OS for use with integrated Windows servers" on page 173.
- Allocate an iSeries tape drive to an integrated server by varying off the tape drive from i5/OS and locking it on the integrated server. See "Allocate the iSeries tape drive to an integrated Windows server" on page 173.

- Transfer control of an iSeries tape drive to a different integrated server. See “Transfer control of the iSeries tape and optical drives between integrated Windows servers” on page 175.
- Return control a tape drive from an integrated server so that i5/OS can use it. Ensure that you have a correctly formatted tape. See “Return control of a tape drive from an integrated Windows server to the iSeries” on page 174.

If you have problems with an iSeries tape drive, see “Tape problems” on page 210.

Install tape device drivers

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 xSeries servers. 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 iSeries integrated xSeries solutions web site (www.ibm.com/systems/i/bladecenter/windows/tape_driver_migration.html).

Format a tape on i5/OS for use with integrated Windows servers

To use iSeries tape drives with integrated Windows servers, you must use a tape format that they recognize. To produce a non-labeled tape acceptable to Windows, use the i5/OS Initialize tape (INZTAP) command.

To format a tape, do the following steps:

- Put the tape you want to use in the iSeries tape drive.
- At the i5/OS command line, type:

  ```
  INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)
  CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
  ```

  where *tap01* is the name of your tape drive. Press Enter.

Allocate the iSeries tape drive to an integrated Windows server

To use an iSeries tape drive from the integrated Windows server console, you must vary it off on i5/OS and lock it onto the integrated server. You must lock the device before starting applications or their services.

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. IBM iSeries 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 iSeries tape drive to an integrated server, follow these steps:

1. Vary off the tape drive on i5/OS:
   - To do this from iSeries 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 iSeries Integrated Server Support**.
   b. Expand **IBM iSeries Integrated Server Support**.
   c. Expand the network server description name.
   d. Select **iSeries Devices**.
   e. Select the tape object that you want to lock.
   f. Right-click and select **All Tasks, Lock Device.**
3. If you need other information about the tape device to enable an application to recognize it, see "Identify iSeries tape devices for applications" on page 175. If you have problems, see "Tape problems" on page 210.

Return control of a tape drive from an integrated Windows server to the iSeries

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 an iSeries tape drive from an integrated Windows server to iSeries, follow these steps:

1. Unlock the tape device from the integrated Windows server console.
   a. Click **Start,** then **Programs,** then **IBM iSeries,** then **IBM iSeries Integrated Server Support**
   b. Expand **IBM iSeries Integrated Server Support**
   c. Expand the network server description name.
   d. Select **iSeries 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 iSeries 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. At the i5/OS command line, 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 and the tape drive varies on.
     d. Change the tape to one formatted for i5/OS.

Supported iSeries tape drives

Your ability to use iSeries tape drives from integrated Windows servers depends on tape device model, tape controller, and media type.

Refer to the Integrated xSeries Solutions web site to see which tape devices are supported.

Tape libraries are not supported as libraries, but they may be supported as single devices.

Manual and automatic modes are both supported on Auto Cartridge Facilities (ACF) and Auto Cartridge Loaders (ACL). If the ACL or ACF is in automatic mode the next tape will be loaded automatically if the backup application ejects the full tape. The Windows Backup Utility does this automatically with no user intervention. Veritas Backup Exec displays a dialog box that displays the following ″Please remove the media from the drive, and respond OK.″ Clicking **Respond OK** in this dialog box causes the backup to continue normally.

Identify iSeries tape devices for applications

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 iSeries 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.

Transfer control of the iSeries tape and optical drives between integrated Windows servers

If you have multiple integrated servers only one at a time can use the iSeries tape or optical drive. 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 iSeries, 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 iSeries tape or optical drive between integrated servers, follow these steps:

On the integrated sever console that has control of the drive:

1. Click **Start,** then **Programs,** then **IBM iSeries**, then **IBM iSeries Integrated Server Support**

2. Expand **IBM iSeries Integrated Server Support**
3. Expand the network server description name.
4. Select **iSeries 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 iSeries**, then **IBM iSeries Integrated Server Support**
2. Expand **IBM iSeries Integrated Server Support**
3. Expand the **Network Server Description** name
4. Select **iSeries Devices**
5. Select the device that you want to lock.
6. Select **Action,** then **All Tasks,** then **Lock Device**.

Print from an integrated Windows server to iSeries printers

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 i5/OS printers, perform these tasks:

1. Set up the i5/OS printer for TCP/IP printing. For more information, see TCP/IP Configuration and Reference .
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.

Chapter 11. Administer integrated Windows server users from i5/OS

One of the main advantages of Windows environment on iSeries 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 log onto i5/OS. If they change their i5/OS password, their Windows password changes as well.

For conceptual information, read the article: “User and group concepts” on page 51.

Here are some tasks you can perform:

- “Enroll a single i5/OS user to the Windows environment using iSeries Navigator”
- “Enroll an i5/OS group to the Windows environment using iSeries Navigator” on page 178
- “Enroll i5/OS users to the Windows environment using the character-based interface” on page 178
- “Create user templates” on page 178
- “Specify a home directory in a template” on page 179
- “Changing the LCLPWDMGT user profile attribute” on page 180
- “Enterprise Identity Mapping (EIM)” on page 180
- “End user enrollment to the Windows environment” on page 182
- “End group enrollment to the Windows environment” on page 182
- “The QAS400NT user” on page 183
- “Preventing enrollment and propagation to an integrated Windows server” on page 185

Enroll a single i5/OS user to the Windows environment using iSeries Navigator

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 iSeries Security Reference .

To enroll a single user to the Windows environment, follow these steps:

1. In iSeries Navigator, expand **Integrated Server Administration—>Servers** or **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 “Failures enrolling users and groups” on page 216.

Enroll an i5/OS group to the Windows environment using iSeries Navigator

This procedure enrolls all users in the i5/OS group to the Windows environment. You can find information about creating i5/OS user and group profiles in the iSeries Security Reference .

To enroll an i5/OS group and its members to the Windows environment, 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 “Failures enrolling users and groups” on page 216.

Enroll i5/OS users to the Windows environment using the character-based interface

Enroll users to the Windows environment

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 of relevant CL commands

Table 5.

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.

Create user templates

A user enrollment template is a tool to help you enroll users from i5/OS to the Windows environment more efficiently. Rather than manually configuring many new users, each with identical settings, use a user enrollment template to automatically configure them. You can learn more about user enrollment templates at User Enrollment Templates.

Follow these steps to create a Windows template:

For a Windows 2000 Server or Windows Server 2003 domain:

1. At the integrated server console 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.

For a Windows 2000 Server or Windows Server 2003 server:

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. 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.

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.

Specify a home directory in a template

To allow Windows environment on iSeries 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 server 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: `\\iSeriesWin\homedirs\%username%`. In this example, **iSeriesWin** 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

This article explains how to change the Local Password Management (LCLPWDMGT) user profile attribute. To read about the LCLPWDMGT attribute see "User and group concepts" on page 51 and "Types of user configurations" on page 53.

Follow this procedure in the i5/OS *character-based environment* to change the 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.

Enterprise Identity Mapping (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 Information Center has an entire topic devoted to EIM. See Enterprise Identity Mapping.

To learn the features of the different ways to enroll users to the Windows environment, see "Types of user configurations" on page 53.

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. With Windows environment on iSeries, 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.

End user enrollment to the Windows environment

To end the enrollment of a user to Windows environment 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 Windows environment

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.

End group enrollment to the Windows environment

When you end enrollment of a group to the Windows environment, 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 Windows environment.

However, if the group has any members that were added from the Windows environment 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 environment domains and servers, follow these steps in iSeries 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.

The QAS400NT user

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 the following cases:

- 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, as is discussed in the section "Specify a home directory in a template" on page 179).
- 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. See "Password considerations" on page 55.
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 iSeries Navigator or the CHGNWSUSRA command. Refer to: "Enroll a single i5/OS user to the Windows environment using iSeries Navigator" on page 177, for a description of how to do this. Do not try to use a template when enrolling QAS400NT.

4. Use iSeries 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. Refer to “Preventing enrollment and propagation to an integrated Windows server,” for a description of how to do this.

- 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. Refer to “Preventing enrollment and propagation to an integrated Windows server,” for a description of how to do this.

Preventing enrollment and propagation 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.

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, proceed as follows:

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)`

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 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.

Chapter 12. Back up and recover integrated Windows servers

Because Windows environment on iSeries combines two operating systems (Windows 2000 Server or Windows Server 2003 with i5/OS), 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 iSeries, you have these basic options:

- Do a full system backup on your i5/OS. See the topic Back up your server.
- Back up the network server description (NWSD) and the disk drives that are associated with the integrated server on iSeries. See “Back up the NWSD and other objects associated with an integrated Windows server.”
- Back up individual integrated server files by using the i5/OS SAV and RST commands and i5/OS NetServer or a backup utility. See “Back up individual integrated Windows server files and directories” on page 192.

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, refer to the book Backup and Recovery .
- If you need to restore a network server description and its associated i5/OS disk drives, refer to “Restore an integrated Windows server’s NWSD and disk drives” on page 196.
- To restore integrated server data (files, directories, shares, and the Windows registry) that you backed up with the Save (SAV) command, see “Recover integrated Windows server files” on page 199.
- To restore files that you saved with Windows backup utilities or other utilities, use those utilities.

Back up the NWSD and other objects associated with an integrated Windows server

When you install an integrated server, i5/OS creates a network server description and predefined disk drives for your server that you need to back up. See “Predefined disk drives for integrated Windows servers” on page 162. Some of the disk drives are system-related (the installation and system drives); others are user-related. Because Windows server considers them a unified system, you need to save all the disk drives and the network server description to restore properly.

The Microsoft Windows operating system and the files that are required to start the integrated server are located on the C and D drives of the server. Windows environment on iSeries allows you to save and restore these drives as i5/OS network server storage space objects. These objects are saved as part of the i5/OS system when you perform a full i5/OS system backup. You can also specifically save the network server description and associated storage spaces. Daily backup of the system drive is a good idea.

Saving storage spaces is the fastest but least flexible method for backing up your integrated server because you cannot restore individual files. Alternatively, you can back up specific individual files and directories to eliminate the BOOT disk, RDISK, and registry backups that you would take with a PC-based Windows server. See “Back up individual integrated Windows server files and directories” on page 192.

To back up the network server description and the disk drives that are associated with integrated servers, see these topics:

- “Back up the NWSD of an integrated Windows server” on page 188.
- “Back up iSCSI NWSCFGs and validation lists” on page 188

- “Back up predefined disk drives for integrated Windows servers.”
- “Back up user-defined disk drives for an integrated Windows server” on page 189.
- “Save and restore user enrollment information” on page 190.
- You can see a table of user objects and system objects that you “What objects to save and their location on i5/OS” on page 190.

Back up the NWSD of an integrated Windows server

When you save the storage space objects that are associated with an integrated Windows server, you also need to save the Network Server Description (NWSD). Otherwise, Windows server may not be able to re-establish items such as Windows server File System permissions. 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.

Note: The Save Configuration (SAVCFG) command will save the objects associated with an NWSD.

Back up the NWSH of an iSCSI attached integrated Windows server

To save an NWSH, 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 NWSH configuration.

Back 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. If default names were used, specify the generic name `nwsdname*`.
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`.

Back up predefined disk drives for integrated Windows servers

When you install an integrated server, i5/OS creates the system and installation source (C and D) drives as predefined drives that you need to save. See “Predefined disk drives for integrated Windows servers” on page 162.

Notes:

1. Treat a Windows network server description, its predefined disk drives, and any user-defined disk drives linked to it 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 may not be able to reestablish items such as Windows server File System permissions.
2. If the server was created on a pre-V4R5 OS/400 system, see Back up predefined disk drives for integrated Windows servers created on pre-V4R5 OS/400 systems in the V5R3 iSeries Information Center.

To save disk drives (network server storage spaces) that are in the system disk pool (ASP) on i5/OS, do this:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
2. Shut down the integrated server to prevent users from updating files during the backup. See “Start and stop an integrated server” on page 149.
3. On the i5/OS command line, type `SAV` and press F4.
4. If you are saving the storage space to tape, specify the name of your tape device (for example, `/QSYS.LIB/TAP01.DEVD`) in the *Device* field.

   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.
5. In the `Name` field under `Objects:`, specify ’`/QFPNWSSTG/stgspc`’, where `stgspc` is the name of the network server storage space.
   - For the system (C) drive, use `/QFPNWSSTG/`*`nwsdname`*`1`.
   - To save the D drive, use `/QFPNWSSTG/`*`nwsdname`*`2`.
   - For storage spaces created in a user disk pool, use `/QFPNWSSTG/stgspc` and also `dev/QASPnn/stgspc.UDFS`, where `stgspc`is the name of the network server storage space and `nn`is the number of the user disk pool.
   - For an independent disk pool, use `/QFPNWSSTG/stgspc` and also `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.
6. Specify values for any other parameters that you want and press Enter to save the storage space.
7. Then, start the integrated server. See “Start and stop an integrated server” on page 149.

You can read more here: “What objects to save and their location on i5/OS” on page 190.

Back up user-defined disk drives for an integrated Windows server

The disk drives that you create for your integrated servers are in the integrated file system. To save these storage spaces from the user disk pool (ASP) on i5/OS, you use the Save (SAV) command.

Note: Treat a network server description (NWSD), its predefined disk drives, and any user-defined disk drives linked to it as a unit. Save and restore them at the same time. They constitute a full system and should be treated as such. Otherwise, the integrated server may not be able to re-establish items such as Windows server File System permissions.

To save disk drives in a user disk pool (ASP) on i5/OS, do this:

1. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
2. For network server storages spaces created in an independent disk pool, verify that the auxiliary storage pool (ASP) device is varied on before saving the ’dev/independent ASP name/stgspc.UDFS’ object.
3. Shut down the integrated server by varying off the network server description to prevent users from updating files during the backup. See “Start and stop an integrated server” on page 149.

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, `/QSYS.LIB/TAP01.DEVD`) in the *Device* field.

   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.) Otherwise, use the name of your device (for example, `/QSYS.LIB/TAP01.DEVD`).
6. In the *Name* field under `Objects:`, specify ’`/QFPNWSSTG/stgspc`’ and also ’`dev/QASPnn/stgspc.UDFS`’, where `stgspc` is the name of the network server storage space and *xx* is the number of the disk pool.
   - For storage spaces created in a user disk pool, use `/QFPNWSSTG/stgspc`and also `dev/QASPnn/stgspc.UDFS`, where `stgspc`is the name of the network server storage space and *xx* is the number of the user disk pool.
   - For an independent disk pool, use `/QFPNWSSTG/stgspc` and also `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 save the storage space.
8. Start the Windows server. See “Start and stop an integrated server” on page 149.

You can find more information about backing up system objects and the appropriate save commands in Backup, recovery, and availability.

The method that is described above allows you to back up and recover entire network server storage spaces. To back up and recover individual files, you can use the new function: “Back up individual integrated Windows server files and directories” on page 192.

Save and restore user enrollment information

In some situations, you may need to restore user profiles and their enrollment information. The following information describes the i5/OS commands and API to save and restore user profiles used for integrated Windows server enrollment. More i5/OS backup and recovery security information may be found in the Backup and Recovery of Security Information section in the iSeries Security Reference .

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 iSeries 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

Many objects are created as a result of installing Windows environment for iSeries. 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. See “Back up individual integrated Windows server files and directories” on page 192.

Objects to save

Object content	Object name	Object location	Object type	Save command
Integrated server boot and system drive	nwsdname1	/QFPNWSSTG	Predefined network server storage spaces in system disk pool (ASP)	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname1') DEV('/QSYS.LIB/*TAP01*.DEVD')
Integrated server boot and system drive	nwsdname1	/QFPNWSSTG	Predefined network server storage spaces in user disk pool	GO SAVE, option 21 or 23 SAV OBJ(('/QFPNWSSTG/nwsdname1') ('/dev/QASPnn/nwsdname1.UDFS')) DEV('/QSYS.LIB/*TAP01*.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage space in system disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/nwsdname2') DEV('/QSYS.LIB/*TAP01*.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage spaces in user disk pool	GO SAVE, option 21 or 23 SAV OBJ(('/QFPNWSSTG/nwsdname2') ('/dev/QASPnn/nwsdname2.UDFS')) DEV('/QSYS.LIB/*TAP01*.DEVD')
Integrated server installation source drive	nwsdname2	/QFPNWSSTG	Predefined network server storage spaces in an independent disk pool (ASP)	GO SAVE, option 21 or 23 SAV OBJ(('/QFPNWSSTG/nwsdname2') ('/dev/independent ASP name/nwsdname2.UDFS')) DEV('/QSYS.LIB/*TAP01*.DEVD')
User data and applications	Various	/QFPNWSSTG	User-defined network server storage spaces in system disk pool	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/*TAP01*.DEVD')
User data and applications	Various	/QFPNWSSTG	User-defined network server storage spaces in user disk pool	GO SAVE, option 21 or 23 SAV OBJ(('/QFPNWSSTG/stgspc') ('/dev/QASPnn/stgspc.UDFS')) DEV('/QSYS.LIB/*TAP01*.DEVD')
User data and applications	Various	/QFPNWSSTG	User defined network server storage spaces in an independent disk pool	GO SAVE, option 21 or 23 SAV OBJ(('/QFPNWSSTG/stgspc') ('/dev/independent ASP name/stgspc.UDFS')) 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(5722SS1) 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	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
i5/OS TCP interfaces	QATOCLIFC	QUSRSYS	logical file	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
iSCSI NWSCFG and associated validation list	Various	QUSRSYS	Network Server Configuration and associated values	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDL)
iSCSI path certificate store	nwsdname.*	/QIBM/UserData/NWSDCert	Certificate store file	GO SAVE, option 21 or 23 SAV OBJ('/QIBM/UserData/NWSDCert/nwsdname.*')

Object content	Object name	Object location	Object type	Save command
iSCSI service processor certificate store	nwscfgname.kdb	/QIBM/UserData/Director /classes/com/ibm /sysmgt/app/iide	Certificate store file. Save if security initialization method is 'automatically generate certificate'.	GO SAVE, option 21 or 23 SAV OBJ('/QIBM/UserData/Director/classes/com/ibm/sysmgt /app/iide/nwscfgname.kdb')

Note: For integrated Windows servers created on pre-V4R5 systems, see What objects to save and their location on OS/400 in the V5R3 iSeries Information Center.

Back up individual integrated Windows server files and directories

IBM iSeries 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 "Back up the NWSD and other objects associated with an integrated Windows server" on page 187.

For information about the file-level backup function, see these topics:

- First read "File-level backup restrictions."
- To do file-level backup of your integrated server, you must first refer to: "Preliminary administrator setup tasks" on page 193.
- "Save your files" on page 195

You can also use a utility such as the Backup program that comes with Windows (see "Windows Backup utility" on page 196). 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.

File-level backup restrictions

When you use the file-level backup, you need to be aware of the following limitations and restrictions:

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 iSeries 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 iSeries 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 applicatiosns 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 iSeries operation through an EIM enabled application (like iSeries Navigator single-signon). See "SBMNWSCMD and file level backup support for Kerberos v5 and EIM" on page 155 for more information.

Requirements:

- The integrated server must be active and have a working TCP/IP point to point virtual Ethernet connection with i5/OS. 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 userID and password on the integrated server and i5/OS.
- 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 iSeries NetServer to locate servers in the domain. You need to have the iSeries NetServer in the same domain (see "Ensure iSeries NetServer and the integrated Windows server are in same domain" on page 194) 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.

Preliminary administrator setup tasks

Before you can back up your integrated Windows server files at file-level, you must do some preliminary setup tasks:

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 "Enroll a single i5/OS user to the Windows environment using iSeries Navigator" on page 177. Also ensure that the user is a member of the Administrators group. Refer to "Create user templates" on page 178.
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 iSeries Integrated Server Support accesses the file system and translates these shares into path-names. See "Create 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 "Add members to QAZLCSAVL file" on page 194.
4. Ensure that iSeries NetServer is in the same domain as the integrated server for which you want to save files. See"Ensure iSeries NetServer and the integrated Windows server are in same domain" on page 194.
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 Windows server.

Create shares on integrated Windows servers

To enable file-level backup and restoration of integrated server files on i5/OS, create a share over each directory that contains data you want to save. To create shares on integrated 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.

Add members to QAZLCSAVL file

To enable file-level backup and recovery from i5/OS, add a member for each integrated Windows 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, 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.

Ensure iSeries NetServer and the integrated Windows server are in same domain

To save integrated server files for file-level backup, you must have iSeries NetServer in the same domain as the files you want to save.

1. Check the domain for your integrated server:
   a. In iSeries 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 iSeries NetServer:
   a. In iSeries Navigator, select **Network —>** **Servers —>** **TCP/IP**.
   b. Find iSeries NetServer in the list of TCP/IP servers.
   c. Right-click **iSeries NetServer**, and pick **Properties** (or double-click **iSeries NetServer**, then select **File**, then **Properties**). The domain name for iSeries NetServer appears under the **General** information file tab.
3. If iSeries NetServer is not in the same domain as the integrated server, change the domain for iSeries 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 iSeries NetServer (right-click iSeries NetServer and pick **Stop**, then **Start**.)

Save your files

After you finish the necessary preliminaries (see “Preliminary administrator setup tasks” on page 193), 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 “Start and stop an integrated server” on page 149). 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: How to address parts of an integrated Windows server” 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: How to address parts of an integrated Windows server

These examples show how to refer with the SAV or RST commands to specific parts of an integrated server for a server that is named *server1*:

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)`

To save or restore this:	Specify this:
Only the specific file 'myfile.exe'.	`OBJ('/QNTC/server1/gdrive/myfile.exe')`
The integrated server registry.	`OBJ('/QNTC/server1/$REGISTRY')`

Windows Backup utility

You can use the Windows Backup utility and an iSeries tape drive to do backups from the integrated Windows server. See "Use iSeries tape drives with integrated Windows servers" on page 172.

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 in your Windows server documentation from Microsoft.

Restore an integrated Windows server's NWSD and disk drives

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:

Notes:

1. Treat a network server description (NWSD), its predefined disk drives (see "Predefined disk drives for integrated Windows servers" on page 162), 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 need to relink those disk drives. You can do this by using the Add Network Server Storage Link (ADDNWSSTGL) command for each disk drive that is associated with the NWSD:
   ```
   ADDNWSSTGL NWSSTG(Storage_Name) NWSD(NWSD_Name)
   ```
4. When you restore a domain controller, ensure that the domain database held on the server is synchronized with the other domain controllers. When restoring shared drives used by a Windows cluster node, it may be necessary to manually relink the shared drives. Begin by linking the shared quorum resource drive first. You can use the following command to link the shared quorum resource drive:
   ```
       ADDNWSSTGL NWSSTG(Quorum_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
   ```

   Once the quorum resource has been relinked, the remaining shared drives can then be re-linked as well. Use the following command to relink the remaining shared drives:
   ```
       ADDNWSSTGL NWSSTG(Shared_name) NWSD(NWSD_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*CALC)
   ```

   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 may be restricted. For more information, see "Restore integrated Windows server NWSDs" on page 198.

To restore an integrated server's NWSD and disk drives, refer to these pages:

- “Restore predefined disk drives for integrated Windows servers”
- “Restore user-defined disk drives for integrated Windows servers”
- “Restore integrated Windows server NWSDs” on page 198

Restore predefined disk drives for integrated Windows servers

Disk drives that contain the Windows operating system and registry are in the integrated file system. You restore these predefined disk drives just as you do user-defined disk drives. To restore disk drives in the integrated file system on i5/OS, use the Restore (RST) command:

1. If you are restoring from save media, ensure that you have mounted your media.
2. If there are no network server storage spaces that 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.
3. To restore the storage spaces, type `RST` and press F4.
4. In the `Name` field under `Objects:`, specify `'/QFPNWSSTG/`*`stgspc`*`'` and `'dev/QASP`*`nn`*`/`*`stgspc`*`.UDFS'`, where *`stgspc`* is the name of the network server storage space and *`nn`* is the number of the disk pool.

   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.

   To restore the system (C) drive, use `/QFPNWSSTG/`*`nwsdname`*`1`. To restore the D drive, use `/QFPNWSSTG/`*`nwsdname`*`2`.
5. Specify values for any other parameters that you want and press Enter to restore the storage space.
6. You also need to restore any user defined disk drives that are associated with the server and restore the NWSD. See “Restore user-defined disk drives for integrated Windows servers”. When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Note: If the server was installed before V4R5, see Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems in the V5R3 iSeries Information Center.

Restore user-defined disk drives for integrated Windows servers

Although you can now back up individual files and directories (see “Back up individual integrated Windows server files and directories” on page 192), the fastest way to restore large amounts of data is to restore the entire storage space. If you back up your user storage space from the \QFPNWSSTG directory, you can restore only the entire storage space. See “Back up user-defined disk drives for an integrated Windows server” on page 189. You cannot restore individual files from this backup.

To restore disk drives in the integrated file system, do this:

1. If you are restoring from save media, ensure that you have mounted your media.
2. 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.
3. To restore the storage spaces, type RST and press F4.
4. In the Objects: name field, specify '/QFPNWSSTG/stgspc' and 'dev/QASPnn/stgspc.UDFS', where stgspc is the name of the network server storage space and nn is the number of the disk pool.

   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.
5. Specify values for any other parameters that you want and press Enter to restore the storage space.
6. You also need to restore any predefined disk drives that are associated with the server and restore the NWSD. See "Restore integrated Windows server NWSDs." When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restore integrated Windows server NWSDs

In a disaster recovery situation, you would restore all the configuration objects, one of which is the integrated Windows server's network server description (NWSD). In some situations, for example when you migrate to new Integrated xSeries 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. To restore the NWSD, you use the Restore Configuration (RSTCFG) command:

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 "Start and stop an integrated server" on page 149.

Restore integrated Windows server NWSHs for iSCSI attached servers

In a disaster recovery situation, you would restore all the configuration objects, one of which is the network server host adapter (NWSH). To restore the NWSH, you use the Restore Configuration (RSTCFG) command:

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.

Notes:

1. When you restore an NWSH, it must be started before starting the integrated server.

Restore integrated Windows server NWSCFGs for iSCSI attached servers

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. (If you want to restore multiple NWSCFGs, enter the generic names "nwsdname*". You can also explicitly identify the object names by typing + and press `Enter`.)
   - To restore the default connection security network sever configuration, specify the name of the NWSD followed by CN.
   - To restore the default service processor network sever configuration, specify the name of the NWSD followed by SP.
   - To restore the default remote system network sever configuration, specify the name of the NWSD followed by RM.
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.

Recover integrated Windows server files

IBM iSeries 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: How to address parts of an integrated Windows server" on page 195 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.

Chapter 13. Uninstall the Windows server operating system from the integrated server hardware

You can use the Delete Windows Server (DLTWNTSVR) command to uninstall Windows server from an Integrated xSeries Server. Prior to running the Delete Windows Server command, shut down your integrated Windows server from i5/OS. See "Start and stop an integrated server" on page 149.

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 offline before this command is issued.

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 procedure:

1. Shut down the integrated server, see "Start and stop an integrated server" on page 149.
2. "Unlink integrated Windows server disk drives" on page 168.
3. "Delete integrated Windows server disk drives" on page 168.
4. "Delete an integrated Windows server's NWSD."
5. "Delete an integrated Windows server's line descriptions" on page 202.
6. "Delete TCP/IP interfaces associated with an integrated Windows server" on page 202.
7. "Delete controller descriptions associated with an integrated Windows server" on page 202.
8. "Delete device descriptions associated with an integrated Windows server" on page 203.
9. "Delete network server configurations associated with an iSCSI integrated Windows server" on page 203

If you remove all your Windows and Linux servers that use a particular network server host adapter (NWSH) object from i5/OS and plan not to install any more servers that use the NWSH, you can delete the NWSH. See "Delete a network server host adapter" on page 120.

If you remove all your Windows and Linux servers from i5/OS and plan not to install any more, you can delete IBM iSeries Integrated Server Support to free up the storage the product uses. See "Delete the IBM i5/OS Integrated Server Support, i5/OS option 29 (5722–SS1)" on page 203.

Delete an integrated Windows server's NWSD

Before you delete a network server description (NWSD), you need to unlink its disk drives (see "Unlink integrated Windows server disk drives" on page 168) and delete storage spaces that are associated with that NWSD (see "Delete integrated Windows server disk drives" on page 168). 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.

Delete an integrated Windows server's line descriptions

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.

Delete TCP/IP interfaces associated with 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.

Delete controller descriptions associated with an integrated Windows server

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.

Delete device descriptions associated with an integrated Windows 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.

Delete network server configurations associated with an iSCSI integrated Windows 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**.

Delete the IBM i5/OS Integrated Server Support, i5/OS option 29 (5722–SS1)

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.

Note: Removing the program does not automatically delete existing network server descriptions or user-defined disk drives. However, it does render them unusable. You can find information about deleting network server descriptions and disk drives in Chapter 13, “Uninstall the Windows server operating system from the integrated server hardware,” on page 201.

To delete IBM i5/OS Integrated Server Support, follow these steps:

1. On i5/OS, type the command `GO LICPGM` and press Enter.
2. Choose option `12` from the `Work with Licensed Programs` menu and press Enter.
3. Page down the list of licensed programs until you see the description `Integrated Server Support`

4. Type `4` in the `Option` field to the left of the option. Press Enter, and i5/OS deletes the option.

Chapter 14. Troubleshoot integrated Windows servers

If your integrated server is not functioning properly, follow these steps to attempt to correct the problem:

1. Try restarting the integrated server. See “Start and stop an integrated server” on page 149.
2. Display information about the NWSD and its associated lines, controllers, and devices. See “View or change integrated Windows server configuration information” on page 152.
3. If the problem persists, look for helpful information in the logs. See “Check message and job logs”.
4. Next look for the specific problem in the section “Problems with integrated Windows servers” on page 208.
5. Also check the Informational APARs for the latest tips and service information. You can find these at the System i integration with BladeCenter and System x web site .
6. If the integrated server becomes damaged, you may be able to preserve installed applications and user data by reinstalling it. See “Reinstall an integrated Windows server” on page 238.
7. If you need information about collecting service data to send to support personnel, see “Collect integrated Windows server service data” on page 238.

Other options to resolve problems

If a solution to the problem you are having is not addressed by the troubleshooting sections in this chapter, other service options may help resolve the problem.

- See Troubleshooting on the Integrated xSeries solutions web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).
- For problems with specific applications, contact the application provider for support.
- For Integrated xSeries Server hardware errors or server installation problems, contact IBM Service.
- For unrecoverable server errors (for example, blue screens), you might be able to find additional information on these web sites:
  – Support for the iSeries family (www.ibm.com/servers/eserver/support/iseries/).
  – Microsoft Help and Support (http://support.microsoft.com).

If additional assistance is required, under IBM service contracts, IBM service will assist in determining the correct path for problem resolution. Contact the IBM Support Line for assistance.

Check message and job logs

Information about integrated Windows servers is logged in several places. If you have a problem, this information may help determine its cause.

Monitor job log

The Monitor job log (see the topic “Monitor job” on page 207) contains messages that vary from normal processing events to detailed error messages. To check this log, do this:

1. At the i5/OS command line, use the Work with active job (WRKACTJOB) command and find the job in the QSYSWRK subsystem with the same name as your network server. If the job does not appear on this display, the job has either ended or has not started.
2. If you find the job, use option 5 to work with the job and option 10 to display the job log.
3. Press F10 for detailed messages.

4. If you find useful information in the log, write down the job ID (all three parts: Name, User, and Number). Then print the log with this command: `DSPJOBLOG JOB(number/user/name) OUTPUT(*PRINT)`.

Note: If the problem caused your monitor job to end or you are debugging a problem that happened before the present monitor job, search for a spooled file that contains information in the previous job log. To find spooled files that deal with your network server, use this command: `WRKSPLF SELECT(QSYS *ALL *ALL nwsd_name)`.

QVNAVARY job log

The QVNAVARY job log contains messages that deal with the vary on and vary off of the IXS or IXA attached network server description when you shut down and restart from of the network server description when you shut down and restart from Windows server. To check this log for shutdown and startup errors, do this:

1. At the i5/OS command line, use the Work with active job (WRKACTJOB) command and find the QVNAVARY job in the QSYSWRK subsystem.
2. Use option 5 to work with the job and option 10 to display the job log.

You can also use WRKJOB JOB(QVNAVARY).

For IXS or IXA attached xSeries servers, a batch job using the name BTnwsdname is submitted to perform the vary off and vary on needed to 'reboot' the server.

Identify the qualified name of the job that was submitted in the QVNAVARY joblog. Locate the joblog for the submitted 'reboot' job by fully qualifying the jobname using WRKSPLF SELECT(*ALL) JOB(qualjobname).

List all 'reboot' jobs with WRKSPLF SELECT(*ALL) JOB(BTnwsdname)

Job log of the job that initiated a vary on or off

If a batch job or interactive user initiated a vary on or off of the NWSD from i5/OS, the log for that job might provide helpful information. For example, if you used a VRYCFG or WRKCFGSTS command, you can use the Display job (DSPJOB) command and option 10 to look at the job log.

Server message queue

If during the installation you specified a message queue for your network server, that message queue can provide helpful information.

1. If you need to verify whether you specified a message queue, at the i5/OS command line, type `DSPNWSD NWSD(nwsd_name)` and press Enter. If it is set to `*none`, only serious messages go to the QSYSOPR message queue.
2. If a message queue is specified, use this command on i5/OS to display the messages: `DSPMSG MSGQ(library/queue)`

System operator's message queue

The integrated server updates the system operator's message queue (QSYSOPR) with normal startup and shutdown messages in addition to failure messages. To display these messages from the character-based interface, enter `DSPMSG QSYSOPR`.

Communications message queue

iSCSI attached servers include a communications message queue parameter. If during the installation you specified a communications message queue for your network server, that message queue can provide helpful information about communications status messages.

1. If you need to verify what message queue was specfied, at the i5/OS command line, type DSPNWSD NWSD(nwsd_name) and press Enter. If the communications message queue is set to *SYSOPR, messages go to the QSYSOPR message queue.
2. If a communications message queue is specified, use this command on i5/OS to display the messages: DSPMSG MSGQ(library/queue)

Profile synchronization job log

The profile synchronization job log contains EIM and user profile enrollment messages. To check this log, enter `WRKJOB QPRFSYNCH`.

Monitor job

Every active integrated Windows server has a monitor job that starts when you start the server. The monitor job runs in the QSYSWRK subsystem under the QSYS user profile. The job name is the name of the network server description that it is monitoring.

When the monitor job starts, i5/OS sends an informational message, CPIA41B, to the QSYSOPR message queue. This message contains the job ID of the monitor job. You can use this job ID with the Work with Job (WRKJOB) command to find the monitor job log and other job-related information for the monitor job.

Additional logs and messages for iSCSI attached servers

Network server host adapter job log
Network server host adapters are assigned to specific system jobs by i5/OS. The job log of the system job associated with the Network server host adapter can provide helpful information.

1. To determine the name of the system job at the i5/OS command line, type `DSPDEVD DEVD(nwshname)` and press `Enter`. Page down to the job name values.
2. Use the Display job (DSPJOB) command and select option 10 to look at the job log for the job identified above.

Network server host device message queue
Network server host adapters include a message queue parameter. This message queue can provide helpful information.

1. If you need to determine the message queue that is being used, see “Display network server host adapter properties” on page 118. Click on the **Communications** tab and note the message queue name and library.
2. 2. To display the message queue using iSeries Navigator, do the following steps:
   a. Expand **Basic Operations—> Messages**.
   b. Right-click **Messages** and select **Customize this View—> Include...**
   c. Select the **Message queue** option and fill in the message queue name and library that are shown on the network server host adapter properties panel.

      Note: If “System operator” is shown on the NWSH properties panel, then specify QSYSOPR as the message queue name.

Product Activity Log (PAL)
Some errors related to the iSCSI network, such as CHAP authentication failures, are logged in the PAL. To access the PAL, do the following steps:

1. Run the Start System Service Tools (STRSST) CL command.

2. Select **Start a service tool**
3. Select **Product Activity Log**

Problems with integrated Windows servers

If your integrated Windows server is not working correctly, check to see if your problem fits into this list:

- "STOP or blue screen errors" on page 209
- Problems using Software maintenance program. See "IBM iSeries Integrated Server Support snap-in program" on page 219.
- **Drive problems**
  - "A full integrated server system drive" on page 209
- **Device problems**
  - "Optical device problems" on page 210
  - "Tape problems" on page 210
- **Starting/stopping problems**
  - "Problems starting an integrated Windows server" on page 212
  - "Problems hot sparing between servers" on page 213
  - "NWSD configuration file errors" on page 215
- **Externally attached xSeries servers**
  - "DASD in IXA or iSCSI attached servers" on page 216
- **User and group enrollment problems**
  - "Failures enrolling users and groups" on page 216
  - "User enrollment authorization problems" on page 217
  - "Password problems" on page 218
- **iSCSI attached xSeries or IBM BladeCenter servers**
  - "Problems with iSCSI attached servers" on page 220
  - "Boot and storage path network analysis" on page 221
  - "Managing path certificates" on page 222
  - "IBM Director Troubleshooting" on page 222
    - "Discovery problems" on page 223
    - "Problems with SSL connections" on page 224
  - "Virtual Ethernet problems with iSCSI attached servers" on page 225
- **Networking problems**
  - "Virtual Ethernet problems with IXS and IXA attached servers" on page 227
  - "Problems with external networks" on page 230
  - "Manually update LAN drivers on the integrated Windows server" on page 231
  - "Point to point virtual Ethernet IP address conflicts" on page 233
  - "IFS access problems" on page 235
  - "Problems with TCP/IP over virtual Ethernet" on page 234
  - "Problems accessing Windows Server 2003 shares using the QNTC file system" on page 235
- "Problems sharing hosted system hardware" on page 214
- "Problems with saving integrated Windows server files" on page 236
- "Unreadable messages in the server message queue" on page 237
- "Problems getting a Windows system memory dump" on page 237

If the above topics do not address the problem you are investigating, refer to the integrated xSeries solutions web site Troubleshooting page at http://www.ibm.com/systems/i/bladecenter/troubleshooting.html. This web page references additional sources of troubleshooting information.

STOP or blue screen errors

When you get blue screen errors, take the following actions to try to determine the cause of the errors and how to correct the errors:

1. On the i5/OS command line, type `DSPMSG QSYSOPR`.
2. Press Enter. The QSYSOPR message queue appears.
3. Look through the messages for any that may help you determine what caused the blue screen.
4. Restart the integrated server by varying it off, then back on, from i5/OS (see “Start and stop an integrated server” on page 149).
5. Inspect the Event log on Windows for errors, type of stop code, and other diagnostic information.
6. Check for PAL entries and VLOGs
7. If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.
8. For iSCSI attached servers, see iSCSI troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

A full integrated server system drive

The system drive contains the Windows server operating system and may contain applications and data as well. If this drive fills up, it can cause such errors as full drive messages and paging file errors.

To keep the system drive from filling up, take one or more of these steps:

- Increase the size of the system drive during the installation of Windows server.
- When you install applications, install them on a user-defined storage space instead of taking the default of installing them to your system drive.
- Move your Windows server paging file to a user-defined storage space instead of defaulting to the system drive. If you move your paging file, you will not be able to collect a system-memory dump if a STOP error or blue screen occurs. However, if you want to do this, follow these steps:
  1. Right-click the **My Computer** icon and select **Properties**.
  2. Select the **Advanced** tab.
  3. Click the **Performance** options button.
  4. Click the **Change** button for **Virtual Memory**.
  5. Select a user-defined storage space that has the amount of free space that you need.
  6. Click **OK**.
- Move your Windows server memory dump to a user-defined storage space instead of defaulting to the system drive. To do this, follow these steps:
  1. Go to **Start**, then **Settings**, then **Control Panel**.
  2. Click the **Startup/Shutdown** tab.
  3. Select the **Write debugging information to** box in the **Recovery** section of the panel.
  4. Select a user-defined storage space that has enough free space (about 12 MB larger than your RAM size). Refer to the Windows documentation for additional recommendations and requirements for page size.
  5. Click **OK**.

Note: If you move your Windows server memory dump to a user-defined space, you will have to copy the dump file to tape to send it to technical support.

- If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

Optical device problems

If the i5/OS optical device does not work with an integrated Windows server, take these actions:

1. Make sure that you have varied on the optical device on i5/OS. Find out how to vary on the optical device in “Use iSeries optical drives with integrated Windows servers” on page 171.
2. Make sure the optical drive is allocated to the integrated server.
3. Make sure that there is optical media in the drive.
4. If your system has logical partitions, make sure that you have allocated the optical device to the same partition as the integrated server.
5. Look in the event log for optical device errors.
6. Make sure that the optical device shows up in **My Computer** on the integrated Windows server.
7. Recovery steps for optical devices:
   a. Close the IBM iSeries Integrated Server Support snap-in program
   b. Vary off the optical device on the iSeries
   c. Vary the optical device on
   d. Reallocate the device to the integrated server
8. If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page .
9. If you cannot find the solution there, contact your technical support provider.

If an integrated server fails before unlocking an optical device, the device will be unavailable to i5/OS or to other integrated servers. For more information, see “Locked optical device for a failed server.”

Locked optical device for a failed server

If the integrated server fails before unlocking an optical device (or varying off the server), the optical device will be unavailable to i5/OS or other Windows Servers. You will need to vary off the optical device using WRKCFGSTS *DEV *OPT and vary it back on to free the lock.

Tape problems

If the iSeries tape drive does not work with an integrated Windows server, take these actions:

1. Verify that you have varied off the tape drive on i5/OS and locked it on an integrated server. See “Allocate the iSeries tape drive to an integrated Windows server” on page 173. Devices may fail to lock for one of these reasons:
   - The tape device or its tape library is varied on.
   - The device driver is not loaded.
   - The tape device is not supported.
   - If you have problems with locking the device, verify that the device driver is loaded on the integrated server. This typically happens automatically. See “Verify that the tape drive device driver is loaded” on page 211.
   - Verify that your tape drive is supported. See “Supported iSeries tape drives” on page 175.
2. More advanced applications might lock devices to services that continue after the application interface is dismissed. This prevents other applications from being able to use the device. These services may restart automatically after a system restart, locking the device to the application. To see services of an application (such as Seagate and Computer Associates), do this:

   a. Click on **Start**, **Programs**, **Administrative Tools**, then **Component Services.**
   b. Double-click **Services.**
   c. If necessary, you can stop services from the **Services** window.
3. You may have multiple integrated servers. If so, verify that the tape drive is unlocked on all of them except the one on which you want to use it. See "Transfer control of the iSeries tape and optical drives between integrated Windows servers" on page 175.
4. If your system has logical partitions, ensure that you allocated the tape drive to the same partition as the integrated server.
5. Verify that the drive contains a properly formatted tape. See "Format a tape on i5/OS for use with integrated Windows servers" on page 173.
6. Verify that the drive is not on the list of restricted devices on i5/OS by using the Display NWSD command (DSPNWSD).
7. Look in the event log for tape errors.
8. See if the tape device shows up in the Device List:
   a. Click on **Start**, **Programs**, **Administrative Tools**, then **Computer Management**.
   b. Select **System Tools**, then **Device Manager**.
   c. Verify that the tape drive shows up in **Device List**.
9. If the problem still persists, check the technical information databases at the IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

Verify that the tape drive device driver is loaded

Before applications running on an integrated server can use the iSeries tape drive, the device driver must be loaded on the integrated server. This is typically automatic. For more information about supported tape drives, see "Supported iSeries tape drives" on page 175.

To ensure that the tape device driver is loaded, follow these steps.

1. On the Windows server task bar, click **Start**, then **Programs**, then **Administrative Tools.**
2. Click **Computer Management**, then **System Tools**, then **Device Manager**.
3. Expand the icon with your computer's name on it. If a tape device is loaded, a Tape Device icon appears.
4. Expand the **Tape device** icon to see the loaded tape device drivers.

If you have an IBM iSeries Tape Drive that does not require a third party driver and need to manually load device drivers, complete these steps at the integrated server console.

1. Click on **Start**, then **Settings**, then **Control Panel**.
2. Click on **Add/Remove Hardware**.
3. On the Add/Remove Hardware Wizard, click **Next**.
4. Select **Add/Troubleshoot a device** and click **Next**.
5. On the **Choose a Hardware Device** section of the Add/Remove Hardware Wizard window, choose **Add a new device** and click **Next**.
6. From the **Find New Hardware** section of the Add/Remove Hardware Wizard window, choose ″No, I want to select the hardware from a list,″ and click **Next**.
7. On the Hardware Type section, scroll down the combo box to **Tape drives**, select it, and click **Next**.
8. In the Manufacturers pane of the Select a Device Driver section, select **IBM**. In the Models pane, select **IBM iSeries Tape Drive** and click **Next**.
9. Click **Next** on the ″IBM iSeries Tape Drive″ section of this window.
10. If the ″Files Needed″ box appears, enter `%SystemRoot%\System32\drivers`, where C: is your system drive, into the ″Copy files from″ box. Click **OK**.

11. On the "Completing the Add/Remove Hardware Wizard" section of the Add/Remove Hardware Wizard window, click **Finish**. All the tape devices should load.
12. After restarting your computer, repeat steps 1 – 4 to confirm that your devices are loaded.

For information about loading other tape device drivers, see "Install tape device drivers" on page 173.

Problems starting an integrated Windows server

If your integrated server will not start, perform these steps to determine the problem.

1. Check the status of the server. Verify that the current status of the NWSD is VARIED OFF. If it is not, vary off the NWSD; then retry starting the server. See "Start and stop an integrated server" on page 149. If the status of the server is VARY ON PENDING even though the integrated server did not start, there may be a device driver problem.
2. Look for error messages and possible corrective actions in the job log where the vary on of the NWSD was performed.
3. Look in the QSYSOPR message queue for failure messages and possible corrective actions.
4. If you created a server configuration file that might be causing problems, try repairing or resetting the server configuration file. See "NWSD configuration file errors" on page 215.
5. If you initiated a restart from the integrated server, perform these steps.
   a. On i5/OS, enter the command WRKACTJOB SBS(QSYSWRK).
   b. Press Enter.
   c. Locate the job QVNAVARY.
   d. Select option 5 to work with the job.
   e. If the job is active or on the job queue, select option 10 to display the job log. Look for failure messages and possible corrective actions.
   f. If you have ended the job, enter WRKSPLF SELECT(*CURRENT *ALL *ALL QVNAVARY) to display the spooled file.
6. Enter the command WRKPRB to see logged problems.

For IXS or IXA attached xSeries server, a batch job using the name BTnwsdname is submitted to perform the vary off and vary on needed to 'reboot' the server.

Identify the qualified name of the job that was submitted in the QVNAVARY joblog. Locate the joblog for the submitted 'reboot' job by fully qualifying the jobname using WRKSPLF SELECT(*ALL) JOB(qualjobname).

List all 'reboot' jobs with WRKSPLF SELECT(*ALL) JOB(BTnwsdname) .

Emergency Repair

If the problem persists due to a failing system drive but you have a successful backup of that drive, try this emergency repair. To recover lost data and return the system to a functioning state, follow these steps.

Note: These examples use the NWSD name *ERS* with a system drive named *ERS1*.

1. Unlink the failing system drive (typically the C: drive) by using this command: RMVNWSSTGL NWSSTG(*ERS1*) NWSD(*ERS*).
2. Copy the failing system drive to a new name by using this command: CRTNWSSTG NWSSTG(*ERSBKP*) FROMNWSSTG(*ERS1*).
3. Restore your latest backup of the system drive.
4. Link in the restored system drive by using this command: ADDNWSSTGL NWSSTG(*ERS1*) NWSD(*ERS*).

5. Link in the failing system drive from step 1 by using this command: `ADDNWSSTGL NWSSTG(ERS1BKP) NWSD(ERS)`
6. Vary on the NWSD by using this command: `VRYCFG CFGOBJ(ERS) CFGTYPE(*NWS) STATUS(*ON)`.
7. Copy any key files, such as data files, from the failing system drive which have changed from the latest backup.
8. Install any applications that you added or upgraded since the latest backup.
9. Vary off the NWSD by using this command: `VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)`.
10. Unlink the failing system drive from step 5 by using this command: `RMVNWSSTGL NWSSTG(ERS1BKP) ERS(ERS1)`.
11. Until you are sure you have removed all data from the failing system drive, you can relink the drive (step 5) and copy additional files to the restored drive. Once you are sure that you have removed all data from the failing system drive, make a new backup of all storage spaces. Refer to "Back up predefined disk drives for integrated Windows servers" on page 188 for steps to backup storage spaces. Then delete the failing system drive by using this command: `DLTNWSSTG NWSSTG(ERS1BKP)`.

Problems hot sparing between servers

The main reason that hot sparing between integrated servers might fail is hardware compatibility. Windows Server 2003 activation may also cause problems. See the following sections for details.

Hot spare hardware compatibility

Switching a Windows server from one set of integrated server hardware to another is like migrating the Windows system drive from one PC to a second PC. Differences in the required hardware abstraction layer (HAL), the basic input/output system (BIOS) level, or the devices that are installed on the two PCs can cause problems with the migration. During the initial boot of Windows on the second PC, hardware differences are detected and are handled in one of several ways:

- Some hardware differences can be automatically handled via plug and play.
- Some hardware differences may require manual intervention. For example a new device driver may need to be installed.
- If the hardware differences are great enough, they can prevent the second PC from booting. For example, the two PCs may require incompatible versions of the HAL.

These same hardware compatibility considerations apply when hot sparing between IXS servers, between IXA attached xSeries servers and between iSCSI attached IBM xSeries or BladeCenter servers. In order for the hot spare migration to work successfully, the hardware configurations of the two servers should be closely matched.

Integrated xSeries Server (IXS) hot spare

In order to use hot spare between IXS servers, they should be compatible types and they should have a comparable configuration of LAN adapters, etc. The Integrated xSeries server configurations table on the following web page gives the specific IXS hot spare configurations that are supported: www.ibm.com/systems/i/bladecenter/ixs/system_config.html.

xSeries or IBM BladeCenter server hot spare

In order to use hot spare between IXA attached xSeries servers or between iSCSI attached xSeries or IBM BladeCenter servers, it is strongly recommended that you use the same type of xSeries or IBM BladeCenter blade servers. For example, an xSeries model 236 can be a hot spare for another xSeries model 236. In addition, the xSeries servers should have a similar configuration of PCI adapters, and so on.

Note: It may be possible to hot spare between two xSeries or blade server models that are not the same type. However, there are often significant hardware differences between xSeries or blade models. Therefore, you should test the specific combination of xSeries or blade server models that you plan to use for hot spare in this case. You should test to verify that the xSeries or blade server models have compatible hardware configurations and can be migrated seamlessly between each other before you use them for hot spare server backup in a production environment.

Windows Server 2003 activation

Each time a Windows Server 2003 server's storage spaces are switched to another hot spare integrated server, Windows Activation may be triggered. There are a limited number of free activations per license key. If activation is triggered enough times, this may require a phone call to Microsoft in order to re-activate. This can limit the speed that a server can be re-activated. Volume licenses of Windows Server 2003 can help in this case, since activation is not required.

Problems sharing hosted system hardware

For information about problems sharing hosted system hardware, see these links.

- "Multiple NWSDs defined to use the same hosted system hardware"
- "Special considerations for iSCSI attached systems"

Multiple NWSDs defined to use the same hosted system hardware

It is possible to define multiple network server descriptions (NWSDs) to control the hardware of a particular Integrated xSeries Server (IXS), xSeries system, or IBM BladeCenter blade. For non-iSCSI attached servers, these NWSDs must be in the same iSeries partition. However, for iSCSI attached servers, these NWSDs can be defined on the same iSeries partition, another partition in the same iSeries system, or on an entirely different iSeries system. For example, you may have an NWSD defined to use an xSeries system for production work during normal business hours and another NWSD defined to use the same xSeries system at other times.

Only one NWSD can use a particular piece of server hardware at any point in time. Therefore, if there are multiple NWSDs defined to run on the same hardware and one of them is currently using it, the others are not allowed to start until the NWSD that is currently using the hardware is shut down (varied off . This protects against one NWSD inadvertently taking over the hardware that is being used by another NWSD.

If you are having problems starting an NWSD and the server hardware is currently being used by another NWSD, then the correct way to transfer control of the hardware from one NWSD to another NWSD is to first shut down the NWSD that is currently using the hardware and then start the NWSD that needs to use the hardware next.

Special considerations for iSCSI attached systems

For iSCSI attached servers, the server hardware state is used to control access to the hardware and ensure that only one NWSD is using the hardware at any point in time. When starting (varying on) the NWSD, the specific behavior for an iSCSI attached server depends on the type of service processor that the server has:

- For xSeries servers with a BMC service processor, the hardware must initially be in a powered off state.
- For xSeries server with an RSA II or an IBM BladeCenter with a Management Module, the hardware must not be booted to an operating system (for example DOS or Windows). An xSeries system that is sitting at the insert diskette prompt is allowed, but the system will wait for a period of time to ensure that no other system is attempting to use the system.

Otherwise, the start operation will fail. When shutting down (varying off) the NWSD, the NWSD's xSeries or BladeCenter blade hardware will be left in a powered off state.

In addition to the case when an NWSD is currently using the server hardware, there are other possible reasons that the server hardware is in a powered on state. For example, the server hardware may have been powered on to perform hardware setup, such as loading firmware or changing BIOS settings. Another example is when the server operating system has encountered an unrecoverable error, resulting in a failed server, but leaving the hardware in a powered on state. For these cases, starting an NWSD in the normal way may fail because the server hardware is not in a powered off state or the service processor indicates that an operating system is still running.

There are a couple of ways to recover from this:

- If an NWSD is currently using the hardware, but the server operating system failed, then try shutting down the server. In most cases, this will power off the server hardware and make it available to the same or another NWSD. If shutting down the NWSD does not resolve the problem try the method described below.
- When starting an NWSD, there is a reset system option to force the server hardware to be reset during the start of the NWSD. You can use this option to start an NWSD that uses server hardware that is in a state that would normally cause the start (vary on) of the server to fail.

Attention: Use the reset system option only when you are sure that the server hardware is not currently being used by another NWSD. If you use the reset system option to start an NWSD when there is another NWSD that is running on the hardware, the other NWSD will fail and can incur data loss or corruption.

To reset a remote system using iSeries Navigator, follow these steps:

1. Expand **Integrated Server Administration**.
2. Expand **Servers**.
3. Right-click a server from the list available.
4. Select **Start with options...**
5. Check the **Reset remote system** option.
6. Click **Start**. A confirmation panel is shown.
7. Click **Start** on the confirmation panel to start and reset the remote system.

If you want to use a CL command, see the Reset system (RESETSYS) keyword on the Vary Configuration (VRYCFG) command.

NWSD configuration file errors

If you suspect that an NWSD configuration file that you created is causing an error, try resetting the NWSD configuration file parameter to *NONE. See “Reset the NWSD configuration file parameter” on page 216. If the error disappears, your NWSD configuration file most likely has a problem.

If the NWSD configuration file is causing errors, you have these options.

- Continue without using your own NWSD configuration file.
- “Use a previous version of the integrated server file” on page 216
- “Repair the NWSD configuration file”

Repair the NWSD configuration file

If you want to repair your NWSD configuration file to eliminate the errors, consider these options.

1. Check the logs for error and recovery information. See “Check message and job logs” on page 205.
2. Edit the NWSD configuration file.
3. Restart. See “Start and stop an integrated server” on page 149.

Reset the NWSD configuration file parameter

You can set the Configuration file parameter of the NWSD to *NONE to prevent the changes that are causing errors from being made to the integrated server file. To prevent i5/OS from using your NWSD configuration file, follow these steps.

1. On the i5/OS command line, type `WRKNWSD` to work with your network server descriptions (NWSD).
2. On the line by the network server that is having problems, choose option `2` (Change).
3. In the `Configuration file` field, select *NONE.
4. Vary on the network server and see if the error has gone away.

Note: Existing modifications to any files that are processed by a configuration file will remain unchanged. A .BKU file exists with the file contents before the last modification performed by varying on the server. This file can be used to replace the changed version or the file can be restored from a previous backup if one is available.

Use a previous version of the integrated server file

If you have a working version of the integrated server file, you can change the file back to this working version. To change it follow these steps.

1. Reset the configuration file parameter of the NWSD to *NONE to prevent the changes that are causing errors from being made to the integrated server file. See “Reset the NWSD configuration file parameter.”
2. Choose the file that you want to reset to a previous version.
3. If the server is functional and varied on, log on to the server or run a remote command (see “Run integrated Windows server commands remotely” on page 153) from the i5/OS console to rename the files:
   - Rename the file that is causing problems to another name.
   - Rename the previous version of the file to the original name.
4. Vary the integrated server off and back on to use the previous version of the file.

DASD in IXA or iSCSI attached servers

Local hard disk drives are not supported in an xSeries server when it is direct attached to the iSeries with the Integrated xSeries Adapter. Local hard disk drives are not supported in an IBM xSeries or BladeCenter server when it is attached to the iSeries with an iSCSI HBA. In most cases, the local hard disk drive will not show up. If the drive does happen to appear, and it is used, unpredictable results may occur. When attaching using an xSeries or IBM BladeCenter servers in the direct attach mode to the iSeries via an IXA or an iSCSI HBA, make sure any local hard disk drives are removed.

Failures enrolling users and groups

If you cannot enroll groups or users to the Windows environment on iSeries, follow this procedure to determine the problem.

From i5/OS:

- Check for errors in the message log for this network server description (NWSD) (designated during server installation to be QSYSOPR, a user-defined message log, or the user job log). Follow the error message Recovery actions to correct the problem. You can also find error codes on the Work with NWS Enrollment (WRKNWSENR) display.
- If the message log has `User Admin error NTA0282`, see “User enrollment authorization problems” on page 217.
- Make sure that the status of the server is `VARIED ON`.
- Check enrollment status (see “Enroll a single i5/OS user to the Windows environment using iSeries Navigator” on page 177) and look for error messages. Press F5 to refresh the status.
- Verify that i5/OS is set to keep passwords (QRETSVRSEC is set to 1). Also verify that users who are trying to enroll sign-on to i5/OS **after** this value is set.

- Specify and create a message queue for the NWSD; check the queue for messages.
- On i5/OS, enter the `WRKACTJOB` command. Check the `QPRFSYNCH` job in the `QSYSWRK` subsystem. Check the job log by pressing F10 for more detailed messages.
- On i5/OS, enter the `WRKJOB` ***nwsdname*** command, where *nwsdname* is the name of the NWSD for your integrated server. If the job is active, display the job log (Press F10 for more detail messages). If you end the job, display the spooled file.

From the integrated Windows server:

You can also try the following steps to determine the problem.

- See if the User Administration Service is running.
  1. From the integrated server's **Start** menu, select **Programs**, then **Administrative Tools**, then **Component Services**.
  2. Select **System Tools**, then **Services**.
  3. See if **iSeries User Administration** appears in the list of services.
  4. If the **iSeries User Administration** service is listed, but the status does not show that it is started, Right-click **iSeries User Administration** and select **Start** from the menu.
  5. If **iSeries User Administration** is not listed, do the following to reinstall it:
     a. From the **Start**, select **Run**, and type `command` to open a command prompt window.
     b. Go to the C: drive (or the current Windows drive).
     c. Type `%SystemRoot%\as400wsv\admin\qvnadaem /install` and press Enter.
     d. Close the **Services** window.
     e. Re-open **Services**.
     f. If you have not started **iSeries User Administration**, click **Start**.

If you get an error message stating that a Windows domain controller cannot be found, it may be that you are trying to enroll users to a Windows workgroup. 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. In iSeries Navigator, it will sometimes appear that you can enroll i5/OS users to these workgroups, but attempting to do this will result in an error. There is no seperate list of Windows workgroup users like there is for a Windows domain.

User enrollment authorization problems

If you get an error (NTA0282) that indicates insufficient authorization to create and update integrated server users, take action as appropriate.

- If you are trying to enroll users and groups to a domain for the first time, ensure that you set up a QAS400NT user ID to provide the necessary authorization. The topic, "The QAS400NT user" on page 183, tells you how. Also ensure that the user is configured as a traditional user, which means that the user must specify an iSeries password and have local password management enabled. See "Types of user configurations" on page 53.
- If you have been successfully enrolling users and groups for awhile, check to see if the i5/OS password for the QAS400NT user has expired. When the QAS400NT user password expires, the account on the integrated server also expires. To correct this situation, do the following.
  1. Enable the integrated server account.

     On a domain controller:

     a. Open **Start —> Programs —> Administrative Tools**.
     b. Select **Active Directory Users and Computers**.
     c. Right-click **Users**, then double-click **QAS400NT**.
     d. Click on the **Account** tab at the top of the **User Properties** window.

    e. Change the **Account expires** date to a date in the future and click **Never**.

    On a local integrated Windows server:

    a. Open **Start**, **Programs**, **Administrative Tools**.
    b. Select **Computer Management**.
    c. Expand **System Tools**; then expand **Local Users and Groups**.
    d. Right-click **QAS400NT** from the list.
    e. Click on the **Account** tab at the top of the **User Properties** window.
    f. Change the **Account expires** date to a date in the future and click **Never**.

2. On i5/OS, use the Change user profile (CHGUSRPRF) or Change password (CHGPWD) command to change the QAS400NT user password.
3. Restart the iSeries User Administration Service.
    a. Click on **Start**, then **Programs**, then **Administrative Tools**, then **Component Services**.
    b. Click on **Services**.
    c. Click on **iSeries User Administration**, then right-click **Stop** to stop the service.
    d. Click on **iSeries User Administration**, then right-click **Start** to restart the service.

Restarting the service automatically retries the enrollment of the users and groups.

To avoid this problem, be sure to change the QAS400NT password periodically on your i5/OS system to prevent the password from expiring.

If you have more than one iSeries with multiple integrated servers that participate in a Windows domain, you can minimize password expiration problems by implementing the steps described here: "The QAS400NT user" on page 183.

- If the problem still persists, check the technical information databases at the IBM eserver iSeries Support Web page. If you cannot find the solution there, contact your technical support provider.

Password problems

Previously, all characters that were allowed in i5/OS passwords were also allowed in Windows passwords. Now, i5/OS allows longer passwords and more characters than Windows supports. You should use i5/OS passwords containing only characters and password lengths allowed in Windows passwords if you want to enroll users. More i5/OS password level security information may be found in the Planning Password Level Changes section of the iSeries Security Reference .

If a password keeps expiring each day after being changed from the integrated server console, it means that the user forgot that the password must be changed from i5/OS. Changing the i5/OS password eliminates the problem.

If the i5/OS and Windows server passwords do not match, perform these tasks to determine why.

1. Check to see if the user is configured as a Windows user. See "Types of user configurations" on page 53.
    a. On the i5/OS command line, type `WRKUSRPRF`.
    b. Type in the correct UserID.
    c. Check to see if the attribute `LCLPWDMGT` (Local password management) is set to *NO. If so the user is configured to have an i5/OS password of *NONE and the i5/OS and Windows passwords will not be the same.
2. Check to see that i5/OS is set to store passwords:
    a. On the i5/OS command line, type `WRKSYSVAL SYSVAL(QRETSVRSEC)`.
    b. Enter a `2` in the `Option` field; press Enter.
    c. Verify that `Retain server security data` is set to 1. If it is not, change it to 1.

3. On the integrated Windows server, make sure that the User Administration Service is running. See “Failures enrolling users and groups” on page 216 for related information.
4. Check to see the i5/OS password support level:
   a. On the i5/OS command line, type WRKSYSVAL SYSVAL(QPWDLVL).
   b. Enter a 5 in the Option field; press Enter.

   The password level of i5/OS can be set to allow user profile passwords from 1 - 10 characters or to allow user profile passwords from 1 - 128 characters. The i5/OS password level of 0 or 1 supports passwords from 1 - 10 characters and limits the set of characters. At level 0 or 1, i5/OS will convert passwords to all lowercase for Windows server. The i5/OS password level of 2 or 3 supports passwords from 1 - 128 characters and allows more characters including upper and lower case characters. At level 2 or 3, i5/OS will preserve password case sensitivity for Windows server. A change to the i5/OS password level takes effect following an IPL.
5. Check the enrollment status of the user. Make sure the user did not already exist in the Windows environment with a different password before you attempted to enroll the user (see “Enroll a single i5/OS user to the Windows environment using iSeries Navigator” on page 177). If the user did exist with a different password, enrollment will have failed. Change the Windows password to match the i5/OS password; then perform the enrollment procedure again.
6. If the problem still persists, check the technical information databases at the eServer IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

IBM iSeries Integrated Server Support snap-in program

You may experience an error when trying to run the IBM iSeries Integrated Server Support snap-in program. The program may not start, may provide unexpected information, or an error can occur during use.

If the IBM iSeries Integrated Server Support snap-in display never appears the following steps can help you determine the problem.

- Check to see if there is already an instance of IBM iSeries Integrated Server Support snap-in or the Lvlsync program on the system. You can only run one instance of these programs at a time. If there is already an instance of either program in operation, then a new call to either program will return. Finish using the current program before trying to start a new instance.
- Ensure that the user has administrator-level access and special authorities. The IBM iSeries Integrated Server Support Snap-in programs require these authorizations. Retry starting the program with administrator authority.
- Ensure that you have started iSeries NetServer. iSeries NetServer starts automatically with the QSERVER subsystem on i5/OS. Start iSeries NetServer if i5/OS has not already started it.
- Ensure that you have enabled the guest user profile on iSeries NetServer. If not, then enable the guest user profile so that guests can access the iSeries NetServer (see “Plan for a Windows user with authorities to access iSeries NetServer” on page 63). When you have enabled guest access, first stop and then restart iSeries NetServer and then retry running the IBM iSeries Integrated Server Support snap-in program.
- Check the system event log on the Windows server for any messages pertaining to the IBM iSeries Integrated Server Support snap-in program.

The IBM iSeries Integrated Server Support snap-in display may appear, but the information that i5/OS displays may not be what you expected. If so, the following steps can help you determine the problem.

- Verify that the latest service pack PTF is available and in an active state on i5/OS. You can use the Display PTF (DSPPTF) command to do this.
- Verify that the service pack you believe that you have installed is actually installed on the integrated server.

- Check the system and application event log on the integrated server for any messages pertaining to the Integrated Server Support snap-in program.

When you perform an action with the IBM iSeries Integrated Server Support snap-in program, problems can occur. The following list helps you solve problems that can occur after you click the **OK** button.

- A drive letter must be available for the IBM iSeries Integrated Server Support snap-in program to proceed. This drive letter need only be available temporarily. If all drive letters are in use, try freeing a drive letter for use with IBM iSeries Integrated Server Support snap-in and retry the program.
- The IBM iSeries Integrated Server Support snap-in program takes the specified action. The system may or may not be restarted depending on the set of files updated. It may take a short time for the system shutdown and start up to occur.
- Check the system and application event log on the integrated server for any messages pertaining to the IBM iSeries Integrated Server Support snap-in program.
- If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page. If you cannot find the solution there, contact your technical support provider.

Problems with iSCSI attached servers

If you are experiencing one of the problems listed below, you may begin troubleshooting by performing the actions listed. This is not a comprehensive list, so some problems may require actions beyond those listed here. To find information that may help you troubleshoot problems, see “Check message and job logs” on page 205.

Initializing the service processor configuration fails

If there is a message CPDC4xx or CPFC4xx in the system operator’s message queue (QSYSOPR) or the job log of the batch job or interactive user involved, see “IBM Director Troubleshooting” on page 222.

When installing or starting a server, the NWSD status stays VARIED OFF

- Ensure that all required network server host adapters configured for the server are varied on before installing or starting a server. If a network server host adapter will not vary on, check for messages in the network server host device’s message queue.
- If there is a message CPDC4xx or CPFC4xx in the system operator’s message queue (QSYSOPR) or the job log of the batch job or interactive user involved, see “IBM Director Troubleshooting” on page 222.

With the hosted system powered on, a server will not start

See “Problems sharing hosted system hardware” on page 214.

The hosted system’s console displays ’No iSCSI devices found’ or prompts for diskette

- The iSCSI HBA configured for boot in the hosted system was unable to do so.
- There may be an iSCSI configuration problem. See iSCSI Troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).
- If message CPPC056 is in the Product Activity Log, a CHAP configuration problem is likely.
- There may be a network problem between the hosted system’s iSCSI HBA configured for boot and the iSeries HBA corresponding to the path configured for the NWSD’s system drive storage space. See “Boot and storage path network analysis” on page 221.

The NWSD status is VARIED ON, but Windows does not begin to boot

- There may be an iSCSI configuration problem. See iSCSI Troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).
- If message CPPC056 is in the Product Activity Log, a CHAP configuration problem is likely.

- There may be a network problem between the hosted system's iSCSI HBA configured for boot and the iSeries HBA corresponding to the path configured for the NWSD's system drive storage space. See "Boot and storage path network analysis."

The NWSD status is DEGRADED

Ensure that all required network server host adapters configured for the server are varied on. If a network server host adapter will not vary on, check for messages in the network server host device's message queue.

Storage using a path other than the boot path does not show up in Windows

- There may be a network problem between the hosted system and the iSCSI HBA in the iSeries that corresponds to the non-boot path. See "Boot and storage path network analysis."
- If message CPPC056 is in the Product Activity Log, there is a CHAP problem. In this case, it is most likely due to a problem with the digital certificates that the Windows environment on iSeries needs to securely transfer its own sensitive data between i5/OS and Windows. See "Managing path certificates" on page 222.

Storage using a path other than the boot path sometimes shows up late in Windows

- This is normal the first time the server is started after you change certain i5/OS configuration information, such as SCSI local interface information in the network server host adapter or CHAP information in the remote system configuration.
- This is normal if an iSCSI HBA in the hosted system has not been used with this particular NWSD before. This would be the case when an iSCSI HBA is replaced in the hosted system, or when using a different hosted system as a hot spare.
- If your application involves an automatic start service that is sensitive to the above situations, see the Advanced iSCSI tasks Web page (www.ibm.com/systems/i/bladecenter/iscsi/advancedtasks.html).

User enrollment or submit remote command fails with NTA02BB, NTA028A, NTA028B

- There is a problem with the digital certificates that the Windows environment on iSeries needs to securely transfer its own sensitive data between i5/OS and Windows. See "Managing path certificates" on page 222.
- For NTA028A and NTA028B, ensure that the time and date on the hosted system doesn't differ significantly from the date on the iSeries, as this can cause digital certificates to appear to be invalid.

Boot and storage path network analysis

For more information about these steps and additional troubleshooting procedures, see iSCSI troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

- On the hosted system, use the CTRL-Q utility to display the hosted system's iSCSI HBA MAC addresses. Ensure that these match the SCSI interface adapter address values in the i5/OS remote server configuration. This step may be skipped if you are here because a manually configured boot failed.
- Use the CTRL-Q utility or Device Manager view of the SCSI driver to PING the SCSI IP address of the appropriate iSCSI HBA for iSeries.
- If PING fails, perform the following steps.
  - Ensure that the physical network is properly connected, and that devices in the network, such as switches, are functioning.
  - Ensure that requirements defined in "iSCSI network" on page 29 are satisfied.
  - If a firewall or a similar packet filtering function is involved, ensure that the firewall allows Internet Control Message Protocol (ICMP) packets to pass. Unlike SCSI IP addresses, LAN IP addresses can be affected by firewall software running in Windows.

- If your NWSD uses IP security (IPSec) rules other than *NONE, See iSCSI Troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

- If ping succeeds, perform the following steps.
  - If a firewall or a similar packet filtering function is involved, see "Configure a firewall" on page 131. Unlike SCSI IP addresses, LAN IP addresses can be affected by firewall software running in Windows.
  - If DHCP boot fails and a routed network is involved, ensure that an appropriately configured DHCP relay agent (also known as a BOOTP relay boot) exists in the network.

Managing path certificates

Note: This section pertains only to iSCSI attached systems.

Normally Windows environment on iSeries automatically generates the digital certificates it needs to securely transfer its own sensitive data between i5/OS and Windows. These are called path certificates. If you suspect a path certificate problem, you can do the following.

- Ensure that 5722-SS1 Option 34 (Digital Certificate Manager) is installed.
- Ensure that i5/OS and Windows have compatible digital certificates by generating new certificates when starting the server. This should only be done in unusual situations, such as when an old version of a storage space for a Windows system drive is restored without restoring the corresponding i5/OS certificate store also. To generate new path certificates using iSeries Navigator, follow these steps:
  1. Expand **Integrated Server Administration**.
  2. Expand **Servers**.
  3. Right-click a server from the list available.
  4. Select **Start with options...**
  5. Check the **Regenerate path certificates** option.
  6. Click **Start**.

If you want to use a CL command, see the Generate path certificate (GENPTHCERT) keyword on the Vary Configuration (VRYCFG) command.

IBM Director Troubleshooting

Note: This section pertains only to iSCSI attached systems.

If you cannot connect to IBM Director (for example, when starting or shutting down a server) take the following actions:

- Wait five minutes and retry the operation.
- Stop and restart IBM Director
  - At the i5/OS command line enter `ENDTCPSVR SERVER(*DIRECTOR)`
  - It will take several minutes or more for Director server to stop. Status of the stop process can be obtained by running the following from qsh: `/qibm/userdata/director/bin/twgstat`. After a few minutes, it should eventually report "inactive" state.
  - Start the qsh interpreter by entering `qsh` at the i5/OS command line.
  - From qsh run: `/qibm/userdata/director/bin/twgstart`
- Verify the IBM Director properties file configuration

  The IBM Director properties file is installed during the IBM Director installation in the location /QIBM/ProdData/Director/classes/com/ibm/sysmgt/app/iide/IIDETask.properties.

  Verify that the IBM Director properties file exists. If it does not exist, reinstall IBM Director or contact your service representative.
- Verify that a port is specified in the IBM Director properties file.

  This file should contain a line that specifies `"port = xxxxx"` where *xxxxx* is the port number. If the line does not exist, do these steps:

  1. Edit the file and add a line that contains "port = 5779". 5779 is the default port used for the i5/OS connection to IBM Director.
  2. Restart IBM Director.

- Verify the port used by IBM Director is not in use by another application

  After starting IBM Director, verify that the port specified in the IBM Director properties file is not in use by another application.

  1. Using iSeries Navigator, expand **Network—>TCP/IP Configuration—>IPv4—> Connections**.
  2. Right-click the list entry that has the same port number in the **Local Port** column that was specified in the IBM Director properties file and select **Jobs**.
  3. In the jobs list, look for a job with job name **Qcpmgtsvr** and user **Qcpmgtdir**. This should be the only job that is using the specified port.

  If there are any other jobs using the port, then you must change the port that is used by IBM Director using these steps:

  1. In the IBM Director properties file, change the port number specified in the line `"port = xxxxx"` where *xxxxx* is the port number.
  2. Restart IBM Director.

Discovery problems: If a message is logged that indicates that the remote server or enclosure is not found, then the IBM Director interface was not able to find the targeted service processor on the network. See "Remote server discovery and management" on page 142.

If you are using a Remote Supervisor II service processor, verify that you are using the most recent firmware. See iSCSI install read me first Web page (www.ibm.com/systems/i/bladecenter/iscsi/readme/).

If you are not using unicast addressing to discover the service processor, do the following steps:

- Verify that your iSeries server has a physical network connection to the service processor of the remote system.
  - See Ping from iSeries Navigator in the TCP/IP troubleshooting topic collection.
- If your iSeries server has a physical network connection to the service processor, check the firewall settings for the routers or switches on the iSCSI network. Network routers or switches between the iSeries LAN interface and the service processor might not support multicast addressing or are not configured to allow multicast addressing.

  Network routers or firewalls can block SLP multicast packets. The routers or firewalls may need to be configured to allow the Service Location Protocol IP address of 239.255.255.253 or port number 427 to allow passage of the SLP packets.
- Configure your service processor to use unicast addressing.

  The service processor must have a static host name or IP address configured. You can do this using the BIOS utility for an RSA II or the service processor web interface. See "Use the Management Module or RSA II web interface" on page 146 for instructions on how to use the service processor web interface to configure the service processor.

  Change the service processor configuration to use unicast addressing, which uses the host name or IP address that was set in the service processor above to connect to the service processor. See "Change service processor configuration properties" on page 124.

If you are using unicast addressing to discover the service processor

- Verify your service processor IP address or host name is configured correctly both in the remote system service processor and in the service processor configuration on i5/OS.
- See the TCP/IP troubleshooting topic for general TCP/IP troubleshooting procedures.

Problems with SSL connections: A number of different problems can occur if the Secure Socket Layer (SSL) connection to the service processor is configured. See “Configure service processor SSL” on page 130

The certificate is not imported into the correct i5/OS certificate store.

If you are using the manual security mode, verify that the service processor certificate authority (CA) root is in the iSeries *SYSTEM certificate store.

1. Connect to the service processor web interface.
2. Display the certificate. Note the certificate authority in the “Issued by” field of the certificate.
3. Connect to the iSeries Digital Certificate Manager (DCM) interface to determine if the CA is listed as a certificate in the *SYSTEM certificate store.
   a. Determine the root CA of the Certificate that was installed in the Service Processor.
      1) Connect to the Service Processor web interface with your web browser by going to http://***hostname*** (where ***hostname*** is the host name of the service processor) or http://***ipaddress*** (where ***ipaddress*** is the IP address of the service processor).
      2) Follow your browser’s help instructions to view the security certificate that verified the web site’s identity.
      3) Follow your browser’s help instructions to view the Certificate Hierarchy.
      4) The highest entry in the hierarchy will be the root CA Certificate.
      5) Note the name that is shown for the root CA certificate for use in step h below.
   b. Connect to the iSeries Digital Certificate Manager (DCM) interface. See Start DCM in the Digital Certificate Manager topic.
   c. Click **Select Certificate Store**.
   d. Select ***SYSTEM** and click **Continue**.
   e. Enter the certificate store password for the *SYSTEM certificate store.
   f. On the left pane, click **Fast Path**.
   g. Select **Work with CA certificates** and click **Continue**.
   h. On the **Work with CA Certificates** page, look for an entry in the Certificate Authority (CA) field that matches the name of the root CA Certificate that was determined in step a.
   i. If the **Status** field for this entry is **Enabled** then the CA is properly configured.
   j. If the **Status** field for this entry is **Disabled** then it must be enabled with the following steps:
      1) Select the radio button to the left of the Certificate Authority (CA) entry that needs to be enabled.
      2) Select the ″Enable″ pushbutton at the bottom of the table.
      3) The CA is now properly configured.
   k. If there is not an entry in the Certificate Authority (CA) fields that matches the name of the root CA Certificate that was determined in step a), add the CA by doing these steps:
      1) Refer to the original e-mail that you received from the Certificate Authority (CA). This e-mail should have contained the certificate (which was imported into the Service Processor) and the associated trusted root certificate.
      2) FTP the trusted root certificate to a directory in the IFS File system on the iSeries and note the full path and file name.
      3) On the left pane, select **Manage Certificates** to display a list of tasks.
      4) From the task list, select **Import certificate**.
      5) Select **Certificate Authority (CA)** as the certificate type and click **Continue**.
      6) Specify the fully qualified path and file name for the CA certificate file and click **Continue**. A message displays that either confirms that the import process succeeded or provide error information if the process failed.

7) The CA is now properly configured.

The service processor configuration is not initialized.

If you are using the automatic security mode, the service processor configuration must be initialized after the automatic security mode is configured.

Do the following steps:

- If this is the first time that the remote system service processor is being initialized, then follow the procedure described in “Initialize a service processor” on page 124 to initialize a new service processor.
- If the remote system service processor has previously been initialized, then follow the procedure described in “Initialize a service processor” on page 124 to synchronize the user, password, and certificate from the remote system service processor to the service processor configuration.

The service processor certificate identifier is not recognized.

If you are using manual security, verify that the service processor’s certificate field matches the service processor certificate identifier configured in the service processor configuration.

1. Display the service processor configuration (see “Display service processor configuration properties” on page 124) and click the **Security** tab. Note the values for service processor certificate identifier component and compare value. The component values map to a certificate field as follows:
   - Common name – Issued to (Subject) Common Name (CN)
   - E-mail address – Issued to (Subject) (E)
   - Organizational unit – Issued to (Subject) Organizational Unit (OU)
2. Access the service processor’s web interface.
3. View the service processor security certificate.
4. Compare the certificate fields to the compare values shown in the service processor configuration.
5. If these values do not match, see use the method described in “Change service processor configuration properties” on page 124 to enter the correct value. Then see “Initialize a service processor” on page 124 for information about how to synchronize the certificate from the remote system service processor to the service processor configuration.

Note: In the service processor configuration, you can specify that you do not want to use the service processor certificate.

The service processor does not support SSL.

- If a secure connection is not required, then see “Change service processor configuration properties” on page 124. On the **Security** tab, select the **Do not use a certificate (requires physical security)** option and save the changes.
- Verify that your service processor supports SSL.
  1. See “Configure remote server and service processor discovery” on page 142.
  2. If your service processor is SSL capable, contact your service representative to determine if a firmware or hardware update will be necessary to add SSL support.

Virtual Ethernet problems with iSCSI attached servers

To see information about the connections available to the Windows TCP/IP stack, enter **ipconfig /all** at a Windows command prompt. You should see information about the following things:

- External network adapters
- The LAN interfaces for the iSCSI HBA ports
- Virtual Ethernet adapters for your iSeries server

Match the results of the ipconfig command with one of the following troubleshooting cases and perform the actions suggested for that case until the problem is resolved.

A configured LAN IP address is missing in ipconfig

This case applies if an internet address for a LAN interface in the i5/OS remote configuration does not match an IP address that ipconfig shows for any iSCSI HBA. To display the remote system configuration, see "Display remote system configuration properties" on page 121.

- Examine the ipconfig results to find the physical addresses (MAC addresses) of the iSCSI HBAs. If a physical address displayed by ipconfig is different than the adapter address for the LAN interface in the i5/OS remote system configuration, do the following steps.
  1. Shut down the server from the Windows console.
  2. Vary off the NWSD from i5/OS. See "Start and stop an integrated server" on page 149.
  3. Change the adapter address for the LAN interface in the remote system configuration.
  4. Using i5/OS, start (vary on) the NWSD. See "Start and stop an integrated server" on page 149.
- Open **Control Panel**, then **Administrative Tools**, then **Services**. Ensure that **iSeries Shutdown Manager** is in the list of services and has a status of **Started**. This service automatically assigns LAN IP interface information from the i5/OS remote system configuration to ports having the configured MAC addresses.
- Look in the **Application event log** in Windows for events with a source of **iSeries Shutdown Manager**.
- Close any network properties window having **General**, **Authentication**, and **Advanced** tabs because this type of window locks resources required for assigning an IP address. If you close this type of window, wait 30 seconds for iSeries Shutdown Manager to assign the missing IP address, and enter **ipconfig /all** again.
- If none of the ipconfig results describe an installed iSCSI HBA, open Device Manager in Windows and ensure that the network driver for the iSCSI HBA is installed and enabled. If the driver has a yellow '!' or is grayed out, look in the System event log in Windows for events with a source of QL40xx and ensure that the iSCSI HBA is not disabled by the system BIOS setup menu.

Ipconfig shows a configured iSCSI HBA connection in media disconnected state

This case applies if ipconfig shows an iSCSI HBA connection that is in media disconnected state and has a physical address that matches an adapter address in the i5/OS remote system configuration.

- Ensure that the physical network is properly connected, and that devices in the network, such as switches, are functioning at the physical link to the hosted system's iSCSI HBA.

Ipconfig shows an IBM iSeries Virtual Ethernet connection in media disconnected state

- Virtual Ethernet requires a working iSCSI network, so iSCSI HBA problems must be resolved first. Ensure that ipconfig shows the LAN addresses in the i5/OS remote system configuration before proceeding.
- Ensure that the physical network is properly connected, and that devices in the network, such as switches, are functioning beyond the physical link to the hosted system's iSCSI HBA.
- Ensure that requirements defined in "iSCSI network" on page 29 are satisfied.
- Open **Control Panel**, then **Administrative Tools**, then **Services**. Ensure that **iSeries Manager**, **iSeries Shutdown Manager**, and **iSeries Virtual Ethernet Manager** are in the list of services and have a status of **Started**.
- Look in the **Application** event log in Windows for events with a source of **iSeries Virtual Ethernet Manager**.
- If a firewall or a similar packet filtering function is involved, see "Configure a firewall" on page 131. LAN IP interfaces in the i5/OS remote system configuration can be affected by firewall software running in Windows.

- If your NWSD uses IPSec rules other than *NONE, see the iSCSI troubleshooting web page (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Ipconfig shows an IBM iSeries Virtual Ethernet connection with an incorrect IP address

- Manually configure the IP address in Windows. For point to point virtual Ethernet, see “Point to point virtual Ethernet IP address conflicts” on page 233. For other virtual Ethernet networks, only steps 1 - 5 of this procedure apply.

‘Virtual Ethernet x’ is configured in i5/OS and ‘IBM iSeries Virtual Ethernet x’ is missing in ipconfig

- In i5/OS, verify that the line description exists for the virtual Ethernet of interest. For point to point virtual Ethernet, see “Explore point to point virtual Ethernet networks” on page 113.
- Open **Control Panel**, then **Administrative Tools**, then **Services**. Ensure that **iSeries Virtual Ethernet Manager** is in the list of services and has a status of **Started**. This service automatically creates and removes IBM iSeries Virtual Ethernet adapters to match the line description configuration in i5/OS.
- Ensure that the system is not set to block installation of unsigned drivers. For details, see steps 1-4 of “Begin the LAN driver installation or update” on page 231. If you change the setting from **Block**, restart the **iSeries Virtual Ethernet Manager** service, wait 30 seconds and enter **ipconfig /all** again.
- Open **Device Manager** in Windows and ensure that the network driver for the IBM iSeries Virtual Ethernet adapter of interest is installed and enabled. If a yellow ‘!’ is shown near the driver, look in the **System** event log in Windows for events with a source of **Qvndvimp**.

Ipconfig results look OK but large transfers fail

- Ensure that the IBM iSeries Virtual Ethernet adapters and the ‘LAN’ side of iSCSI HBA ports are not configured to use a larger maximum transmission unit than the iSCSI network supports. For example, not all switches support 9000 byte jumbo frames. Check the specifications of your network equipment. For more information, see “Maximum transmission unit (MTU) considerations” on page 139.

Virtual Ethernet problems with IXS and IXA attached servers

For the purposes of this section, the virtual Ethernet point to point LAN and the virtual Ethernet ports 0-9 are all considered virtual Ethernet adapters or virtual Ethernet ports.

There are two kinds of virtual Ethernet device drivers, virtual Ethernet Adapter (VE) and a virtual Ethernet Data Transport (DT).

- The virtual Ethernet Adapter corresponds to the driver that appears as the adapter, called ’virtual’ because no NIC hardware is associated with it.
- The virtual Ethernet Data Transport is the driver that provides a connection to the system bus connecting all the virtual Ethernet networks.

When a VE port cannot communicate across the system bus, it reports that the cable for the port is unplugged (cable disconnected). This is an important concept for troubleshooting virtual Ethernet errors.

The virtual Ethernet Ports under Windows are automatically installed and uninstalled by the virtual Ethernet Utility (VEU). The utility receives signaling through a configuration file from the NWSD. For example, when a user creates a Line Description under the NWSD for a given virtual Ethernet Port the VEU installs the corresponding VE port. Rebooting the Windows server configures the VE port address.

The following virtual Ethernet components use the listed driver.

- virtual Ethernet Adapter: qvndvemp.sys
- virtual Ethernet Data Transport: qvndvedt.sys
- virtual Ethernet Install Utility: qvndveu.exe

Troubleshooting virtual Ethernet problems

When the communication between any VE ports is not functioning, you need to perform two general tasks to troubleshoot the problem.

1. Determine the status of the VE ports.
2. Match the observed results to the following troubleshooting cases.

Determine VE port status

To determine the status of the VE ports.

- Use the iSeries console to determine if a line description for the VE port is created under the NWSD.
- Use the Windows console to open the **Network and Dial Up Connections** folder and determine if the VE port icon is present.

Match port status with troubleshooting cases

Match results of your determination of the status of the VE ports to one of the following troubleshooting cases.

- "Both line description and icon are present."
- "Line description is present and icon is missing" on page 229.
- "Line description is missing and icon is present" on page 229.
- "Both line description and icon are missing" on page 229.

In each case, you must first verify the i5/OS side then verify the Windows side. To verify the Windows side, you may need to open the Event Log and the Device Manager.

- To open the Event Log, from the Windows **Start** menu, select **Programs**, then **Administrative Tools**, then **Event Viewer**.
- To open the Device Manager, from the Windows **Start** menu, select **Settings**, then **Control Panel**, then **Administrative Tools**, then **Computer Management**, then **Device Manager**.

Both line description and icon are present

Verify the i5/OS side

Check the line description. When the line description is in the FAIL state, perform the following steps.

1. Collect PAL entries and VLOGs
2. Contact support
3. Verify the Windows side

Otherwise, when the line description is in the VARY-ON PENDING, VARY-ON, or RCYPND state, verify the Windows side.

Verify the Windows side

Open the **Network and Dialup Connections** window and check the VE icon.

- When the VE icon appears functional and the line description is in the VARY-ON state, verify that the IP addresses are properly configured. If the problem persists, contact support.
- When the VE icon appears functional and the line description is in VARY-ON PENDING or RCYPND state, verify for entries in the PAL and contact support.
- When the VE icon has a red X (cable disconnected), open the Event Log and locate entries for the qvndvemp.sys driver.
  - When you find entries for qvndvemp.sys, record them and contact support. Driver initialization is likely to have failed, and an IOP dump may be required to determine the problem.
  - When you do not find any entries for qvndvemp.sys, contact support and indicate the state of the line description. The problem is likely to be related to an i5/OS LIC problem.

Line description is present and icon is missing

Verify the i5/OS side

Check the line description. When the line description is in the FAIL state, perform the following steps.

1. Collect PAL entries and VLOGs
2. Contact support
3. Verify the Windows side

Otherwise, when the line description is in the VARY-ON PENDING, VARY-ON, or RCYPND state, verify the Windows side.

Verify the Windows side

Open the **Device Manager**, click **Network Adapters** to list the installed adapters, and locate the entry for the VE port.

- When the VE port has an exclamation point (!). beside it, complete the following steps.
  1. Open the Event Log, locate any entries for the qvndvemp.sys driver and record them.
  2. Contact support. The driver failed to initialize, which requires assistance to diagnose the cause.
- When the VE port has a red X, complete the following steps.
  1. Right-click the VE port and select **Enable**.
  2. Open the **Network and Dialup Connections** window and locate the VE icon.
  3. If the VE port icon is missing or it remains gray, open the **Event Log**.
  4. Locate entries for the qvndvemp.sys driver, record any that you find, and contact support. The VE port failed to load or start.

Line description is missing and icon is present

Verify the i5/OS side

Verify that no line description is currently present for the VE port under the NWSD, then verify the Windows side.

Verify the Windows side

Open the **Network and Dialup Connections** window and check the VE icon. When the installation VEU failed to remove the VE port, reboot the integrated server to clear this condition. If the problem persists, complete the following steps.

1. Use the VEU to manually remove the VE port by using the following command.

   ```
   qvndveu -a -R -x [port_id]
   ```

   where `[port_id]` is either a decimal (`0-9`) that corresponds to the port being removed or `p`, for point to point (point to point virtual Ethernet).
2. After running the command, if the VE port icon is no longer present, the process has completed. However, if the VEU failed to uninstall and remove the VE port, continue with the remaining steps.
3. Collect the VEU log file (D:\as400nt\qvndveu.log).
4. Open the **Event Log**, locate any entries for the qvndvemp.sys driver and record them.
5. Contact support. Ensure that you have the following at hand.
   - Any entries that you recorded for qvndvemp.sys
   - The VEU log file that you previously collected

Both line description and icon are missing

Verify the i5/OS side

You must have a line description in the NWSD for a VE port to be installed. Use the instructions found here,“Configure virtual Ethernet networks” on page 111, to create a line description.

Note: To add a line description, the NWSD needs to be varied off. Once you have created the line description and rebooted the integrated Windows server, the installation VEU automatically creates the VE port under Windows.

When a VE port problem persists after you successfully create a line description and reboot the integrated server, come back to this troubleshooting section and follow the instructions for the newly matched failing case.

Verify the Windows side

When no i5/OS line description is present, a VE port should not be listed under Windows. Install the line description as described in “Configure virtual Ethernet networks” on page 111 and restart the integrated server to see if this fixes the problem.

Problems with external networks

If you have a problem with an integrated server’s external network

- Review the integrated Windows server event log for either communication errors or device driver errors. You can use the Windows **Event Viewer** to do this. Event logs associated with external adapters supported by 2890, 2892, and 4812 Integrated xSeries Servers may have one of the following in the event log Source field: IBMTRP, PCNET, ALTND5, E100B, or E1000. If you can not find text in event logs for the IBMTRP token-ring service, you need to make changes in the Windows Registry.

  Note: If you are not familiar with the process for making changes in the Windows Registry, contact a service representative.

  If you are familiar with this process, to make the text in the event logs viewable, complete the following steps.

  1. From the Windows **Start** menu, click **Run**.
  2. Type `regedit.`
  3. In the Registry Editor, go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP`
  4. Select **EventMessageFile**.
  5. From the Registry Editor **Edit** menu, select **Modify**.
  6. Type `%SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll`
  7. Close the Registry Editor and restart the integrated server.
- For Ethernet adapters, ensure that a driver with **iSeries** or **AMD PCNET Family Ethernet Adapter (PCI)** in its name is listed and has a status of **started**.
  1. Click on **Start**, then **Administrative Tools**, then **Computer Management**, then **System Tools**, then **Device Manager**, then **Network Adapters**.
  2. Ensure that a driver with **iSeries** or **AMD PCNET Family Ethernet Adapter (PCI)** in its name is listed and has a status of **started**.
- For token-ring networks, also in **Device Manager**, ensure that you have started the **IBM High-Speed 100/16/4 Token-Ring PCI Adapter** or **IBM PCI Token-Ring Adapter**.

  Note: The start up setting should be **Enable**.
- For token-ring networks, ensure that the Network Data Rate setting is appropriate for your network.
- For Ethernet networks, ensure that the Link Speed and Duplex settings are appropriate for your switch or hub. If your 4812 or 5701 does not connect at speeds greater than 100 million bits per second, check

your switch's specifications for compliance with the IEEE 802.3ab standard. Windows LAN drivers for 4812 or 5701 Gigabit Ethernet ports may be limited to 100 million bits per second when connected to some early model non-compliant switches.

- The 10/100 Mbps Ethernet port on the 2892 Integrated xSeries Server does not support direct connection to certain 10 Mbps hubs and routers that lack **auto-polarity** functionality. If you are having difficulty getting your 2892 10/100 port to work at all with a 10 Mbps hub or router, check its specifications for **auto-polarity** support. Also, see if your 2892 10/100 port works with other devices.
- If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

Manually update LAN drivers on the integrated Windows server

Windows 2000 Server and Windows Server 2003 generally automatically install LAN drivers that are appropriate for your LAN adapters and ports. However, if you have a special situation you can manually install or update a LAN driver.

To manually install or update a LAN driver for an adapter other than virtual Ethernet in an externally attached Netfinity or xSeries server, go to the IBM Personal computing support Web site and select **Servers**, then **Device driver file matrix**.

To manually install or update a LAN driver for an adapter or port in an Integrated xSeries Server or for virtual Ethernet, complete the following tasks.

1. "Begin the LAN driver installation or update."
2. "Select the adapter to install or update."
3. "Complete the LAN driver installation or update" on page 232.

Begin the LAN driver installation or update

To begin the manual installation or update of the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet, complete the following steps.

1. From the Windows **Start** menu, select **Settings**, then **Control Panel**.
2. Double-click **System**.
3. In the **System Properties** window, select the **Hardware** tab.
4. If the new LAN driver is not digitally signed, or if you are unsure whether or not the LAN driver is digitally signed, ensure that the driver signing policy is set to Ignore.
   a. In the **System Properties** window, click **Driver Signing**.
   b. Note the current setting, then click **Ignore**, and then click **OK**.
5. Click **Device Manager**.
6. "Select the adapter to install or update."

Select the adapter to install or update

After you complete the steps to begin the installation or update (see "Begin the LAN driver installation or update") of the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet, you will need to select the adapter.

To select the adapter that you want to install or update, complete the following steps.

1. In the **Device Manager** window, open **Network Adapters**.
2. Under **Network Adapters**, right-click the adapter that you want to update and select **Properties**.
3. In the **Properties** windows for the adapter, click the **Driver** tab.
4. Click **Update Driver** or **Install Driver** (only one will display).
5. In the **Update Device Driver Wizard** dialog box, click **Next**.
6. "Complete the LAN driver installation or update" on page 232.

Complete the LAN driver installation or update

Ensure that you have completed the first two tasks required to manually install or update the LAN driver or port in an Integrated xSeries Server or for virtual Ethernet.

- "Begin the LAN driver installation or update" on page 231.
- "Select the adapter to install or update" on page 231.

To complete the LAN driver or port installation or update, use one of the following procedures that fits your situation.

- You are using Windows 2000 Server or have been directed to install the LAN driver from a specific folder for Windows Server 2003.
- You are using Windows Server 2003 and have not been directed to install the LAN driver from a specific location.

If you are using Windows 2000 Server, or if you have been directed to install the LAN driver from a specific location for Windows Server 2003.

To complete the LAN driver installation or update, perform the following steps.

1. Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.
2. Click **Have Disk** to open the **Install From Disk** dialog box and specify the location of the driver.
   - If you were directed to install the driver from a specific drive and folder, click **Browse** to specify the location, then click **Open**.
   - Otherwise, click **Browse** to specify the location on the system drive (typically C:) of the driver that corresponds to the adapter that you are installing or updating. Use the following list to locate the folder that contains the driver for your specific hardware.
     - `\wsv\ibm` for hardware type 2744
     - `\wsv\alt` for hardware types 2743 and 2760
     - `\wsv` for virtual Ethernet
     - `\wsv\amd` for hardware type 2838 in Windows 2000
     - `\windows\inf` for hardware types 2723 and 2838 in Windows Server 2003
     - `\wsv\itl` for hardware type 2892 in Windows 2000
     - `\wsv` for hardware type 2892 in Windows Server 2003
     - `\wsv\alt` for hardware types 4812, 5700, and 5701 in Windows 2000
     - `\wsv\itg` for hardware type 4812, 5700, and 5701 in Windows Server 2003
3. Click **OK**.
4. In the **Update Device Driver Wizard** dialog box, if the appropriate driver is not already highlighted, select it from the list, then click **Next**.
5. Click **Next** again.
6. If there is a Ret Code 22 when the Update Driver procedure completes, the adapter may be disabled. To enable the adapter in this case, in the **Device Manager** window, right-click the disabled adapter and select **Enable**.
7. If you want to install or update more adapters, see "Select the adapter to install or update" on page 231.

   Note: If Windows indicates that a restart is needed after any driver update, defer it until there are no more adapters to update.
8. If you changed the driver signing policy when you began the installation or update (see "Begin the LAN driver installation or update" on page 231), restore the original policy.

If you are using Windows Server 2003 and you have not been directed to install the LAN driver from a specific location.

To complete the LAN driver installation or update, perform the following steps.

1. Select **Search for a suitable driver for my device** and click **Next**.
2. Click **Next** to show compatible hardware.
3. Deselect all **Optional search locations**, click **Next**, the click **Next** again.
4. If there is a Ret Code 22 when the Update Driver procedure completes, the adapter may be disabled. To enable the adapter in this case, in the **Device Manager** window, right-click the disabled adapter and select **Enable**.
5. If you want to install or update more adapters, see "Select the adapter to install or update" on page 231.

   Note: If Windows indicates that a restart is needed after any driver update, defer it until there are no more adapters to update.
6. If you changed the driver signing policy when you began the driver installation or update (see "Begin the LAN driver installation or update" on page 231), restore the original policy.

Point to point virtual Ethernet IP address conflicts

IBM iSeries Integrated Server Support uses IP addresses in the range of 192.168.x.y for the integrated server's point to point Ethernet network. By default, the actual addresses are selected by the i5/OS Install Windows server (INSWNTSVR) command. For details and examples, see "Assign point to point virtual Ethernet IP addresses" on page 234. Depending on your network, there might be conflicts with addresses that are already in use. To avoid potential conflicts you can use the VRTPTPPORT parameter for an Integrated xSeries Server or the Integrated xSeries Adapter attached xSeries server.

If a conflict requires you to change the addresses, you must ensure that the point to point virtual Ethernet occupies its own subnet on i5/OS. The subnet mask that is used is 255.255.255.0. To ensure that the point to point virtual Ethernet is on its own subnet, use IP addresses of the form a.b.x.y, where a.b.x is the same value for both sides of the point to point virtual Ethernet. Also verify that the value of a.b.x is unique on your network.

To change the point to point virtual Ethernet addresses because of a conflict, take the following action.

1. At the i5/OS console, enter the command `DSPNWSD NWSD(name) OPTION (*PORTS)`. Make a note of the `Attached` line for the port number `*VRTETHPTP`, which is also known as the line description.
2. Use the Configure TCP (CFGTCP) command and option 1 to display the TCP interfaces. Make a note of the IP address and the subnet mask associated with the line description that you found in step 1.

Note: An IP address entered at the Windows console for the point to point virtual Ethernet overrides the values that are set in the NWSD for the TCPPRTCFG parameter `*VRTETHPTP`.

1. Click on **Start—>Settings–>Control Panel**, then **Network and Dial-up Connections**.
2. Right-click the correct **Local Area Connection** for the point to point virtual Ethernet and select **Properties** from the menu.
3. Select **TCP/IP Protocol** from the list of installed protocols and press the **Properties** button to display the TCP/IP properties.
4. Change the IP address for the new value that you have selected.
5. Click **OK**, then **Close** to close the application.
6. Shut down the integrated Windows server without doing a restart.
7. On i5/OS, vary off the NWSD.
8. Use the Remove TCP/IP interface (RMVTCPIFC) command with the IP address you recorded in step 2.
9. Use the Add TCP/IP interface (ADDTCPIFC) command to add the new interface. Use the IP address that you selected for the i5/OS side of the point to point virtual Ethernet. You also need to enter the subnet mask and line description that you recorded in steps 1 and 2.
10. On the i5/OS command line, type `CHGNWSD NWSD(name)`, and press F4.

a. Page down to the section labeled `TCP/IP port configuration`.

b. Change the IP address in the `Internet address` field for the port `*VRTETHPTP` to the value that you used in step 3. Press Enter for the change to take effect.

c. Vary on the NWSD.

Note: If you are installing multiple servers, to avoid further conflicts, assign point to point virtual Ethernet IP addresses (see “Assign point to point virtual Ethernet IP addresses”) instead of letting the INSWNTSVR command generate them. The `Virtual PTP Ethernet port` parameter allows you to enter IP addresses that you know to be unique on your system.

Assign point to point virtual Ethernet IP addresses

By default, the Install Windows server (INSWNTSVR) command assigns point to point virtual Ethernet IP addresses of the form 192.168.x.y. To avoid potential conflicts, you can use the VRTPTPPORT parameter on this command to assign IP addresses that you know are unique on your system.

If you let the command assign addresses and then discover a conflict, you can change the IP addresses. For IXS and IXA attached integrated servers, the command assigns to x a value that is based on the resource number of the Integrated xSeries Server. The command looks for a pair of values y and y+1 (starting with y=1), with addresses that are not in use on that i5/OS. The command assigns the lower number of the pair to the i5/OS side of the point to point virtual Ethernet and the higher number to the Windows server side.

For example, suppose you have a 2892 Integrated xSeries Server with a resource name of LIN03. After running the Install Windows Server (INSWNTSVR) command you might end up with the following addresses for the point to point virtual Ethernet.

```
192.168.3.1 (i5/OS side)
192.168.3.2 (Windows server side)
```

In case of a conflict on a server that you have installed, verify that a particular substitute value (for example, 192.168.17) is not used on your network and change the IP addresses to that value.

```
192.168.17.1 (i5/OS side)
192.168.17.2 (Windows server side)
```

Be aware that an IP address entered at the Windows console for the point to point virtual Ethernet overrides the value set in the NWSD for the TCPPORTCFG parameter *VRTETHPTP port .

If the problem still persists, check the technical information databases at the @server IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider. If the problem persists, contact IBM for service.

Problems with TCP/IP over virtual Ethernet

Verify that the TCP/IP configuration for the point to point virtual Ethernet is correct. If the i5/OS TCP/IP configuration is new or has changed, perform the following procedure to verify that the TCP/IP configuration in Windows is correct.

1. Click **Start** —> **Control Panel** —> **Network Connections** or **Start** —> **Settings** —> **Network and Dial up Connections**.
2. Right click **Network Connections** or **Network and Dial-up Connections** to show a popup menu and select **Open**.
3. Double-click **IBM iSeries Virtual Ethernet point to point Connection**.
4. Click on the **Properties** button.
5. Select the Internet Protocol (TCP/IP)

6. Click on the **Properties** button. If the **Use the Following IP Address** is selected and the IP address from the i5/OS console is displayed, you do not need to proceed any further. If the Obtain an IP address automatically is selected, continue with the next step.
7. Select the radio button: **Use the Following IP Address**.
8. On an i5/OS command line, type the following command, where ’nwsd’ is the name of the NWSD for your server, then press Enter; DSPNWSD NWSD(nwsd) OPTION(*TCPIP)
   - On the DSPNWSD dialog box, find the port named *VRTETHPTP. This shows the IP address and subnet mask values for the point to point virtual Ethernet.
   - On the integrated server console, type the point to point virtual Ethernet IP address and subnet mask values that were shown by the DSPNWSD command.
9. Click OK.
10. Click OK.
11. Click Close.

For information about verifying the TCP/IP configuration in i5/OS and Windows, see “Explore point to point virtual Ethernet networks” on page 113.

The point to point virtual Ethernet used by each active server must use a distinct IP subnet. To learn more about subnet requirements or to change the TCP/IP configuration, see “Point to point virtual Ethernet IP address conflicts” on page 233.

Verify that the iSeries Virtual Ethernet adapters are configured correctly and that they are working.

To troubleshoot a virtual Ethernet adapter, see one of the following topics.
- “Virtual Ethernet problems with iSCSI attached servers” on page 225.
- “Virtual Ethernet problems with IXS and IXA attached servers” on page 227

To verify that a line description is configured correctly for a virtual Ethernet adapter, see Chapter 6, “Manage virtual Ethernet and external networks,” on page 111.

Ensure that a firewall is not interfering.

If a firewall is involved, such as a software firewall running in Windows, it must be configured to allow required traffic.
- For the IP address of the IBM iSeries Virtual Ethernet point to point connection, allow TCP dynamic ports to prevent failure of integrated server administrative applications. Do not use Network Address Translation (NAT).
- For the IP address of an IBM iSeries Virtual Ethernet connection, allow protocols and ports required by your applications.
- For the IP address of an iSCSI HBA connection, see “Configure a firewall” on page 131.

Problems accessing Windows Server 2003 shares using the QNTC file system

If you cannot use the i5/OS QNTC file system to access shares on a Windows Server 2003 server that has Active Directory installed (for example, it is a domain controller), then you may need to do some additional setup. See “Enabling Kerberos with a Windows Server 2003 Active Directory Server” on page 104.

IFS access problems

When you try to access the i5/OS integrated file system (IFS) from an integrated Windows server through iSeries NetServer, the access may fail in the following situation.

- If you are using a Universal Naming Convention (UNC) name with an IP address in it and
- Both point to point virtual Ethernet and external LAN paths exist between the integrated Windows server and i5/OS

Either change the UNC name to use the iSeries NetServer name instead, or disable the external LAN path and then retry the operation that failed.

Problems with saving integrated Windows server files

If you have problems with doing file-level backup of your integrated server files, check the Windows event log and i5/OS QSYSOPR message queue for messages.

- If you get a session initialization error (CPDB050) or session communication error (CPDB055) when you try to save files, do this.
  1. Ensure that i5/OS NetServer is in the same domain (see "Ensure iSeries NetServer and the integrated Windows server are in same domain" on page 194) as the integrated server for which you want to save files.
  2. Ensure that you complete the steps "Create shares on integrated Windows servers" on page 193 and "Add members to QAZLCSAVL file" on page 194.
  3. Ensure that the QSERVER subsystem is running.
  4. Ensure that TCP/IP is active:
     a. Use option 1 of the CFGTCP command.
     b. Press F11 to view the interface status.
     c. Type a 9 next to the appropriate network service to start the TCP/IP interface.
     d. Press F5 to refresh the view. The appropriate TCP/IP service should now be active.
  5. Then try saving your files again.
- If you get an error message that indicates a problem with exchanging security information (CPDB053) or logging on to the server (NTA02AE), do this:
  1. Ensure that you are enrolled on the integrated server as part of the Administrators group.
  2. Ensure that you have the same password on i5/OS and on the integrated server.
  3. Then try saving your files again.
- If you get an error message (CPDB058) that indicates a problem with processing the share file member, ensure that the QAZLCSAVL file is set up correctly.
  1. Check that you have completed this step: "Create shares on integrated Windows servers" on page 193.
  2. As well as this step: "Add members to QAZLCSAVL file" on page 194. Also you must have listed in that file the share that you specified on the Save (SAV) command.
- If you get an error message (NTA02A3) that indicates a problem communicating with NTSAV, verify that the Remote Procedure Call service is running.
  1. On the integrated server task bar, click **Start** —> **Programs** —> **Administrative Tools**.
  2. Double-click **Services**.
  3. Verify that the Remote Command Service is running.
- The following errors may appear when doing a SAV.
  – `CPFA09C Not authorized to object`
  – `CPD3730 Cannot save directory /qntc/(server)/(share)/System Volume Information`

  These errors indicate that the directory, **System Volume Information**, was not saved. This is a hidden, system directory that can be accessed only by the Windows SYSTEM account. If you ignore this message, the directory and its contents will not be saved (it contains intermediate log files used when encrypting files). Otherwise, you can add permissions for the user who is running SAV to this directory. To set the permissions, you will need to make the directory visible (don't hide hidden files, and don't hide protected operating system files). Refer to the Windows 2000 Server or Windows Server 2003 help for information about setting folder permissions.

You may also see a CPFA09C error if you run file-level backup as QSECOFR, whether QSECOFR is enrolled to the server or not. Use a different enrolled user profile that has a backup on the integrated server.

Unreadable messages in the server message queue

Windows event log messages do not display correctly if the message queue coded character set identifier (CCSID) is set to `*HEX (65535)`. If you get unreadable messages in the server message queue (identified by the MSGQ parameter of the NWSD), take the following action.

1. At the i5/OS console, enter the command `CHGMSGQ` to change the server message queue CCSID to something other than `*HEX (65535)`, for example `*MSG`.

   For example, if the message queue name is `MYSVRQ` in library `MYLIB`, then you can use the following command on i5/OS to change the message queue CCSID: `CHGMSGQ MSGQ(MYLIB/MYSVRQ) CCSID(*MSG)`.
2. If the problem still persists, check the technical information databases at the eServer IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

Problems getting a Windows system memory dump

If sufficient space is available on the system drive, your integrated Windows server is automatically configured to collect a system memory dump when a STOP error or blue screen occurs. If a system memory dump is not collected, do the following.

1. Select **Start**, then **Programs**, then **Administrative Tools**.
2. Click on **Computer Management**.
3. In the **Action** menu, click **Properties**.
4. Select the **Advanced** tab
5. Click the **Startup/Recovery** button.
6. Check the **Write debugging information to:** box. The default path to the memory.dmp file that is created when a blue screen occurs is `%SystemRoot%`, which is `C:\WINNT` for Windows 2000 Server and `C:\WINDOWS` for Windows Server 2003.

Other problems that can prevent a system-memory dump from being taken include.

- Insufficient paging file size specified. The paging file size must be large enough to hold all of physical RAM, plus 12 MB. To verify the amount of physical RAM on your machine, do the following.
  1. Select **Start**, then **Settings**, then **Control Panel**.
  2. Double-click **System**. The value listed under **Computer** on the **General** page indicates the amount of physical RAM you have on your system.

  To verify or change the paging file size, do the following.
  1. Select the **Advanced** tab, and click the **Performance Options** button of the **Virtual Memory** section. The **Virtual Memory** part of the window shows the current paging file size.
  2. If you need to change the paging file size, click the **Change** button.
- The paging file is not located on the system drive. A system memory dump is not collected unless the paging file is located on the system drive. The system drive is the C: drive. To verify or change this, do the following.
  1. Select the **Advanced** tab, and click the **Performance Options** button of the **Virtual Memory** section.
- Insufficient space is available on the drive you specified as the path to the memory.dmp file. The default path for the memory.dmp file is the system drive, but you may change it to another drive. Verify that sufficient free space exists on the system drive or the drive you chose if you changed it. The free space needed is equal to the size of physical RAM, plus 12 MB.

- If the problem still persists, check the technical information databases at the eserver IBM iSeries Support Web page . If you cannot find the solution there, contact your technical support provider.

Reinstall an integrated Windows server

If an integrated Windows server becomes damaged, you may be able to preserve installed applications and user data by reinstalling it. Try either logging on or starting up with DOS by using the Boot menu of the NT loader (NTLDR). (This is only possible if the boot drive is still formatted as FAT.) You can then reinstall Windows server. Doing this returns the system to the base level code of Windows server originally installed. You must then reapply any Microsoft service packs that you had installed. You should also reinstall the latest IBM iSeries Integrated Server Support service pack.

To reinstall Windows server, try this.

1. Stop the integrated server. See "Start and stop an integrated server" on page 149
2. At the boot menu, select to boot PC-DOS or Windows server, whichever is working.
3. If you selected Windows server, open an MS-DOS window.
4.
   - For Windows 2000 enter `winnt /s:D:\i386 /u:D:\unattend.txt`
   - For Windows Server 2003 enter `winnt /b /t:C: /s:D:\i386 /u:D:\unattend.txt`
5. In the DOS window, enter this:
   ```
   D:
   cd \i386
   winnt /s:D:\i386 /u:D:\unattend.txt
   ```
6. Press Enter.

Note: The network drives may become so damaged that you cannot log on to the integrated Windows server or start up with DOS. In this case, try restoring all predefined and user-defined storage spaces from usable backups. See "Back up predefined disk drives for integrated Windows servers" on page 188 and "Back up user-defined disk drives for an integrated Windows server" on page 189.

Windows 2000 Server and Windows Server 2003 also provide the Windows Recovery Console, which is a command-line console that provides limited access to the system to perform many administrative tasks or repair the system. Refer to the Windows 2000 Server or Windows Server 2003 documentation for additional information.

You may also have to reinstall from the very beginning by following this procedure: "Start the installation from the i5/OS console" on page 90.

Collect integrated Windows server service data

If you need to supply service data to support personnel, first consult the i5/OS logs (see "Check message and job logs" on page 205) and the Windows event log. You can also make a copy of the Windows event logs on i5/OS (see "Message logging" on page 152) and make Windows server dumps for remote troubleshooting. These topics help you create dumps to collect further diagnostic information.

1. "Create an integrated Windows server memory dump on i5/OS."
2. To find out how this dump can tell you which configuration and log files to look at first, refer to "Use the network server description (NWSD) dump tool on i5/OS" on page 239

Create an integrated Windows server memory dump on i5/OS

You can create a Windows memory dump file on i5/OS to help you solve integrated server problems. When you install Windows server on iSeries, by default the dump goes to the system drive.

- `%SystemRoot%\Memory.Dmp` for Windows Server 2003.

- `%SystemRoot%\Memory.Dmp` for Windows 2000 servers.

Note: For Windows to successfully create a complete memory dump the pagefile must reside on the system drive and be at least equal to the memory size plus 12 megabytes. The memory contents are written into the pagefile during the dump. This is the first step in the memory dump process. During the second step the data from the pagefile is written to the actual dump file. This step occurs when the system is booted again after the dump. The drive that contains the memory dump file (memory.dmp by default) must have free space at least as large as the amount of installed memory.

The memory dump is enabled by default if the system drive has enough room for the paging file. To verify that the memory dump support is enabled or to write the memory.dmp file to a different drive, follow these steps.

1. Go to **Start**, then **Settings**, then **Control Panel**.
2. Open the **System** application.
   - Click the **Advanced** tab, then the **Startup and Recovery** button.
3. Click on the **Write Debugging Information To** check box.
4. Change the location of the dump file if necessary.
5. If you want the system to overwrite the file every time a Kernel STOP Error occurs, click the **Overwrite any Existing File** check box.
6. Select the appropriate type of memory dump (Small Memory Dump, Kernel Memory Dump, or Complete Memory Dump) based on the size of the page file and the amount of free space available on the system drive.
7. Click **OK**.

Use the network server description (NWSD) dump tool on i5/OS

You can use the network server description (NWSD) dump tool (QFPDMPLS) to dump the different configuration and log files that are used with your integrated Windows server. To do this you need *ALLOBJ special authority.

To do this, take these steps:

1. Vary off the NWSD (see “Start and stop an integrated server” on page 149).
2. At the i5/OS command line, type

   ```
   CALL QFPDMPLS PARM(nwsdname)
   ```

   where nwsdname is the network server description name.

   The program creates a database file QGPL/QFPNWSDMP with multiple members. Each database file member name has the NWSD name followed by two digits (01 - 99). For example, for an NWSD named MYSERVER, the first member name would be MYSERVER01.
3. Display the member to see the contents of the different files associated with your server description. Different files are important for problem analysis, depending on which installation step is causing a problem.
4. Refer to the following table to note the importance of each file during a particular installation step. If a file is marked 1, refer to it first during problem analysis, 2 second, and 3 last. Files that are not marked are not relevant to installation, but may be relevant at other times. Some members are not created until the post-installation phase.

Note: You cannot use QFPDMPLS to retrieve files on the system drive if you convert the drive to NTFS.

You may not find all the files listed below on some servers. If a particular file is not found, the file will not be retrieved by the QFPDMPLS API and the corresponding database member will not be created.

NWSD configuration and log files

Member Name	Data Type	File Name	Windows Directory	Install	Post-Install
nwsdname01	Txt	CONFIG.SYS	C:\	3	3
nwsdname02	Txt	AUTOEXEC.BAT	C:\	2	2
nwsdname03	Txt	BOOT.INI	C:\		
nwsdname04	Txt	HOSTS	C:\ or D:\		3
nwsdname05	Txt	QVNI.CFG	C:\ or D:\		
nwsdname06	Txt	QVNACFG.TXT	C:\ or D:\		
nwsdname07	Txt	QVNADAEM.LOG	C:\ or D:\		
nwsdname08	Txt	DUMPFILE.C01	C:\		
nwsdname09	Bin	DUMPFILE.C01	C:\		
nwsdname10	Txt	DUMPFILE.C02	C:\		
nwsdname11	Bin	DUMPFILE.C02	C:\		
nwsdname12	Txt	UNATTEND.TXT	D:\	1	
nwsdname13	Txt	INSWNTSV.LNG	D:\	2	
nwsdname14	Txt	INSWNTSV.VER	D:\	2	
nwsdname15	Txt	QVNADAEM.LOG	D:\		
nwsdname16	Txt	QVNARCMD.LOG	D:\		
nwsdname17	Txt	QVNDT400.LOG	D:\		
nwsdname18	Txt	QVNDVSTP.LOG	D:\		
nwsdname19	Txt	QVNDVSCD.LOG	D:\		
nwsdname20	Txt	QVNDVSDD.LOG	D:\		
nwsdname21	Txt	EVENTSYS.TXT	D:\		
nwsdname22	Txt	EVENTSEC.TXT	D:\		
nwsdname23	Txt	EVENTAPP.TXT	D:\		
nwsdname24	Txt	PERFDATA.TSV	D:\		
nwsdname25	Txt	REGSERV.TXT	D:\		
nwsdname26	Txt	REGIBM.TXT	D:\		
nwsdname27	Txt	REGIBMCO.TXT	D:\		
nwsdname28	Txt	DUMPFILE.D01	D:\		
nwsdname29	Bin	DUMPFILE.D01	D:\		
nwsdname30	Txt	DUMPFILE.D02	D:\		
nwsdname31	Bin	DUMPFILE.D02	D:\		
nwsdname32	Txt	HOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname33	Txt	LMHOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname34	Bin	MEMORY.DMP	C:\WINNT		
nwsdname35	Txt	VRMFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\VRM		
nwsdname36	Txt	PTFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname37	Txt	PTFUNIN.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname38	Txt	A4EXCEPT.LOG	D:\		
nwsdname39	Txt	DUMPFILE.E01	E:\		
nwsdname40	Bin	DUMPFILE.E01	E:\		
nwsdname41	Txt	DUMPFILE.E02	E:\		
nwsdname42	Bin	DUMPFILE.E02	E:\		
nwsdname43	Txt	CMDLINES.TXT	D:\I386\OEM	2	
nwsdname44	Txt	QVNABKUP.LOG	D:\AS400NT		
nwsdname45	Txt	QVNADAEM.LOG	D:\AS400NT		
nwsdname46	Txt	QCONVGRP.LOG	D:\AS400NT		
nwsdname47	Txt	SETUPACT.LOG	C:\WINNT	1	
nwsdname48	Txt	SETUPAPI.LOG	C:\WINNT	1	
nwsdname49	Txt	SETUPERR.LOG	C:\WINNT	1	
nwsdname50	Txt	SETUPLOG.TXT	C:\WINNT	1	

Member Name	Data Type	File Name	Windows Directory	Install	Post-Install
nwsdname51	Txt	VRMFLOG.TXT	D:\AS400NT		
nwsdname52	Txt	PTFLOG.TXT	D:\AS400NT		
nwsdname53	Txt	PTFUNIN.TXT	D:\AS400NT		
nwsdname54	Txt	VRMLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\VRM		
nwsdname55	Txt	PTFLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname56	Txt	PTFUNIN.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname57	Txt	QVNDVEU.LOG	D:\AS400NT		
nwsdname58	Txt	SERVICE.LOG	D:\AS400NT		
nwsdname59	Txt	LVDELOEM.LOG	D:\AS400NT		
nwsdname60	Txt	INVOKINF.LOG	D:\AS400NT		
nwsdname61	Txt	LVMASTER.LOG	D:\AS400NT		
nwsdname62	Txt	QITDINST.LOG	D:\AS400NT		
nwsdname63	Txt	QVNDVIMR.LOG	D:\AS400NT		
nwsdname64	Txt	QVNDVIMC.LOG	D:\AS400NT		
nwsdname65	Txt	QVNDSDMR.LOG	D:\AS400NT		
nwsdname66	Txt	QVNDSDMC.LOG	D:\AS400NT		
nwsdname67	Txt	QVNILMGR.LOG	D:\AS400NT		

Chapter 15. Network server description configuration files

You can customize your integrated Windows servers by creating your own configuration files. For example, you might want to change screen resolution or suppress installation of the IPX protocol. You can do this by following these steps.

1. Create an NWSD configuration file. See "Network server descriptions" on page 67.
2. Specify this file with the `Configuration file` parameter when you install a server or create or change a network server description.

Each time the network server starts, i5/OS uses the configuration file to change the specified integrated server file on the server's C or D drive.

When the Install Windows server (INSWNTSVR) command activates the integrated server, it generates a Windows unattended installation setup script file (UNATTEND.TXT). By specifying your configuration file on the INSWNTSVR command, you can use this file during the installation to modify the UNATTEND.TXT file.

Attention: Be careful what you change with configuration files. Avoid removing device drivers from UNATTEND.TXT, for example, or changing the OEM section or the section that installs TCP. Otherwise, your changes might prevent your server from starting. If you are creating a configuration file to modify an installed server, first make a backup copy of whatever files you plan to change.

- To see how your system drive is formatted, you can use the Work with Network Server Storage Spaces Command (WRKNWSSTG) command.
- Before creating a configuration file, read "NWSD configuration file format." This section tells you how to use each entry type.
- You should also read this topic, "Use substitution variables for keyword values" on page 253, to see what variables are available for you to use and how to create your own list.
- You might also want to read: "Example: NWSD configuration file" on page 244.
- Then you are ready to follow this procedure: "Create an NWSD configuration file" on page 244.

If you have problems starting a server after you create a configuration file, see "NWSD configuration file errors" on page 215.

NWSD configuration file format

An NWSD configuration file consists of multiple occurrences of **entry types**, each with a different function. The entry types are:

"Remove lines from an existing integrated server file with CLEARCONFIG entry type" on page 245
Use this entry type if you want to remove all lines from the integrated server file.

"Change an integrated server file with ADDCONFIG entry type" on page 246
Use this entry type to add, replace, or remove lines in the integrated server file.

"Change an integrated Windows server file with UPDATECONFIG entry type" on page 250
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 251
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.

Create an NWSD configuration file

Before creating a configuration file, read the topics “NWSD configuration file format” on page 243 and “Use substitution variables for keyword values” on page 253. You might also want to read “Example: NWSD configuration file.”

To create an NWSD configuration file, do this:

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 243. 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

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'                     |
| *                                                                              |
|                                                                                |
+--------------------------------------------------------------------------------+
```

Remove lines from an existing integrated server 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. If you have problems, see “NWSD configuration file errors” on page 215.

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 243, or on to “Change an integrated server file with ADDCONFIG entry type” on page 246.

- “LINECOMMENT keyword” on page 248
- “TARGETDIR keyword”
- “TARGETFILE keyword” on page 246

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.

Change an integrated server file with ADDCONFIG entry type

You can use the ADDCONFIG entry type to change an integrated Windows 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 243 or on to the “Change an integrated Windows server file with UPDATECONFIG entry type” on page 250.

- “VAR keyword”
- “ADDSTR keyword” on page 247
- “ADDWHEN keyword” on page 247
- “DELETEWHEN keyword” on page 248
- “LINECOMMENT keyword” on page 248
- “LOCATION keyword” on page 248
- “FILESEARCHPOS keyword (ADDCONFIG entry type)” on page 248
- “FILESEARCHSTR keyword” on page 249
- “FILESEARCHSTROCC keyword” on page 249
- “REPLACEOCC keyword” on page 249
- “TARGETDIR keyword” on page 249
- “TARGETFILE keyword” on page 250
- “UNIQUE keyword” on page 250

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 Windows server 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 integrated Windows server 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 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”) 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

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.

Operator	Description
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 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 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" on page 247) 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 file. 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. 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

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. See “Predefined disk drives for integrated Windows servers” on page 162.
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

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

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 Windows 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 243 or on to “Set configuration defaults with the SETDEFAULTS entry type” on page 251.

- "VAR keyword" on page 246
- "ADDSTR keyword" on page 247
- "ADDWHEN keyword" on page 247
- "DELETEWHEN keyword" on page 248
- "LINECOMMENT keyword" on page 248
- "LINELOCATION keyword" on page 248
- "LINESEARCHPOS keyword" on page 248
- "LINESEARCHSTR keyword" on page 248
- "FILESEARCHPOS keyword (UPDATECONFIG entry type)"
- "FILESEARCHSTR keyword (UPDATECONFIG entry type)"
- "FILESEARCHSTROCC keyword (UPDATECONFIG entry type)"
- "TARGETDIR keyword" on page 249
- "TARGETFILE keyword" on page 250
- "VAROCC keyword" on page 250
- "VARVALUE keyword" on page 250

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. Use the value:

- 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”
- “DELETEWHEN”
- “FILESEARCHPOS keyword (SETDEFAULTS entry type)” on page 253
- “FILESEARCHSTR keyword (SETDEFAULTS entry type)” on page 253
- “TARGETDIR” on page 253
- “TARGETFILE” on page 253

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 247) 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 247) 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'
```

Use 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) *

Substitution variable	Description
%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
%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:
1234567890123456789012345678901234567890123456789 0...
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″.

Chapter 16. Related information

Listed below are the iSeries manuals and IBM Redbooks (in PDF format), Web sites, and Information Center topics that relate to the Windows Environment on iSeries topic. You can view or print any of the PDFs.

Manuals

- iSeries Performance Capabilities Reference
- Backup and Recovery
- Hardware installation instructions. See the “Install iSeries features” topic.

Redbooks (www.redbooks.ibm.com)

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959

IBM xSeries and BladeCenter Server Management, SG24-6495

Web Sites

- Latest product and service information: System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/)
- iSeries Performance Management (www.ibm.com/eserver/iseries/perfmgmt)
- IXA install read me first (www.ibm.com/systems/i/bladecenter/ixa/readme/)
- iSCSI install read me first (www.ibm.com/systems/i/bladecenter/iscsi/readme/)
- IXS install read me first (www.ibm.com/systems/i/bladecenter/ixs/readme/)
- Troubleshooting (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

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
AS/400
BladeCenter
DB2
IBM
iSeries
Netfinity
NetServer
OS/400
i5/OS
PAL
Redbooks
ServerGuide
Virtualization Engine
xSeries

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, and 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.

Printed in USA