



System i

System i integration with BladeCenter and System x: IXS and IXA-attached integrated Windows servers

Version 6 Release 1





System i

System i integration with BladeCenter and System x:
IXS and IXA-attached integrated Windows servers

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in “Notices,” on page 137.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-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.

© Copyright International Business Machines Corporation 1998, 2008. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

What's new for V6R1 1

IXS or IXA-attached integrated Windows servers 3

Integrated server concepts	3
Integrated server overview	4
Integrated server advantages	5
Integrated server terminology	6
Integrated server hardware concepts	8
IXS and IXA attached servers	10
Windows console for integrated servers	13
Integrated server considerations	14
Integrated server performance concepts	14
Storage performance for integrated servers	14
Storage space balancing for integrated servers	15
Virtual Ethernet performance for integrated servers	16
Networking concepts for IXS and IXA-attached integrated servers	16
Point to point virtual Ethernet for integrated servers	16
Virtual Ethernet networks for integrated servers	17
External networks for IXS and IXA-attached integrated servers	21
Software concepts for IXS and IXA-attached integrated servers	21
Integrated servers that use integrated xSeries Server (IXS) and Integrated xSeries Adapter (IXA)-attached System x hardware.	22
Network server description for IXS and IXA-attached integrated servers.	23
Hardware resource name for IXS and IXA-attached integrated servers.	24
Network server storage spaces for IXA-attached and IXS integrated servers.	24
Virtual Ethernet line descriptions for IXS and IXA-attached integrated servers	25
TCP/IP interfaces for IXS and IXA-attached integrated servers	25
System bus and HSL data flows for IXS and IXA-attached integrated servers	25
High availability concepts for IXS and IXA-attached integrated servers.	26
Security concepts for IXS and IXA-attached integrated servers	26
User and group concepts for integrated Windows servers	26
User accounts for integrated servers	28
User enrollment templates for integrated servers	30
i5/OS password considerations for integrated servers	31
Installing and configuring IXS and IXA-attached integrated Windows servers	31

Hardware requirements for integrated servers	32
Software requirements for IXS and IXA-attached integrated servers	34
Preparing for the installation of integrated Windows servers	34
Memory requirements for integrated servers	36
Configuring time synchronization for integrated Windows servers	36
Configuring i5/OS TCP/IP for integrated Windows servers	37
Using System i Access for Windows with integrated Windows servers	37
Enabling i5/OS NetServer	38
Planning for a Windows user with authorities to access i5/OS NetServer	38
Installing IBM i5/OS Integrated Server Support	39
Planning for the installation of Windows server	39
Network server descriptions.	40
Installation worksheet for i5/OS parameters	40
Comparison of FAT, FAT32, and NTFS file systems.	53
Finding hardware resource names when you have multiple integrated servers	53
Supported language versions	53
Installing Windows 2000 Server or Windows Server 2003	54
Starting the operating system installation from the i5/OS console	54
Continuing the operating system installation from the integrated Windows server console	56
Completing the integrated server operating system installation	57
Upgrading the IBM i5/OS Integration for Windows Server licensed program.	58
Preparing to Upgrade i5/OS Integrated Server Support	58
After upgrading IBM i5/OS Integrated Server Support	58
Upgrading the integrated server side of IBM i5/OS Integrated Server Support	59
Migrating from 285x or 661x to 2890	60
Integrated xSeries Server hardware	60
Windows Cluster Service	60
Installing Windows Cluster service	61
Installing Windows Cluster service on a new integrated Windows server	61
Installing Windows Cluster service on an existing server	62
Preparing Windows before installing Windows Cluster service on your integrated server	63
Installing Windows Cluster service on the Windows operating system	64
Enabling Kerberos with a Windows Server 2003 Active Directory Server.	66

Installing the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server	66	Connecting to the virtual serial console from a DOS command prompt	78
Adjusting hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server	67	Viewing or changing integrated Windows server configuration information	79
Responding to error messages during installation	67	Finding integrated server message logs	79
Setting an integrated Windows server to automatically vary on with TCP/IP	68	Running integrated Windows server commands remotely	80
Code fixes	68	Guidelines for submitting remote commands to your integrated Windows server	80
Types of code fixes	69	SBMNWSCMD and file level backup support for Kerberos v5 and EIM	82
Synchronizing the integration software level using the integrated Windows server console	69	Using hot spare integrated server hardware	83
Synchronizing the integration software level by using System i Navigator.	70	Switching to hot spare integrated server hardware using System i Navigator	83
Updating the integration software: System i Navigator	70	Switching to hot spare integrated server hardware using the character-based interface	83
Synchronizing the integration software level using a remote command.	70	Managing storage for integrated servers	83
Managing virtual Ethernet and external networks for integrated servers	71	i5/OS storage management for integrated servers	84
Configuring IP address, gateway and MTU values for integrated servers.	71	Disks for integrated Windows servers	85
Configuring virtual Ethernet networks for integrated servers	72	Predefined disks for integrated Windows servers	87
Configuring inter-partition virtual Ethernet networks for integrated servers.	72	Administering integrated Windows server disk drives from i5/OS	87
Configuring inter-partition networks with the Hardware Management Console	73	Accessing the i5/OS integrated file system from an integrated server.	87
Configuring Inter-partition networks without the Hardware Management Console	73	Viewing information about integrated server disk drives	88
Managing point to point virtual Ethernet networks for integrated servers.	74	Adding disk drives to integrated Windows servers	88
Viewing point-to-point virtual Ethernet connections from i5/OS	74	Creating an integrated server disk drive.	88
Viewing point to point virtual Ethernet connections from the integrated Windows server console	74	Linking a disk drive to an integrated server	89
Configuring external networks for integrated servers	75	Formatting integrated server disk drives.	90
Installing network adapter device drivers and adding adapter address information to an integrated Windows server	75	Copying an integrated server disk drive.	90
Removing network adapters from an integrated Windows server	75	Expanding an integrated server disk drive	91
Administering integrated Windows servers.	76	Expanding an integrated Windows server system drive	92
Starting and stopping an integrated server	76	Unlinking integrated Windows server disk drives	92
Starting and stopping an integrated Windows server using System i Navigator	76	Deleting integrated Windows server disk drives	92
Starting and stopping an integrated Windows server using the character-based interface	76	Deleting a disk when removing an integrated server	93
Shutting down an integrated server from the Windows console	77	Windows disk management programs and integrated Windows servers	93
Shutting an integrated server from the Windows console	77	Sharing devices between i5/OS and integrated servers	93
Shutting down your System i hardware when integrated Windows servers are present	77	Finding the device description and hardware resource names for System i devices	93
Connecting to the 4812 IXS virtual serial console	78	Using System i optical drives with integrated Windows servers	94
Connecting to a virtual serial console using the IBM Personal Communications client	78	Locking an optical device.	94
		Transferring control of an optical drive from i5/OS to an integrated server	94
		Transferring control of an optical device from an integrated server to i5/OS	95
		Using System i tape drives with an integrated Windows server	95
		Installing tape device drivers for integrated Windows servers	96
		Formatting a tape on i5/OS for use with integrated Windows servers	96

Allocating a System i tape drive to an integrated Windows server	96	Configuring an integrated Windows server for file-level backup	114
Returning control of a tape drive from an integrated Windows server to i5/OS	97	Creating shares on integrated Windows servers	114
Tested System i tape devices.	97	Adding members to the QAZLCSAVL file	115
Identifying System i tape devices for applications	98	Ensuring i5/OS NetServer and the integrated Windows server are in same domain	115
Transferring control of System i tape and optical drives between integrated Windows servers	98	Saving your integrated Windows server files	116
Printing from an integrated Windows server to System i printers	99	Examples: Saving parts of integrated Windows servers	116
Administering integrated Windows server users from i5/OS	99	Using the Windows Backup utility on your integrated Windows server	117
Enrolling a single i5/OS user to an integrated Windows server using System i Navigator	99	Restoring the NWSD and disk drives for an integrated Windows server	117
Enrolling an i5/OS group to your integrated Windows server using System i Navigator.	100	Restoring predefined disk drives for integrated Windows servers	118
Enrolling i5/OS users to an integrated Windows server using the character-based interface	100	Restoring user-defined disk drives for integrated Windows server	119
Creating user templates for integrated Windows servers	101	Restoring integrated Windows server NWSDs	119
Creating user profiles for a Windows 2000 Server or Windows Server 2003 domain	101	Restoring integrated Windows server files.	120
Creating user profiles on Windows 2000 Server or Windows Server 2003 server	101	Uninstalling the Windows server operating system from the integrated server hardware.	121
Specifying a home directory in a template.	102	Deleting the NWSD for an integrated Windows server	121
Changing the LCLPWDMGT user profile attribute	102	Deleting line descriptions for integrated Windows servers	122
Enterprise Identity Mapping (EIM)	102	Deleting TCP/IP interfaces associated with an integrated Windows server.	122
End user enrollment to integrated Windows servers	104	Deleting controller descriptions associated with integrated Windows servers	122
Ending group enrollment to an integrated Windows server	104	Deleting device descriptions associated with an integrated Windows server.	123
The QAS400NT user	105	Uninstalling IBM i5/OS Integrated Server Support	123
Preventing enrollment and propagation to an integrated Windows server	107	Network server description configuration files	123
Using the PRPDMNUSR parameter to prevent enrollment to a domain through a specific integrated server	107	NWSD configuration file format	124
Using the CRTDTAARA command to prevent enrollment of QAS400NT to a specific integrated server	108	Creating an NWSD configuration file for your integrated server	124
Backing up and recovering IXS or IXA-attached integrated Windows servers	108	Example: NWSD configuration file for an integrated server	125
Backing up the NWSD and other objects associated with integrated Windows servers	109	Removing lines from an existing integrated server configuration file with CLEARCONFIG entry type	125
Backing up the NWSD of an integrated Windows server	109	TARGETDIR keyword	126
Backing up predefined disk drives for integrated Windows servers	109	TARGETFILE keyword	126
Backing up user-defined disk drives for integrated Windows servers	110	Changing an integrated server file with ADDCONFIG entry type	126
Saving and restoring user enrollment information for integrated Windows servers	111	VAR keyword	127
What objects to save and their location on i5/OS	111	ADDSTR keyword	127
Backing up individual integrated Windows server files and directories	113	ADDWHEN keyword	127
File-level backup restrictions for integrated Windows servers	113	ADDWHEN and DELETEWHEN expression operators	127
		DELETEWHEN keyword	128
		LINECOMMENT keyword	128
		LOCATION keyword.	128
		LINESEARCHPOS keyword	129
		LINESEARCHSTR keyword	129
		LINELOCATION keyword	129
		FILESEARCHPOS keyword (ADDCONFIG entry type)	129

FILESEARCHSTR keyword.	129	Set configuration defaults with the	
FILESEARCHSTROCC keyword	129	SETDEFAULTS entry type	132
REPLACEOCC keyword	129	ADDWHEN.	132
TARGETDIR keyword	130	DELETEWHEN	133
TARGETFILE keyword	130	FILESEARCHPOS keyword (SETDEFAULTS	
UNIQUE keyword.	130	entry type)	133
VAROCC keyword	130	FILESEARCHSTR keyword (SETDEFAULTS	
VARVALUE keyword.	130	entry type)	133
Change an integrated server file with		TARGETDIR.	133
UPDATECONFIG entry type	130	TARGETFILE	133
FILESEARCHPOS keyword		Use substitution variables for keyword values	134
(UPDATECONFIG entry type).	131		
FILESEARCHSTR keyword			
(UPDATECONFIG entry type).	131		
FILESEARCHSTROCC keyword			
(UPDATECONFIG entry type).	132		

Appendix. Notices 137

Trademarks	138
Terms and conditions.	139

What's new for V6R1


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

Changes to IXS and IXA-attached integrated Windows servers

- Use the Disable User Profile (DSBUSRPRF) value on the Install Windows Server command or the Network Server Description to specify that user profiles will not be disabled on the Windows operating system when they are disabled on the i5/OS operating system. See “User and group concepts for integrated Windows servers” on page 26.
- A new value for time synchronization is supported. Specify None to ensure that the integrated server time is never synchronized with the i5/OS[®] time. See “Configuring time synchronization for integrated Windows servers” on page 36.
- The Windows Server Installation Advisor no longer supports IXS and IXA-attached integrated servers. Use the “Installation worksheet for i5/OS parameters” on page 40 to select parameters for the Install Window Server (INSWNTSVR) command.

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



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

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

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

How to see what's new or changed

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

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

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

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

IXS or IXA-attached integrated Windows servers

Configure i5/OS and the Microsoft® Windows® operating system to work with System i hardware.

Integrated servers contain both software and hardware components. They enabled a System i product and x86-based Personal Computers (PCs) to work together, and what is more, to allow the System i server to control PCs in order to make them easier to administer.

The first part of an integrated Windows server is the PC hardware which must be added to the System i. There are three basic ways of doing this.

- By using an Integrated xSeries® Adapter, the System i can control IBM® System x x86-based PC hardware.
- An *Integrated xSeries Server (IXS)* is an System i expansion card which contains Random Access Memory (RAM) and a processor. It can be thought of as a PC which has been transplanted inside the frame of a System i product.

The second part is the IBM i5/OS Integrated Server Support (5761-SS1 option 29) option which is installed on i5/OS to give it the capability to control PCs. These PCs are then called integrated Windows servers.

Finally, it is necessary to install the Microsoft Windows 2000 Server or Microsoft Windows Server 2003 operating system.

Integrated server concepts

Understand how to configure an integrated Windows server solution with Integrated xSeries Adapter (IXA) or Integrated xSeries Server (IXS) hardware.

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 IXS or a System x product attached to a System i product with an IXA. Just as the term PC is often used to refer to Microsoft's Windows operating system software running on an x86-based microprocessor and associated hardware, integrated Windows server refers to the combination of hardware and software which make up the entire solution.

Integrated server overview

An integrated server is a combination of hardware and software components.

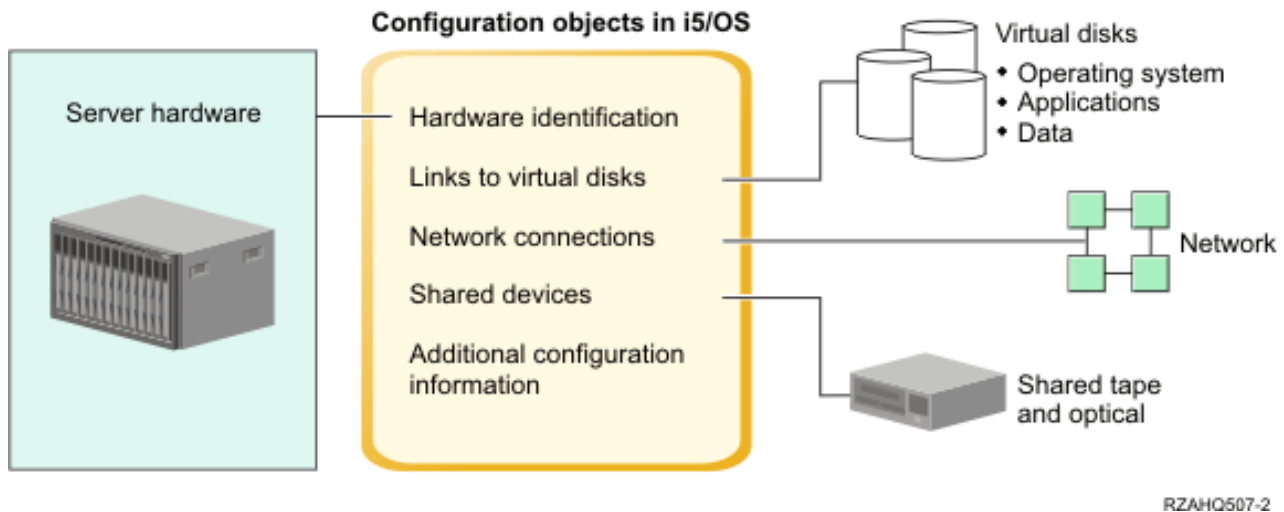


Figure 1. Integrated server overview

Server hardware

The server hardware is the physical hardware (such as the processor and memory) that the integrated server runs on. There are several types of server hardware that can be used for integrated servers, depending on your needs. The server hardware can take the form of a card that plugs into your System i product, an external System x product that is attached to an System i product with an Integrated xSeries Adapter (IXA), or an external System x or BladeCenter system that is attached to an System i product with an iSCSI host bus adapter. The integrated server can also use tape and optical devices that are connected to the hosting i5/OS partition. See "Integrated server hardware concepts" on page 8 for more information about the types of hardware that can be used for integrated servers.

Network

Each integrated server has one or more connections to a network. Both physical network connections with a network adapter and System i virtual Ethernet network connections are supported. See "Networking concepts for IXS and IXA-attached integrated servers" on page 16 for more information about the types of network connections that can be used with integrated servers.

Virtual disks

Each integrated server uses virtual disks that contain the server's operating system, applications, and data. These virtual disks are allocated from i5/OS disk storage. The integrated server treats these virtual disks as physical disks that are contained within the server. However, the integrated server does not actually have any physical disks of its own. See "Software concepts for IXS and IXA-attached integrated servers" on page 21 for more information about virtual disks.

Shared devices

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

i5/OS integrated server configuration objects

Configuration objects in i5/OS describe each integrated server. The i5/OS configuration objects identify the hardware that the integrated server runs on, the virtual disk drives that the integrated server uses, the virtual Ethernet connections that the integrated server uses, and many other attributes of the server. See “Software concepts for IXS and IXA-attached integrated servers” on page 21 for more information about the i5/OS configuration objects that describe an integrated server.

Integrated server advantages

System i integration with BladeCenter and System x provides most of the capabilities of running Microsoft Windows on a PC-based server and provides several advantages over other types of 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 System i disk storage, which is generally more reliable than PC server hard disks.
- You have access to faster System i tape devices for integrated server backups.
- You can back up the entire Windows server as part of your i5/OS backup. This allows you to recover a failed server much faster and easier than with typical file level recovery from the Microsoft Windows operating system.
- Integrated servers implicitly take advantage of superior data protection schemes which exist in i5/OS such as RAID or drive mirroring.
- Typical integrated server configurations have storage space data spread across more System i disks 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® for i5/OS data through an enhanced Open Database Connectivity (ODBC) device driver using System i Access. This device driver enables server-to-server applications between integrated servers and the i5/OS operating system.
- 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 System i 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 the i5/OS operating system. 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 the i5/OS operating system 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)

- You have considerably more flexibility in configuring a full size System x than you have in configuring an Integrated xSeries Server (IXS).
- Full size System x models are released more often, meaning that you can get the most up-to-date x86 processors and other hardware.
- More PCI feature cards are available for full size System x servers than for IXSs.

BladeCenter server attached via an iSCSI host bus adapter

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

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

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 System x server or IBM BladeCenter system without restarting your System i product. This may reduce the overall number of x86 systems needed to provide increased availability.
- Hot spare support also adds flexibility by enabling one spare server to be used to protect multiple production servers.

Integrated server terminology

Use this information to understand terminology for integrated servers that use IXA and IXS hardware.

Baseboard Management Controller (BMC)

A basic low function service processor that is used to control System x products.

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.

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 System i 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**.

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 “Using hot spare integrated server hardware” on page 83.

IBM i5/OS Integrated Server Support

Extension to the i5/OS operating system installed on the System i product 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 BladeCenter server, or an iSCSI HBA attached System x or BladeCenter server.

Integrated xSeries Server (IXS)

A PC (Intel-based computer) on a PCI expansion card that installs inside an System i product.

Integrated xSeries Adapter (IXA)

A PCI expansion card that installs inside selected models of System x products, providing a high-speed link to a System i product.

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. System i 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).

MAC See Media Access Control.

Management Module

A high function service processor that is used to control an 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 description (NWSD)

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

network server storage space (NWSSTG)

i5/OS disk storage allocated to an integrated server.

point to point virtual Ethernet

A virtual Ethernet network configured between a System i product and an integrated Windows server during its installation. It is the link that is used for communication between the System i product and an integrated server.

Remote Supervisor Adapter (RSA)

A high function service processor that is used to control System x products.

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 System x products. See **Remote Supervisor Adapter (RSA)**, **Baseboard Management Controller (BMC)** and **Management Module**.

virtual network


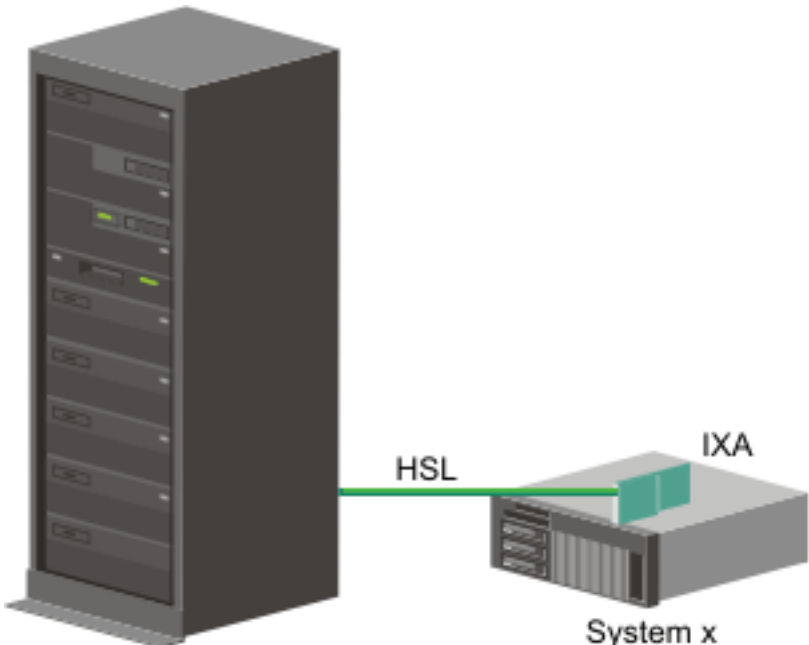
An Ethernet network emulated inside the System i product to allow networks to be created between i5/OS logical partitions, Linux logical partitions, and integrated Windows servers.

Integrated server hardware concepts

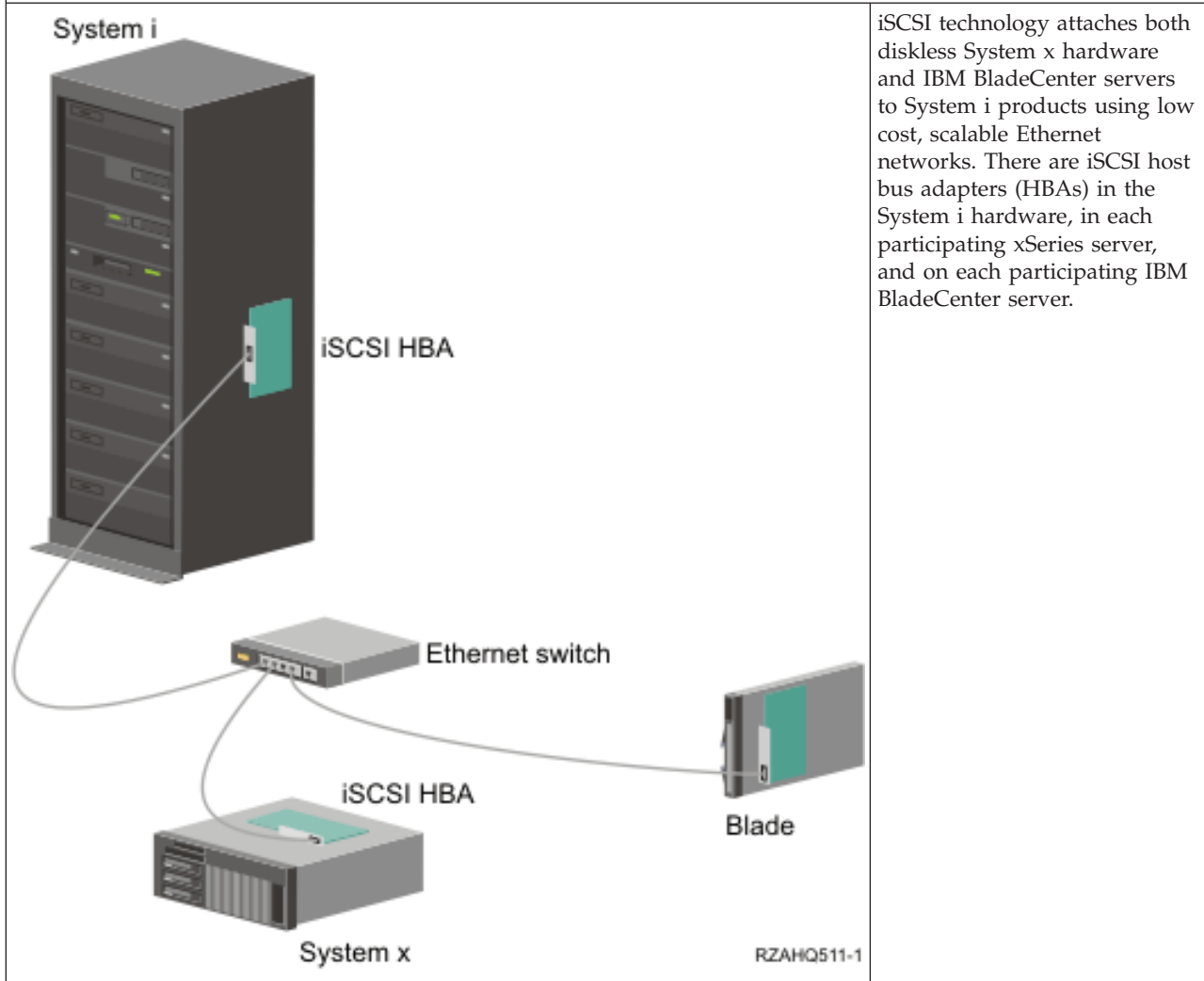
System i products support several hardware configurations to integrate System x or BladeCenter servers.

The following table introduces the essential differences between an Integrated xSeries Server (IXS), an Integrated xSeries Adapter (IXA) attached System x product, and an iSCSI-attached server.

Comparison of IXS, IXA and iSCSI HBA attached System x servers.

 <p>System i</p> <p>RZAHQ019-2</p>	<p>An IXS is a diskless PC Server with processor and memory that is installed inside a System i product.</p>
 <p>System i</p> <p>System x</p> <p>RZAHQ020-2</p>	<p>An IXA is a high-speed link (HSL) bus adapter plugged into a supported System x server. The System x hardware appears as an HSL attached expansion unit to the System i hardware.</p>

Comparison of IXS, IXA and iSCSI HBA attached System x servers.



iSCSI technology attaches both diskless System x hardware and IBM BladeCenter servers to System i products using low cost, scalable Ethernet networks. There are iSCSI host bus adapters (HBAs) in the System i hardware, in each participating xSeries server, and on each participating IBM BladeCenter server.

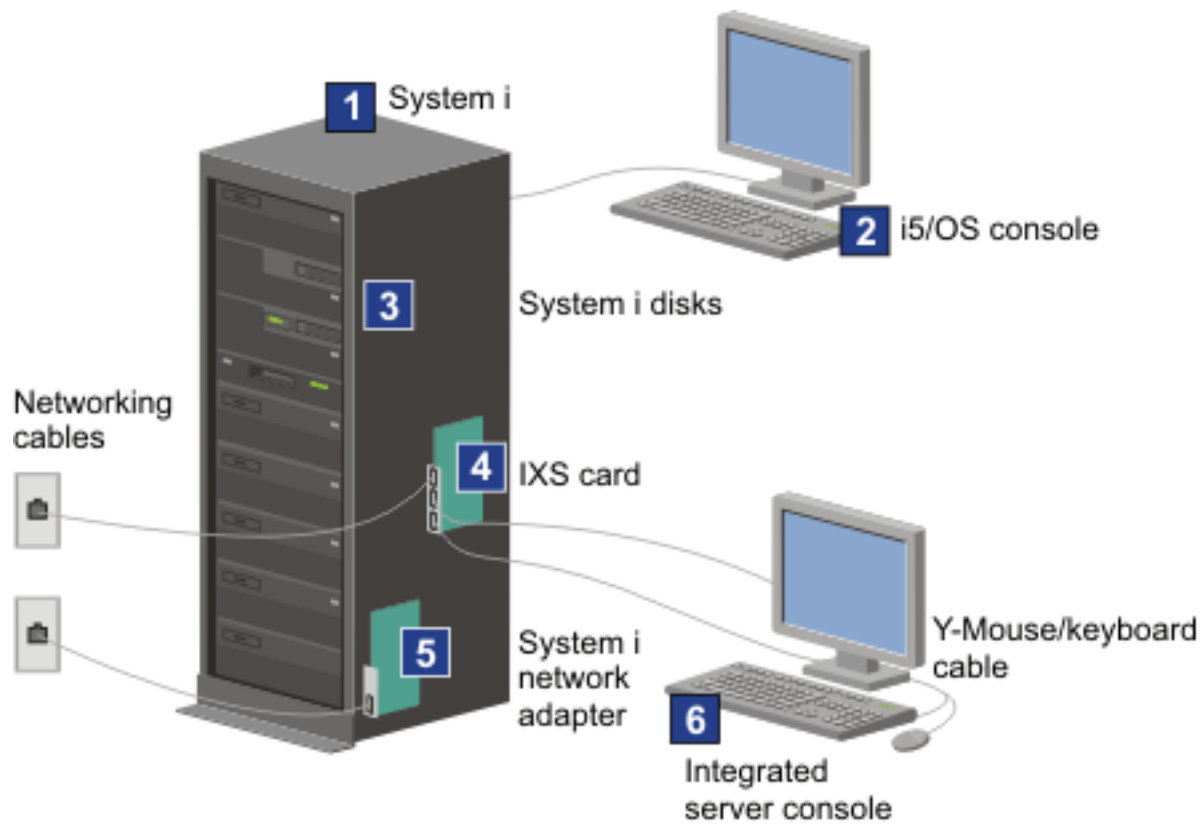
IXS and IXA attached servers

There are several types of hardware that you can use for an integrated server.

You can use an Integrated xSeries Server (IXS) hardware for your integrated server. You can also attach an System x server with an Integrated xSeries Adapter (IXA) or you can attach an System x or BladeCenter server with an iSCSI HBA.

Typical IXS server installation

The following graphic illustrates a typical IXS installation.



RZAHQ025-1

Figure 2. A typical IXS installation

1. You need a compatible System i product. (See “Hardware requirements for integrated servers” on page 32 for compatibility information.)
2. The i5/OS console, from which you connect to the System i product using System i Navigator or the character-based interface, is shown to make clear the distinction between it and the integrated server console.
3. An integrated server does not have its own hard disk drive. i5/OS emulates hard disk space for it to use from the System i disks.
4. The IXS card is an Intel® processor with its own RAM, mounted on a PCI board and plugged into a System i expansion slot. The IXS physically occupies two slots.
5. A typical System i product will have a network card.
6. An integrated server console allows you to interact with the integrated server. An integrated server console might 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 for integrated servers” on page 13.

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 a System i network card (see “Hardware requirements for integrated servers” on page 32 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 System x models, containing processors, memory, and expansion cards, but no disks. All the disk space is housed in the System i product 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 System x products are released more often than IXSs, updated capabilities are available more rapidly. IXA-attached System x products also have their own expansion slots, so they are far more expandable than IXSs.

The following graphic illustrates a typical IXA attached server installation.

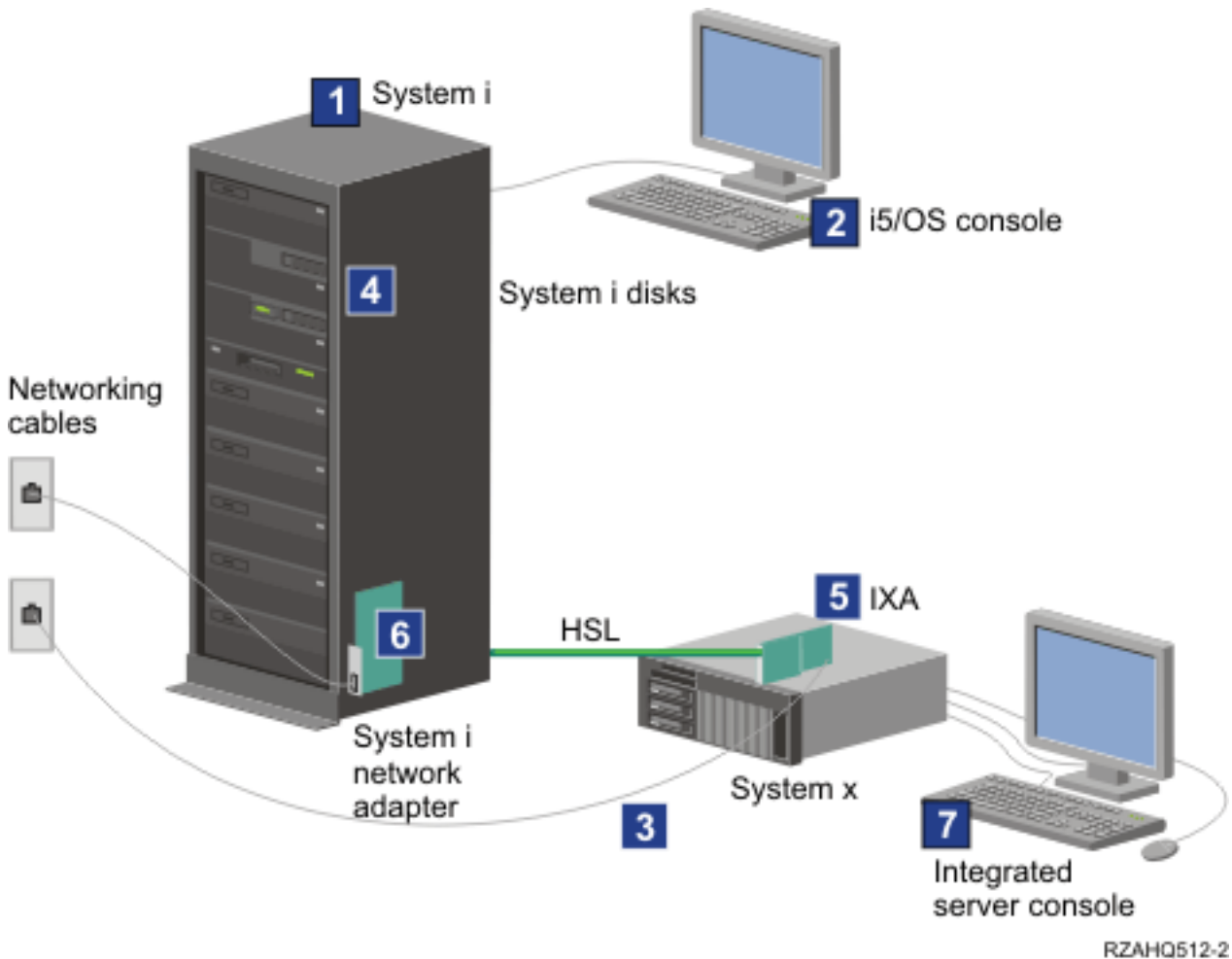


Figure 3. A typical IXA attached server installation

1. You need a compatible System i server. (See “Hardware requirements for integrated servers” on page 32 for compatibility information.)
2. The i5/OS console, from which you connect to the System i product using System i Navigator or the character-based interface, is shown to make clear the distinction between it and the Windows console.
3. A typical System x product will have at least one integrated network controller. Additional network cards can be added to most System x products to further enhance network connectivity. Information about System x network card compatibility can be found on the System i integration with BladeCenter and System x web site.

4. An IXA attached System x product does not have its own hard disk drive. The i5/OS operating system emulates hard disk space for it to use from System i hard disk drives.
5. The IXA card plugs into a specific slot in the System x product and is attached to the product via HSL cables.
6. A typical System i product will have a network card.
7. A integrated server console allows you to interact with the IXA-attached System x product. An integrated server console may consist of a monitor, keyboard, and mouse directly attached to the System x product. For more information about this and other types of integrated server consoles, see “Windows console for integrated servers.”

Windows console for integrated servers

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 System x product, or an iSCSI-attached System x or BladeCenter product, 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 System i 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 “Connecting to the 4812 IXS virtual serial console” on page 78 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 System i 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 System x products 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.

Integrated 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 System i disk space to back up your files or the entire disk image.
- System i tape and disk devices are available.
- LAN adapters, cables, hubs, or switches are not required for TCP/IP communication with the System i product or other integrated servers when using virtual networking.
- Installing the Microsoft Windows operating system in an integrated server environment 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 for integrated servers” on page 84), some techniques necessary to administer storage on a PC server are unnecessary for integrated servers.

Integrated server performance concepts

Integrated server performance is related to memory, processors, and disk configuration.

Integrated servers have their own memory and one or more processors, but share the System i hard disk drive storage through virtual (simulated) disk drives. The disk drives are allocated to Windows by creating a storage space object on the System i product. The major difference between the integrated servers and stand-alone servers is that stand-alone servers tend to use dedicated disk drives and the integrated servers use System i storage spaces as virtual disks. System i integrated servers also include optional features such as Windows drivers to share System i tape devices, CD and DVD drives, along with high speed virtual Ethernet adapters.

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

Storage performance for integrated servers

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

Greater disk performance capacity with System i shared disks

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

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

On servers with dedicated disks, the disk response times tend to be relatively steady. 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 System i storage, CPU and memory are shared between the integrated server and i5/OS 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 System i operations contend for the same disk. Some disk intensive i5/OS 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 System i storage space appears as one disk drive within Windows. When the Physical Disk average queue length (in Windows Performance Monitor) exceeds two, the server performance is not necessarily disk constrained. Assuming that memory paging issues have been ruled out, a queue length of two or a Windows disk utilization of 100% only points to a storage bottleneck if there is only one physical disk drive to perform the operations. There are usually multiple disks on the System i product in the storage space ASP operating in parallel. Typically, two times the number of disks in the ASP might point toward a disk bottleneck. You might also need to account for the average queue lengths of all the servers using the storage ASP.

Storage space balancing for integrated servers

When a storage space is for an integrated server 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 System i storage architecture, regardless of how an ASP or IASP is configured.

The System i product 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 System i product. 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 System i 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 System i product 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

the Microsoft Windows Performance Monitor as you would on any other server. See your Microsoft Windows documentation for information about using the Performance Monitor.

Virtual Ethernet performance for integrated servers

The Virtual Ethernet point to point connection is the default virtual network connection between the System i 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 System i and Windows CPU utilization cost of using the point to point connection is similar to the utilization cost of using a hardware network adapter. The connection is high speed, but total bandwidth is always shared with disk, tape and other 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 System i CPU to switch the traffic between servers, even when the System i product is not an endpoint of the traffic. For most connections this utilization won't be significant. 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 for IXS and IXA-attached integrated servers

IXS and IXA-attached integrated Windows servers use several types of network connections.

Point to point virtual Ethernet for integrated servers

This connection provides general purpose communication between an IXS or IXA-attached integrated server and the hosting i5/OS partition.

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 System i product, and also because, like a virtual Ethernet network, it is emulated within the System i product 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 System i product 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 LIN03, 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 for integrated servers

These are networks created between integrated servers, i5/OS partitions, and other partitions (such as Linux).

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 “Configuring virtual Ethernet networks for integrated servers” on page 72.

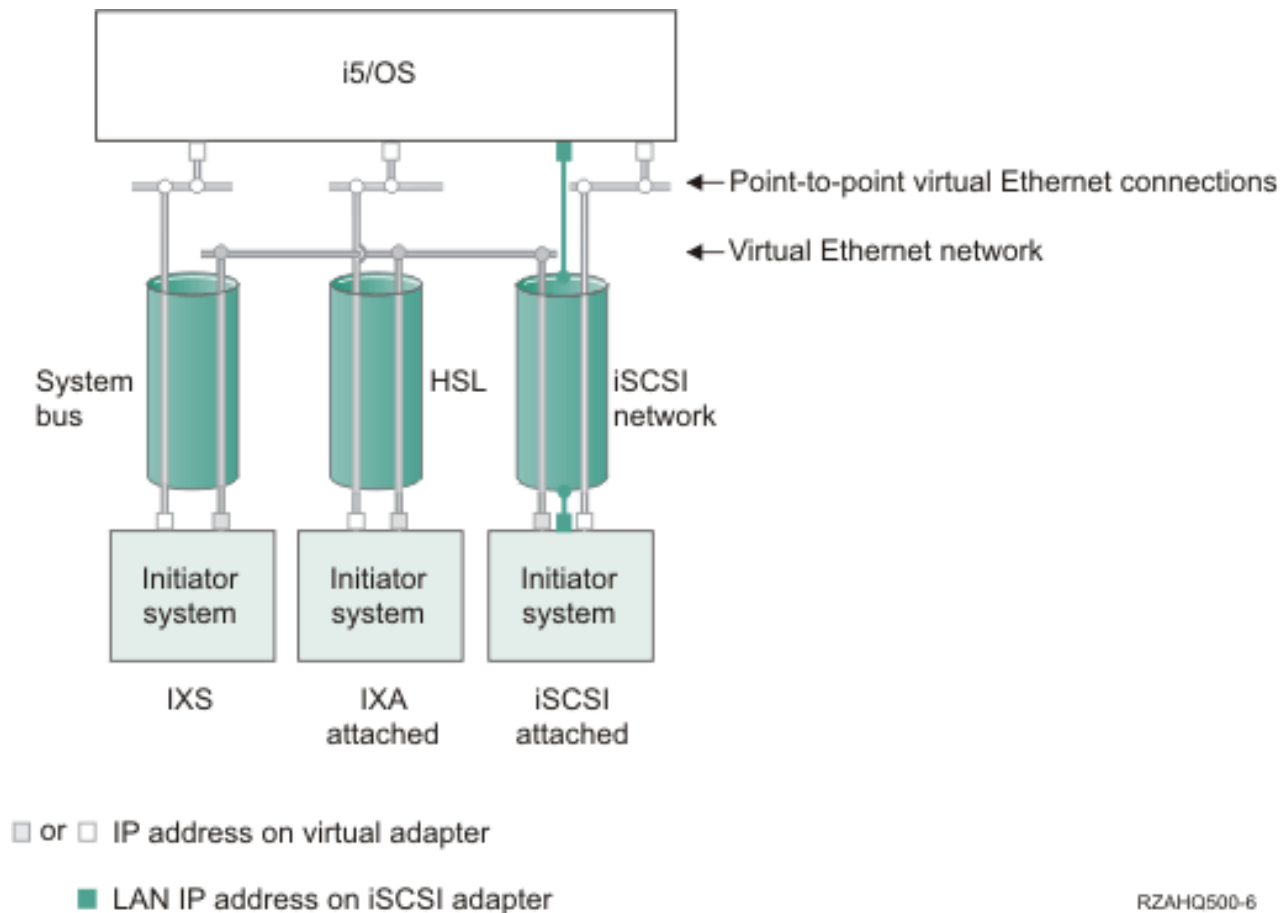


Figure 4. System bus, HSL, and iSCSI network tunnels

All integrated servers can participate in virtual Ethernet networks and can communicate with each other.

- For IXSs, virtual Ethernet traffic flows over System i system buses.
- For IXA-attached hosted systems, virtual Ethernet traffic flows through HSL cables.

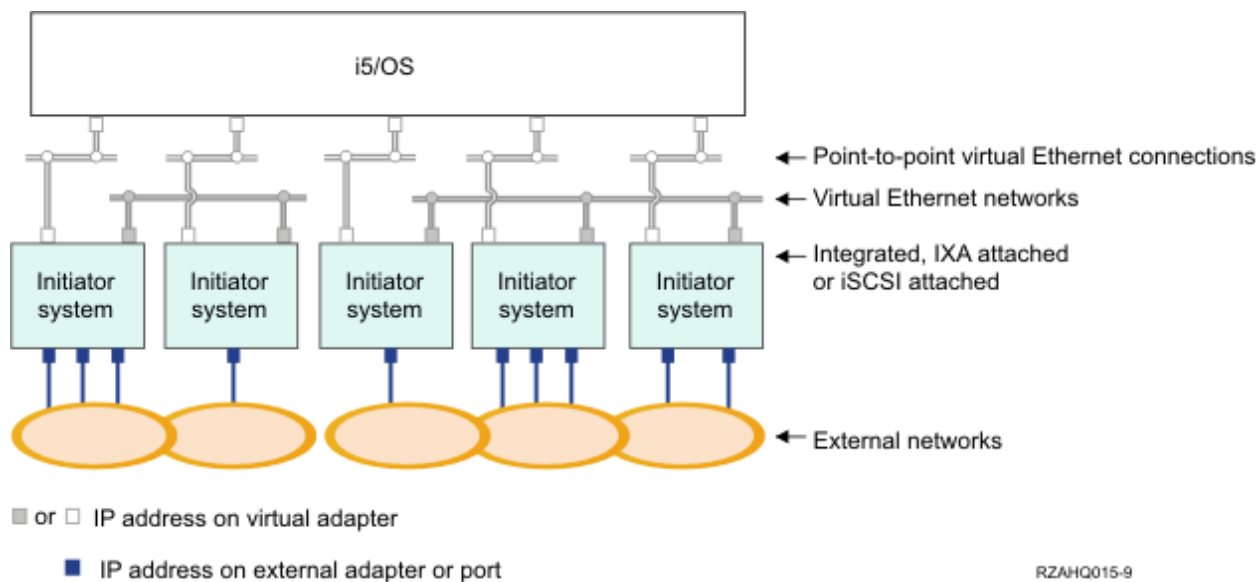


Figure 5. Two isolated groups of integrated Windows servers on the same System i product. Each group has its own virtual Ethernet network.

Figure 5 is intended to help you understand how virtual networks work within the System i product. There are five separate integrated Windows servers. They are all connected to the single, controlling, i5/OS partition with point to point virtual Ethernet networks (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.

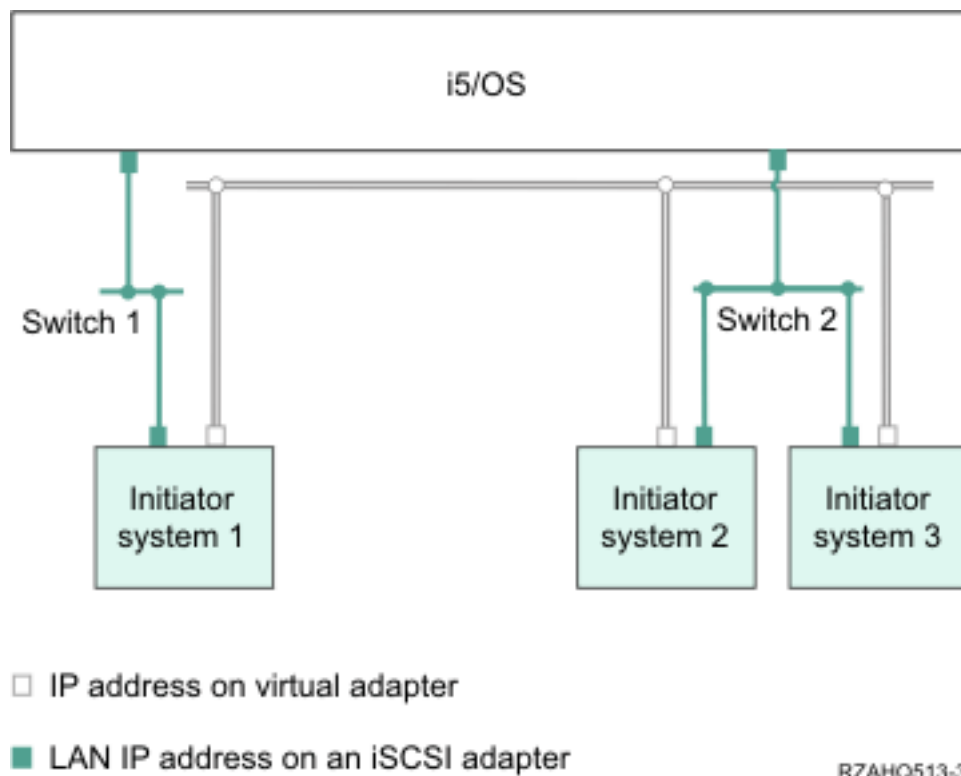


Figure 6. Virtual Ethernet tunneled through iSCSI networks

Virtual Ethernet tunneled through iSCSI networks has some special characteristics that are illustrated in Figure 6.

- 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 System i product, 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 "Configuring inter-partition virtual Ethernet networks for integrated servers" on page 72.

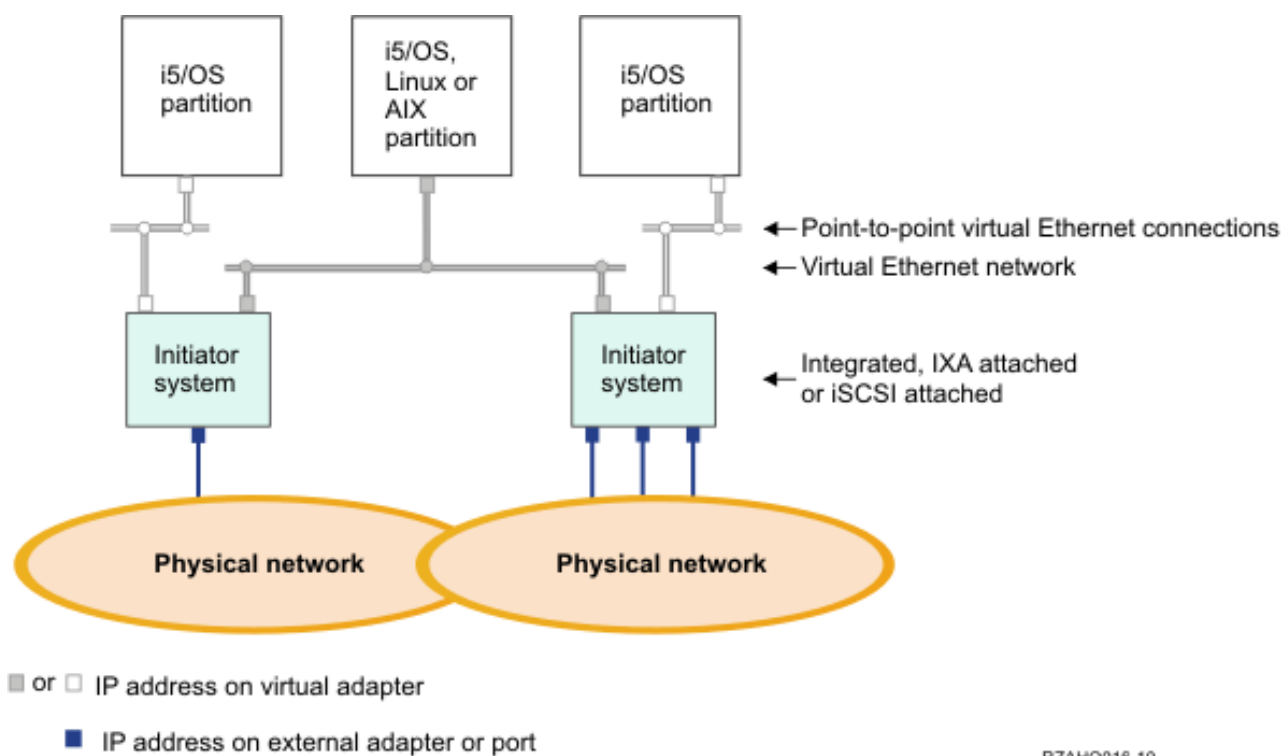


Figure 7. A simple, inter-partition virtual Ethernet network.

Now the System i product has been partitioned, creating three separate virtual i5/OS logical partitions inside the System i product. 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 System i 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 for IXS and IXA-attached integrated servers

An integrated Windows server can participate in external networks just as you can with a normal PC server.

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

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 System i product. It has no PCI expansion slots. Some IXSs can control the System i PCI slot adjacent to where it is installed, and in this way 'take over' an System i 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 System x product and how to configure them for use with integrated servers, see "Configuring external networks for integrated servers" on page 75.

Software concepts for IXS and IXA-attached integrated servers

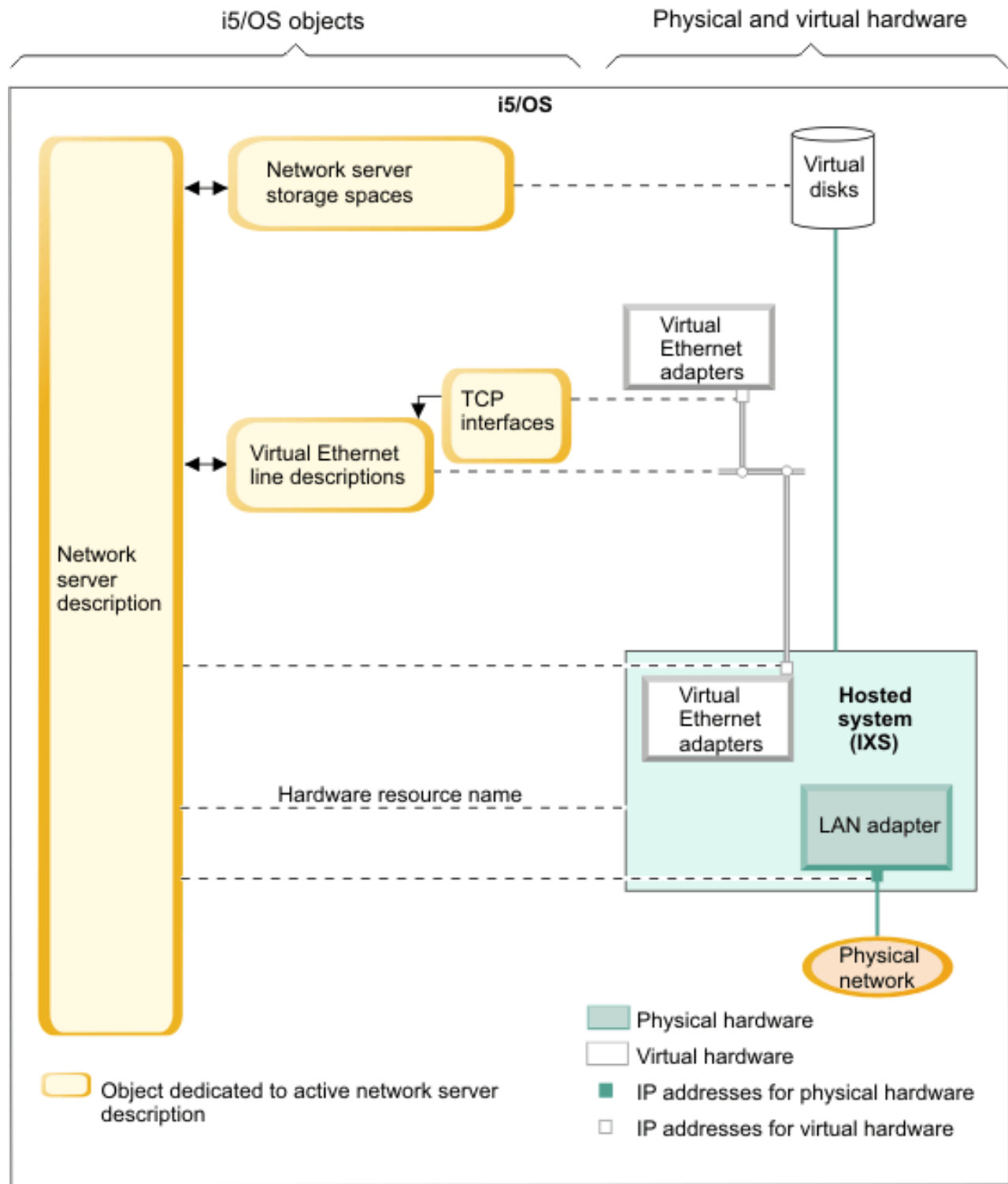
i5/OS provides support for defining, configuring and managing integrated servers, regardless of the type of integrated server hardware.

See the following diagrams for a description of the i5/OS objects that are used for the various hardware configurations. See "Integrated server hardware concepts" on page 8 for a description of the hardware configurations that are supported.

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

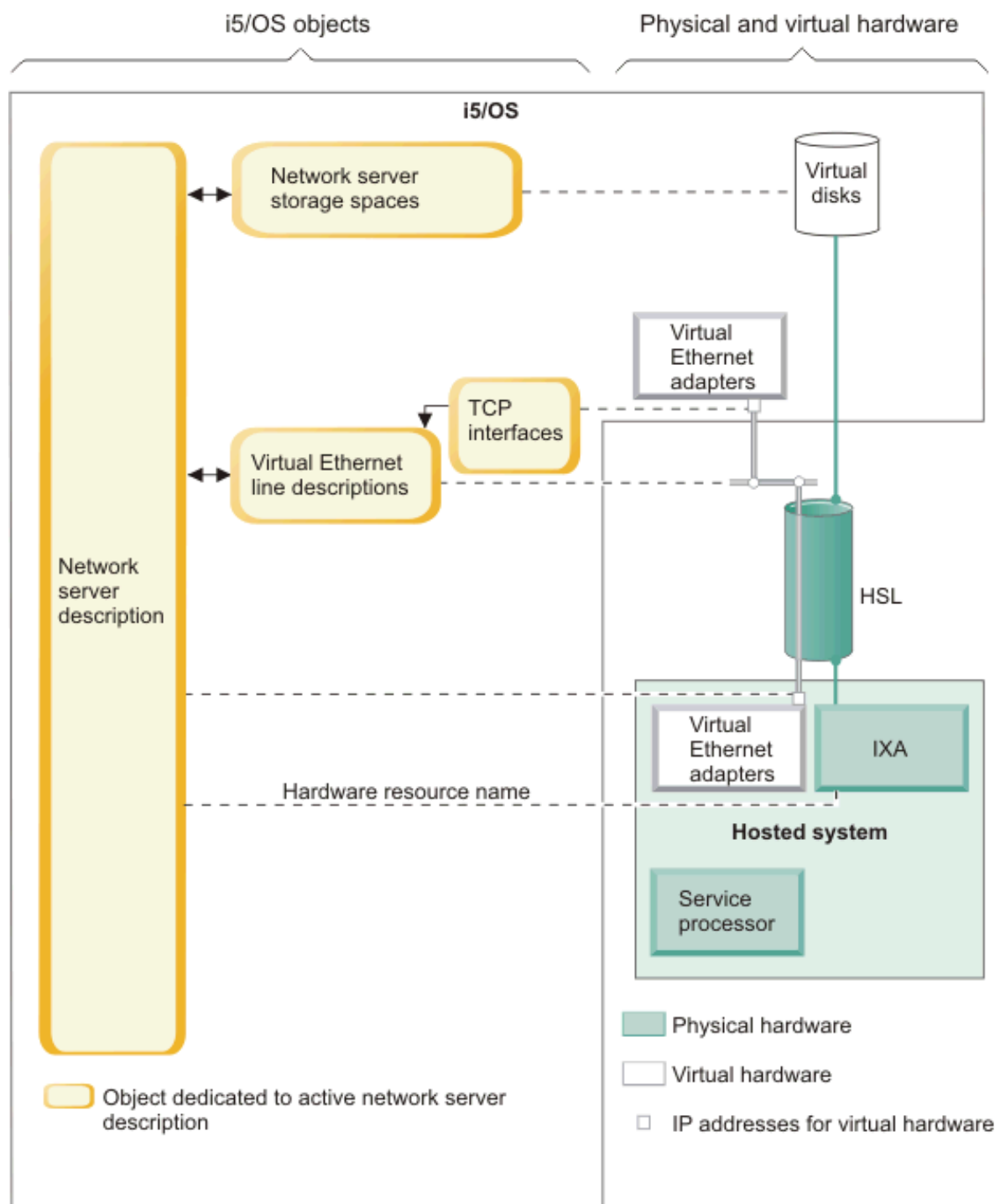
Integrated servers that use integrated xSeries Server (IXS) and Integrated xSeries Adapter (IXA)-attached System x hardware

i5/OS represents IXS and IXA-attached System x products in similar ways.



RZAHQ508-4

Figure 8. IXS Configuration objects in i5/OS



RZAHQ504-2

Figure 9. IXA configuration objects in i5/OS

Figure 9 shows the key i5/OS objects as well as key hardware components that are used for IXS and IXA-attached System x products.

See the following sections for information about the objects in Figure 8 on page 22 and Figure 9.

Network server description for IXS and IXA-attached integrated servers:

The Network Server Description (NWSD) object ties together all of the i5/OS objects that relate to an integrated server. You use this object to stop and start 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 network server description (NWSD) in Figure 8 on page 22 and Figure 9 on page 23 is the key i5/OS configuration object for all types of integrated servers. 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 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 System x product, i5/OS communicates over a high speed link (HSL) bus with the IXA that is installed in the System x product to initiate the start and shut down tasks. The IXA in turn communicates with the service processor (SP) of the System x product to perform the start and shut down tasks.

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

Hardware resource name for IXS and IXA-attached integrated servers:

The i5/OS operating system represents the integrated server hardware by a hardware resource name (for example, LIN23). A reference to the hardware resource name for an IXS or IXA-attached System x product is stored in the NWSD object.

See Figure 8 on page 22 and Figure 9 on page 23.

Note: Since the hardware that an IXS or IXA-attached System x product 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 System x product 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 "Using hot spare integrated server hardware" on page 83.

Network server storage spaces for IXA-attached and IXS integrated servers:

A network server storage space (NWSSTG) represents a virtual disk that the integrated server uses.

See Figure 8 on page 22 and Figure 9 on page 23. 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 5761-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 “Managing storage for integrated servers” on page 83 for more information about virtual disk drives.

Note:

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 “Backing up and recovering IXS or IXA-attached integrated Windows servers” on page 108 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 for IXS and IXA-attached integrated servers:

A Virtual Ethernet line description is used to configure a System i virtual Ethernet network that the integrated server participates in.

See Figure 8 on page 22 and Figure 9 on page 23. 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 for IXS and IXA-attached integrated servers” on page 16 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 for IXS and IXA-attached integrated servers:

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 8 on page 22 and Figure 9 on page 23.

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 for IXS and IXA-attached integrated servers:

The disk drive SCSI and virtual Ethernet data flows between i5/OS and the integrated server over the System i system bus (for an IXS) or a high speed link (HSL) connection between an I/O tower and the System i product (for an IXA).

See Figure 8 on page 22 and Figure 9 on page 23. In essence, the disk drive SCSI and virtual Ethernet protocols are encapsulated or tunnelled within the normal System i system bus/HSL data transfer protocols.

High availability concepts for IXS and IXA-attached integrated servers

System i and System x 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. Integrated server hardware can be hot spared to minimize downtime that is caused by hardware failures. If the hardware that is used to run the integrated server fails, you can quickly switch the hosted system's disk images to compatible spare hardware and restart the hosted system. For more information, see "Using hot spare integrated server hardware" on page 83.

Microsoft Windows Cluster Service (MSCS)

Integrated 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 60.

Security concepts for IXS and IXA-attached integrated servers

Data for IXSs and IXA attached systems travels over a physically secure network.

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

User and group concepts for integrated Windows servers

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

Enrollment

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

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

Windows domains and local servers

Enrollment can be made to either a Windows domain or a local server. A Windows domain is a set of resources (applications, computers, printers) which are networked together. A user has one

account across the domain and needs only to log onto the domain to gain access to all the resources. An integrated server can be a member server of a Windows domain and integrate i5/OS user accounts into the Windows domain.

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

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

Microsoft Windows i5/OS groups

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

AS400_Users

Every i5/OS user, when first enrolled to the Windows 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 System i product, the user will be replaced. This group is a useful place to check which i5/OS user profiles are enrolled to the Windows environment.

AS400_Permanent_Users

Users in this group cannot be removed from the Windows environment by the System i product. It is provided as a way to prevent Windows users from being accidentally deleted by actions taken within i5/OS. Even if the user profile is deleted from i5/OS, the user will continue to exist in the Windows 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 "User accounts for integrated servers" on page 28.

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 102.

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 “i5/OS password considerations for integrated servers” on page 31.

User enrollment templates

You can customize the authorities and properties a user receives during enrollment through the use of user enrollment templates. See “User enrollment templates for integrated servers” on page 30. 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 occurring on each member server. Use the Propagate Domain User (PRPDMNUSR) parameter in the Change Network Server Description (CHGNWSD) or Create Network Server Description (CRTNWSD) commands. See “The QAS400NT user” on page 105 for more information.

| Using the DSBUSRPRF parameter

You can specify whether you want user profiles on integrated Windows servers to be disabled when the corresponding i5/OS user profiles are disabled. Use the Disable User Profile parameter on the Change Network Server Description (CHGNWSD) or Create Network Server Description (CRTNWSD) commands. See “The QAS400NT user” on page 105 for more information.

User accounts for integrated servers

There are several basic types of user accounts for integrated servers.

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 102.

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 102.

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	<ul style="list-style-type: none">• 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.

Table 1. Types of user configurations (continued)

User type	Function provided	User profile definition
Windows password-managed user	<ul style="list-style-type: none"> 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 for integrated servers

A user enrollment template is a tool to help you enroll users from i5/OS to the an IXS or IXA-attached integrated Windows server 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 “Creating user templates for integrated Windows servers” on page 101.

i5/OS password considerations for integrated servers

Ensure that passwords will work correctly for your integrated server users.

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

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




2. The user should use i5/OS passwords containing only characters and password lengths allowed in Windows passwords if they want to enroll users. The password level of i5/OS can be set to allow for user profile passwords of 1 - 10 characters or to allow for user profile passwords of 1 - 128 characters. An i5/OS password level change of the system value QPWDLVL requires an IPL.
3. The i5/OS password level of 0 or 1 supports passwords of 1 - 10 characters and limits the set of characters. At password level 0 or 1, i5/OS converts passwords to all lowercase for Windows.
4. The i5/OS password level of 2 or 3 supports passwords of 1 - 128 characters and allows more characters including uppercase and lowercase characters. At level 2 or 3, i5/OS preserves password case sensitivity for Windows.
5. When the i5/OS passwords of enrolled users expire, their Windows passwords also expire. Users can change their passwords on Windows, but they must remember to also change their passwords on i5/OS. Changing the i5/OS password first automatically changes the Windows password.
6. If the i5/OS system value QSECURITY is 10, the Windows users that are created do not require passwords to sign-on. All other i5/OS QSECURITY levels require that a user object have a password to sign-on. You can find more information about security levels in the Security topic collection.
7. If you are using a language other than English, be aware that using anything but invariant characters in user profiles and passwords can cause unpredictable results. The 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.

Installing and configuring IXS and IXA-attached integrated Windows servers

Install a new IXS or IXA-attached integrated Windows server.

Setting up Windows environment on System i 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 System i, 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/)
 - 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 for integrated servers."
 - b. "Software requirements for IXS and IXA-attached integrated servers" on page 34.
4. For IXS or IXA attached servers, install hardware, if needed. See the Install iSeries features topic collection in the V5R3 i5/OS Information Center. Choose your model of System i product. 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 5.
5. Install the IBM i5/OS Integrated Server Support.
 - a. "Preparing for the installation of integrated Windows servers" on page 34
 - b. "Installing IBM i5/OS Integrated Server Support" on page 39
6. Install Microsoft Windows 2000 Server or Windows Server 2003 to the integrated server.
 - a. "Planning for the installation of Windows server" on page 39
 - b. "Installing Windows 2000 Server or Windows Server 2003" on page 54
7. Now that you have completed the installation, configure the integrated Windows Server.
 - a. "Code fixes" on page 68. These code fixes will correct any errors discovered in the licensed program since its release.
 - b. "Managing virtual Ethernet and external networks for integrated servers" on page 71
 - c. "Setting an integrated Windows server to automatically vary on with TCP/IP" on page 68

Hardware requirements for integrated servers

You must have supported hardware to use an integrated server.


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


1. One of the following Integrated xSeries Server (IXS) or Integrated xSeries Adapter (IXA).

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

Description	Feature code	Type-model
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.

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 collection in the V5R3 i5/OS Information Center. For a description of IXSs, IXAs, and iSCSI HBAs, see “Integrated server hardware concepts” on page 8.

2. A System i model 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
System i 1000/100/10 Mbps Ethernet Adapter (copper UTP)	5701		X	
System i Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	5700		X	
System i Gigabit (1000/100/10 Mbps) Ethernet Adapter (copper UTP)	2760			X
System i Gigabit (1000 Mbps) Ethernet Adapter (fiber optic)	2743			X
System i 2892 10/100 Mbps Ethernet port	2892		X	
IBM System i 10/100 Mbps Ethernet Adapter	2838			X
High-speed 100/16/4 Mbps Token-ring PCI Adapter	2744		X	X
System i 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 System i Access (which includes System i Navigator) installed.

Note: System i Navigator is preferred for most Windows environment on System i configuration tasks.

For additional hardware requirements, see

- “Memory requirements for integrated servers” on page 36
- “Networking concepts for IXS and IXA-attached integrated servers” on page 16



Software requirements for IXS and IXA-attached integrated servers

You need i5/OS fixes, options, and supported operating system software to use an integrated server.

You need this software:

1. i5/OS 5761-SS1 V6R1 or later.
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 5761-SS1. The release shown beside that is your version. (On some releases, you might need to press F11 before the version number appears.)
2. IBM i5/OS Integrated Server Support (5761-SS1 Option 29) V6R1 or later. See “Installing IBM i5/OS Integrated Server Support” on page 39.
3. System i Navigator, which is included with IBM System i Access for Windows (5761-XE1).

Note:

- a. When installing System i Navigator on a Windows PC, do a full install or do a custom installation and select the optional Integrated Server Administration component.
 - b. System i Navigator is preferred for most integrated Windows server configuration tasks.
4. IBM TCP/IP Connectivity Utilities for i5/OS V6R1 or later (5761-TC1).
5. Microsoft Windows 2000 Server or Windows Server 2003. For information about integrating Service Pack 1 with your Windows Server 2003 installation media, see Integrating a service pack with Windows Server 2003  on the System i 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 more information about installing required software, see the Installing, upgrading, or deleting i5/OS and related software topic collection.

Preparing for the installation of integrated Windows servers

Prepare your i5/OS user account, your systems, and your software for the installation of IXS and IXA-attached integrated 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 Security topic collection.

2. Verify “Memory requirements for integrated servers” on page 36.

3. “Configuring i5/OS TCP/IP for integrated Windows servers” on page 37.

4. Decide how many integrated Windows servers and subnets you need for your particular business.

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 System i model, 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 “Enabling i5/OS NetServer” on page 38 and “Planning for a Windows user with authorities to access i5/OS NetServer” on page 38.

6. Select an installation source for your integrated server operating system.

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: 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).

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 “Network server description configuration files” on page 123.
8. If you use logical partitions on your System i model, 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.
9. Prepare your integrated server hardware.

- If the server will be installed on an external System x product using an Integrated xSeries Adapter, refer to the following links:
 - IXA install read me first 
 - Install iSeries features topic collection in the V5R3 i5/OS Information Center.
- If the server will be installed on an Integrated xSeries Server (IXS), see IXS install read me first .

Memory requirements for integrated servers

Several types of memory affect the performance of your integrated server.

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-attached integrated 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

Configuring time synchronization for integrated Windows servers

Time synchronization for your integrated server needs to be configured both in both i5/OS and the integrated server operating systems.

To keep the time on i5/OS and the integrated server synchronized, do the following steps:

1. Select a value for synchronize date and time in the Install Windows Server (INSWNTSVR) command or the change network server description (CHGNWSD) command. Possible values include:
 - *YES The system synchronizes the time between i5/OS and the integrated Windows server every 30 minutes.
 - *NO The system synchronizes the date and time only when the integrated server is started.
 - *NONE The system does not synchronize the date and time for the integrated server.
2. Ensure that the i5/OS time, date, and time zone are correct. Once these values are set they will automatically update themselves every six months for daylight savings time adjustments. The QTIMZON system value replaces the need to manually change the QUTCFFSET 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 “Completing the integrated server operating system installation” on page 57.

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.

Configuring 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 System i Navigator installed, you can use it to configure your TCP/IP connections. The System i Navigator online help tells you how to configure TCP/IP. If you do not have System i Navigator installed, follow these steps:

1. On the i5/OS console, enter the command CFGTCP and press Enter. The Configure TCP/IP menu appears.
2. Select option 12 Change TCP/IP Domain information and press Enter. The Change TCP/IP Domain (CHGTCPDMN) display appears.
3. Specify the Local domain name.
4. In the Domain name server field, specify up to 3 IP addresses and press Enter.

To add a TCP/IP gateway for i5/OS, do the following steps:

1. On the i5/OS console, enter the command CFGTCP and press Enter. The Configure TCP/IP menu appears.
2. From the Configure TCP/IP menu, choose option 2 Work with TCP/IP routes. The Work with TCP/IP Routes display appears.
3. Type 1 in the Option field to add a TCP/IP route. The Add TCP/IP Route display appears.
4. Fill in the appropriate fields with the information for your gateway address.

Using System i Access for Windows with integrated Windows servers

IBM System i Access allows you to connect a personal computer (PC) to a System i product 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 System i Access, users and application programmers can quickly process information, applications, and resources for their entire company.

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

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

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

Additional information sources:

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

Enabling i5/OS NetServer

i5/OS NetServer enables Windows clients to connect to i5/OS shared directory paths and shared output queues by way of TCP/IP.

To install service packs, you must be signed on with a Windows account that corresponds to an i5/OS user profile with the same password, or you must have a guest i5/OS NetServer user profile configured.

If you plan to use i5/OS NetServer only to perform maintenance tasks, you can set it up without System i Navigator. In that case, you can use the method found in the Configuring i5/OS for NetServer topic. If you want the full capabilities of i5/OS NetServer, you need System i Navigator, which requires setting up System i Access (see “Using System i Access for Windows with integrated Windows servers” on page 37) on a PC that you use for administration.

Once you have set up i5/OS NetServer, you need to set up a Windows user with access to i5/OS NetServer or you can set up an i5/OS NetServer guest user profile. See “Planning for a Windows user with authorities to access i5/OS NetServer.”

Planning for a Windows user with authorities to access i5/OS 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 i5/OS NetServer.

The Integrated Server Support code that runs on the Windows server is stored in the i5/OS Integrated File System (IFS) and is downloaded to the Windows server with i5/OS NetServer.

You can use one of the following methods to use this account.

- Sign onto Windows with an account that has a corresponding i5/OS user profile with the same password. This Windows account must also be a member of **Windows Administrators** group. You can enroll the user to Windows after the server has been installed. See “Enrolling a single i5/OS user to an integrated Windows server using System i Navigator” on page 99.
- If you prefer not to create a user profile, you can also use a guest user profile that is configured for i5/OS NetServer.

Once you have set up your i5/OS NetServer user profile, return to “Enabling i5/OS NetServer” or “Preparing for the installation of integrated Windows servers” on page 34.

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

If you have System i Navigator on your system, you can use the graphical interface to set up a guest user profile for i5/OS NetServer with no special authorities and no password.

If you do not have System i Navigator, follow these steps to set up a guest user profile for i5/OS NetServer:

1. On i5/OS, create a user profile with no special authorities and no password:

```
CRTUSRPRF USRPRF(username) PASSWORD(*NONE) SPCAUT(*NONE)
```

Note: See the Security topic collection for information about user profiles.

2. Enter the following command, where *username* is the name of the user profile that you created:

```
CALL QZLSCHSG PARM(username X'00000000')
```

3. To stop i5/OS NetServer, enter the following command:

```
ENDTCPSVR SERVER(*NETSVR)
```

4. To restart i5/OS NetServer, enter the following command:

Installing IBM i5/OS Integrated Server Support

IBM i5/OS Integrated Server Support provides functionality for i5/OS to communicate with integrated server.

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

1. If you are upgrading IBM i5/OS Integrated Server Support from V5R2 or V5R3, refer to this topic, "Upgrading the IBM i5/OS Integration for Windows Server licensed program" on page 58. Perform the steps under "Preparing to Upgrade" and then return here.
2. Insert the i5/OS media containing 5761-SS1 option 29.
3. Type G0 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 media.
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 System i 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 G0 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 System i topic.
12. If you are upgrading IBM i5/OS Integrated Server Support from V5R2 or V5R3, go to "Upgrading the IBM i5/OS Integration for Windows Server licensed program" on page 58. 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 "Upgrading the integrated server side of IBM i5/OS Integrated Server Support" on page 59.

Planning for the installation of Windows server

Plan the parameters you will use for the Install Windows Server (INSWNTSVR) CL command and your integrated 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.

Before you install Windows 2000 Server or Windows Server 2003, you need to fill out the "Installation worksheet for i5/OS parameters" on page 40.

See “Installing Windows 2000 Server or Windows Server 2003” on page 54 to continue.

Network server descriptions

Select a name for the integrated Windows server.

Network server descriptions (NWSDs) represent an integrated Windows server . 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

Plan the parameters that you will use on the Install Windows Server (INSWNTSVR) CL command when you install an IXS or IXA-attached integrated Windows server.

Plan for the Install Windows Server (INSWNTSVR) CL command

Complete this worksheet before you install the Windows operating system. If you need more information on the parameters, see the Install Windows Server (INSWNTSVR) topic.

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

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers

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. 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.	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
Install type (INSTYPE) Full, Basic	<p>Specifies the type of install to perform. Choose one of the following:</p> <p>*FULL</p> <p>Required when installing on an internal Integrated xSeries Server (IXS) and is optional when installing on an external System x product attached with an Integrated xSeries Adapter (IXA).</p> <p>*BASIC</p> <p>Optional install type when installing on an externally attached System x product attached with an IXA. 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 System x installation process using the ServerGuide™ CD.</p>	
Resource name (RSRCNAME) Full, Basic	<p>Identifies the Windows server hardware.</p> <p>For both IXS and IXA-attached System x products, 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.</p>	
TCP/IP port configuration (TCPPORTCFG) Full	<p>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.</p> <p>Notes:</p> <ol style="list-style-type: none"> Only adapters that are directly managed by the System i product 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 System x product cannot be configured with this parameter. 	<ul style="list-style-type: none"> • Port 1 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway (optional) • Port 2 <ul style="list-style-type: none"> – IP address – Subnet mask – Gateway (optional)

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
Virtual Ethernet port (VRTETHPORT) Full, Basic	<p>Specifies the TCP/IP configuration for the virtual Ethernet networks used by the file server.</p> <p>A matching virtual Ethernet port is required to install the Windows Cluster service.</p> <p>*NONE: Specifies that there is no virtual Ethernet port configuration.</p> <p>Element 1: Port</p> <ul style="list-style-type: none"> *VRTETHx: The network server virtual Ethernet port <i>x</i> is configured, where <i>x</i> has a value of 0 through 9. <p>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.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> *NONE An associated port resource name is not associated with the line. resource-name The resource name. 	<ul style="list-style-type: none"> Virtual port 1 <ul style="list-style-type: none"> *VRTETHx IP Address Subnet mask Associated Port (Optional) Virtual port 2 <ul style="list-style-type: none"> *VRTETHx IP Address Subnet mask Associated Port (Optional) Virtual port 3 <ul style="list-style-type: none"> *VRTETHx IP Address Subnet mask Associated Port (Optional) Virtual port 4 <ul style="list-style-type: none"> *VRTETHx IP Address Subnet mask Associated Port (Optional)
TCP/IP local domain name (TCPDMNNAME) Full	<p>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.</p>	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
TCP/IP name server system (TCPNAMESVR) 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 that 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: <p>*ALL i5/OS receives all event log messages.</p> <p>*NONE No event log messages are received.</p> <p>*SYS i5/OS receives system event log messages.</p> <p>*SEC i5/OS receives security event log messages.</p> <p>*APP i5/OS receives application event log messages.</p> <p>Note: If you have the integrated server send its security log to i5/OS (by specifying *ALL or *SEC), be sure to set up the message queue with the correct security.</p>	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
<p>Installation source and system drive sizes and auxiliary storage pool (ASP)</p> <p>(SVRSTGSIZE)</p> <p>(SVRSTGASP)</p> <p>(STGASPDEV)</p> <p>Full, Basic</p>	<p>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.</p> <p>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.</p> <p>The installation source drive (drive D) must be large enough to hold the IBM i5/OS Integrated Server Support code. For *FULL installations of Windows 2000 or Windows Server 2003, the contents of the I386 directory on the Windows server installation CD image are also copied here. The limit is 1,024 to 1,024,000 MB, depending on your resource capabilities. Consider these factors:</p> <ul style="list-style-type: none"> • 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 	<p>Installation source drive:</p> <p>Size:</p> <p>ASP:</p> <p>ASPDEV:</p> <p>System drive:</p> <p>Size:</p> <p>ASP:</p> <p>ASPDEV:</p>

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
Installation source and system drive sizes and auxiliary storage pool (ASP)	i5/OS creates and links the drive as a FAT32 or NTFS network server storage space, depending on the size.	
(Continued)	<p>Notes:</p> <ol style="list-style-type: none"> 1. The INSWNTSVR command automatically sets the system drive size if a size to a minimum size that is determined based in part on factors such as the Windows version and installed memory. 2. When deciding the size of each drive, allow room for future needs such as new applications or upgrades to the Windows server product. If you specify *CALC for SVRSTGSIZE, note that i5/OS will allocate the minimum disk size necessary to install Windows. If you need additional space for applications or data you should consider manually specifying a drive size. 3. Support for independent ASPs (33 - 255) is provided through System i Navigator. For more information about working with independent ASPs, see Independent disk pools. Both the Information Center and System i Navigator refer to ASPs as disk pools. To use an independent ASP, the ASP device must be available prior to running the INSWNTSVR command. 	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
License mode (LICMODE) Full	<p>Determines the license mode to install Microsoft Windows server. Note: This parameter is only allowed when the value specified for WNTSVR is *WIN2000 or *WIN2003.</p> <p>Element 1 License mode:</p> <p>*PERSEAT Indicates that a client license has been purchased for each computer that accesses the server.</p> <p>*PERUSER Indicates that the end user purchased client access licenses for each device or user accessing the Windows Server 2003 server.</p> <p>*PERSERVER Indicates that client licenses have been purchased for the server to allow a certain number of concurrent connections to the server.</p> <p>Element 2 Client licenses:</p> <p>*NONE Indicates that no client licenses are installed. *NONE must be specified when *PERSEAT or *PERUSER is specified.</p> <p>number-client-licenses: Specifies the number of client licenses purchased for the server being installed.</p>	<p>License type:</p> <p>Client licenses:</p> <p>Terminal services:</p>

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
License mode (LICMODE) (Continued)	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.	
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.	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
Disable user profile (DSBUSRPRF) Full, Basic	<p>Specifies whether to disable the integrated servers user profiles if the corresponding i5/OS user profiles are disabled.</p> <p>*AUTO Integrated server user profiles are disabled if corresponding i5/OS user profiles are disabled.</p> <p>*NO Integrated server user profiles are not disabled if corresponding i5/OS user profiles are disabled.</p>	
Shutdown timeout (SHUTDTIMO) Full, Basic	<p>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.</p>	Shutdown timeout:
Restricted device resources (RSTDEVRSC) Full, Basic	<p>Restricts System i tape and optical devices from being used by the integrated server.</p> <p>*NONE Restricts no tape or optical devices from being used by the integrated server.</p> <p>*ALL Restricts all tape and optical devices from being used by the integrated server.</p> <p>*ALLTAPE Restricts all tape resources from being used by the integrated server.</p> <p>*ALLOPT Restricts all optical resources from being used by the integrated server.</p> <p>restricted-device Specify up to 10 device resources that you do not want the integrated server to use.</p>	
Time zone Full	<p>(Optional) Records the time zone of the System i product for use in the Windows server phase of installation. See "Configuring time synchronization for integrated Windows servers" on page 36.</p>	

Table 2. Install Windows Server (INSWNTSVR) CL Command parameters that apply to all types of integrated servers (continued)

Field	Description and Instructions	Value
Virtual Ethernet point to point (VRTPTPPORT) Full, Basic	<p>A local area network exists between i5/OS and Windows server. Both the i5/OS side and the Windows server side of this LAN have IP addresses and subnet masks.</p> <p>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.</p> <p>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.</p> <p>The subnet mask is always 255.255.255.0.</p>	i5/OS-side IP address: Windows server-side IP address:
Configuration file (CFGFILE) Full, Basic	<p>During the installation, creates and specifies a customized NWSD.</p> <p>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).</p>	

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.

Table 3.

Item	Description and Instructions	Value
Cluster name	<p>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.</p> <p>The cluster name is also used to create the network server storage space that will be used as the Windows cluster quorum resource.</p> <p>*NONE: Do not form or join a Windows Cluster.</p> <p>cluster-name: Specify the name of the cluster.</p>	

Table 3. (continued)

Item	Description and Instructions	Value
Cluster configuration: (Elements 1 - 3)	<p>Specifies the parameters required to configure a new Windows Cluster.</p> <p>Notes: This parameter is used to verify the i5/OScluster configuration. The Microsoft configuration wizards are used to install the Cluster service.</p> <p>This parameter is only required when forming a new Windows cluster using the Cluster name (CLU) parameter.</p> <p>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.</p> <p>cluster-domain-name: Specify the domain name to which the cluster belongs when forming a new cluster.</p> <p>Element 2: Quorum resource size Specifies the size in megabytes of the storage space used as the Windows quorum resource.</p> <p>*CALC Specifies that the size should be calculated to be the default value based on the Windows server version (WNTVER) parameter.</p> <p>quorum-size Specifies the Windows quorum resource size in megabytes. The size must be at least 550 megabytes but no larger than 1024000 megabytes.</p>	<p>Cluster domain name:</p> <p>Quorum resource size:</p>

Table 3. (continued)

Item	Description and Instructions	Value
Cluster configuration: (Elements 4-7)	<p>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:</p> <p>1: The storage space is created in auxiliary storage pool 1, the system auxiliary storage pool (ASP).</p> <p>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.</p> <p>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.</p> <p>Element 5: Cluster connection port Specifies the connection port used for the Cluster service communication.</p> <p>*VRTETHx: The network server virtual Ethernet port <i>x</i> is configured, where <i>x</i> has a value of 0 through 9.</p> <p>Note: The virtual Ethernet port must be configured to match this value.</p> <p>Element 6: Cluster Internet Address Specifies the Internet address for the cluster.</p> <p>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.</p> <p>Note: The Internet address selected must be unique across all NWSD objects and the i5/OS TCP/IP configuration.</p> <p>Element 7: Cluster Subnet Mask</p> <p>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.</p>	<p>Quorum resource ASP:</p> <p>Quorum ASP device:</p> <p>Connection port:</p> <p>Cluster Internet Address:</p> <p>Cluster Subnet mask:</p>

Comparison of FAT, FAT32, and NTFS file systems

Windows 2000 Server or Windows Server 2003 allows you to select between the NTFS and FAT32 file systems for your integrated server.

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 Server 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

Finding hardware resource names when you have multiple integrated servers

Do these steps to find device description and hardware resource names for System i devices.

You can have multiple integrated servers of the same type installed on your System i product. Use CL commands to see details about the resources and identify the hardware that is associated with a resource name.

1. If you are not already at the Display Communication Resources display, type DSPHDWRSC *CMN; then press Enter.
2. Type a 7 in the Opt field to the left of the resource name for a File server IOA . The Display Resource Detail display appears. For iSCSI-attached servers, locate the Network Server Host Port. This is the resource to be used when creating an NWSH object. The NWSH object name is used when installing the NWSD.
3. Find the Card Position under the Physical Location heading.
4. Look at the labels on the slots of your System i product. One slot should be labeled with the same number or combination of letters and numbers shown in the Card Position field. This slot contains the integrated server hardware to which the resource name refers.

Supported language versions

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

For most environments, the integrated server should use the same language as i5/OS. For information about supported language versions, see the Install Windows Server (INSWNTSVR) command topic.


Installing Windows 2000 Server or Windows Server 2003

Install the Microsoft Windows operating system for your integrated server.



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 40.

Note:

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 System i product.
2. If you have an Integrated xSeries Server, an Integrated xSeries Adapter, or an iSCSI HBA that is not listed in the “Hardware requirements for integrated servers” on page 32 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/)
 - IXS install read me first  (www.ibm.com/systems/i/bladecenter/ixs/readme/)
2. “Starting the operating system installation from the i5/OS console.”
3. “Continuing the operating system installation from the integrated Windows server console” on page 56.
4. “Completing the integrated server operating system installation” on page 57.

If you encounter any error messages during the installation, see “Responding to error messages during installation” on page 67.

Starting the operating system installation from the i5/OS console

Run the Install Windows Server (INSWNTSVR) CL command to install the operating system for your integrated server.

To install Windows 2000 Server or Windows Server 2003 on System i product, you need *IOSYSCFG, *ALLOBJ, and *JOBCTL special authority. You must have your Windows server license key available. In most cases, it is printed on the back of the installation CD jewel case.

1. Insert the installation media in the optical drive.
 - When performing an installation type of *FULL, place the installation CD in the System i optical drive (unless you plan to use an image of the installation CD).
 - When performing an Install type of *BASIC, place the ServerGuide CD in the attached System x hardware CD-ROM drive.
2. 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 40 in each of the following fields:
3. In the Network server description field (see “Network server descriptions” on page 40 for more information), type the server name from the “Installation worksheet for i5/OS parameters” on page 40 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 40.
5. In the Resource Name field, type the information that you filled out in the “Installation worksheet for i5/OS parameters” on page 40.
6. Choose the Windows server version you want to install; press Enter.
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 System i product 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 40. 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 40.
11. Type the values from the “Installation worksheet for i5/OS parameters” on page 40 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 :
 - a. Specify values for the Install source size and System size fields or select the default *CALC to allow the system to calculate the minimum size.
 - b. If you want to choose a different auxiliary storage pool (ASP) for the install source and system drives, specify it in the corresponding element of either the Storage space ASP or Server storage ASP device fields.
14. Specify either a Windows workgroup or domain in the corresponding To workgroup or To domain parameters.
15. Specify the name of the user who holds the Windows server license you are installing in the Full Name field.
16. 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 53.
18. In the Synchronize date and time field, specify to use the default value *NONE for most environments.

Option	Description
*YES	i5/OS synchronizes the date and time with the integrated server every 30 minutes.
*NO	i5/OS synchronizes the date and time with the integrated server only when you vary it on
*NONE	i5/OS will never synchronize the integrated server date and time with the i5/OS date and time when the network server description is varied on.

19. In the Disable user profile field, specify if this server should disable the user profiles on the integrated server if i5/OS user profiles are disabled.
20. 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.
21. 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.
22. Specify information for the Windows license.
 - a. In the License type field, specify the type of Windows server license that you purchased.
 - b. If you specified *PERSERVER in the License type field, then in the Client licenses field, specify the number of client licenses that you purchased.
 - c. Enter the Terminal services options to install in the Terminal services field.
23. In the Restricted device resources field, type the value from the "Installation worksheet for i5/OS parameters" on page 40.
24. 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.
25. Optional: Configure additional information for your integrated server.
 - 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 "Network server description configuration files" on page 123.
 - Configure a new or existing Windows Cluster configuration.

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

Continuing the operating system installation from the integrated Windows server console

Continue the installation from the integrated server console after you run the Install Windows Server (INSWNTSVR) CL command.

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 "Preparing for the installation of integrated Windows servers" on page 34 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 "Responding to error messages during installation" on page 67.
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 the "Installation worksheet for i5/OS parameters" on page 40. See "Configuring time synchronization for integrated Windows servers" on page 36.

- b. Select a setting for Daylight Saving Time.
 - If you are in an area that observes Daylight Savings Time, leave the **Automatically adjust clock** box checked.
 - If you know for sure that you do not observe Daylight Savings Time, clear the "Automatically adjust clock for daylight savings changes" check box.
5. On the Completing the Windows Setup Wizard panel, click **Finish**.
6. On the **Windows Setup** window, click the **Restart Now** button, or wait 15 seconds and the server automatically restarts.

Note: When installing a domain controller Windows server, Active Directory should be installed at this time by running the DCPROMO command. Refer to the Microsoft documentation for more information about the Active Directory installation.


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 "Completing the integrated server operating system installation."

Completing the integrated server operating system installation

Perform a few final tasks after installing Windows 2000 Server or Windows Server 2003 on the integrated server 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 "Setting an integrated Windows server to automatically vary on with TCP/IP" on page 68.
3. 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.
4. You can create additional disks for applications and data, rather than storing these items on the system drive. See "Adding disk drives to integrated Windows servers" on page 88 for more information.
5. 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 "Managing virtual Ethernet and external networks for integrated servers" on page 71 for more information.
6. You may want to enroll some of your i5/OS users to the Windows server or domain. See "Administering integrated Windows server users from i5/OS" on page 99 for more information.
7. 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.)
8. You can customize your servers by creating your own NWSD configuration file. See "Network server description configuration files" on page 123.
9. If you want Windows clustering, see "Windows Cluster Service" on page 60.
10. 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 66.
11. If you want to set up time synchronization for your integrated server, do the following steps:

- a. Configure i5/OS for time synchronization. See “Configuring time synchronization for integrated Windows servers” on page 36.
 - 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.
12. 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 “Installing the ATI Radeon 7000M video device drivers for Windows 2000 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 66.
 13. 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 “Adjusting hardware acceleration for Windows Server 2003 on the 2892-002 or 4812-001 Integrated xSeries Server” on page 67.

Upgrading the IBM i5/OS Integration for Windows Server licensed program

If you are upgrading i5/OS and IBM i5/OS Integrated Server Support to V6R1, you need the installation media containing 5761-SS1. If you also plan to install new integrated server hardware, make sure you complete this software installation first. As you follow the upgrade procedure in the Install, upgrade, or delete i5/OS and related software topic collection, take these additional steps:

Preparing to Upgrade i5/OS Integrated Server Support:

1. Ensure that you have the latest code fixes installed on all your existing integrated Windows servers, as well as on i5/OS. See “Code fixes” on page 68.
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 System i hardware, and the text description should be File Server IOP or File Server IOA. If you have multiple Integrated xSeries Servers of the same type installed on your System i product, you might 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 System i product. One slot should be labeled with the same number or combination of letters and numbers shown in the Card Position field. This slot contains the Integrated xSeries Server to which the resource name refers.
 - h. Record the information that appears in the Type-model and Serial number fields.
 - i. Press F12 twice to back out of the command.
4. Vary off all of your integrated servers. See “Starting and stopping an integrated server” on page 76.
5. To install the new version of i5/OS on your System i product, return to the procedure in the Install, upgrade, or delete i5/OS and related software topic collection.

After upgrading IBM i5/OS Integrated Server Support:

Configure your integrated server to work with the upgraded version of IBM i5/OS Integrated Server Support.

1. Start the integrated server (see “Starting and stopping an integrated server” on page 76) 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 3 of “Preparing to Upgrade i5/OS Integrated Server Support” on page 58. Verify that the information that appears in the Type-model and Serial number fields match what you recorded for this resource. 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 “Installing IBM i5/OS Integrated Server Support” on page 39.

Upgrading the integrated server side 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.

IBM i5/OS Integrated Server Support is the software which couples together the System i product and its integrated Windows servers. Think of it as a translation program. Half of the program runs on System i 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 “Backing up predefined disk drives for integrated Windows servers” on page 109 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 “Backing up user-defined disk drives for integrated Windows servers” on page 110).

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 i5/OS Information Center.

Migrating 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 or later.

See the Migrate from 285x or 661x to 2890 Integrated xSeries Server hardware topic in the V5R3 i5/OS Information Center.

Windows Cluster Service

Windows cluster service links individual IXS and IXA-attached integrated servers so they can perform common tasks and provides redundancy.

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 System i partition in order to be clustered.

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 .

Installing Windows Cluster service:

Install the Microsoft 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, do the following steps:

1. Install Windows Cluster service on the integrated server. Select one of the following options.
 - “Installing Windows Cluster service on a new integrated Windows server”
 - “Installing Windows Cluster service on an existing server” on page 62
2. “Installing Windows Cluster service on the Windows operating system” on page 64

Installing Windows Cluster service on a new integrated Windows server:

Install the Microsoft Windows Cluster Service with the Install Windows Server (INSWNTSVR) CL command.

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 “Installing Windows 2000 Server or Windows Server 2003” on page 54.

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 “Preparing Windows before installing Windows Cluster service on your integrated server” on page 63.

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 “Configuring virtual Ethernet networks for integrated servers” on page 72.

Installing 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 “Upgrading the integrated server side of IBM i5/OS Integrated Server Support” on page 59. 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:

- “Creating a storage space (quorum resource)”
- “Configuring the virtual Ethernet connection port”
- “Linking 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 “Preparing Windows before installing Windows Cluster service on your integrated server” on page 63.

Creating a storage space (quorum resource):

The first step is to create a storage space to use as the quorum resource.

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

Create a storage space to use as the quorum resource. Use the use the Create NWS Storage space (CRTNWSSTG) CL command and specify the special format *NTFSQR.

Configuring the virtual Ethernet connection port:

Configure the virtual Ethernet connection port for the private cluster communication. See “Configuring virtual Ethernet networks for integrated servers” on page 72. The virtual Ethernet port that you use must match the connection port you specify with the quorum resource network server storage space.

Linking 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).

Preparing Windows before installing Windows Cluster service on your integrated server:

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 “Installing Windows Cluster service on the Windows operating system” on page 64.

Formatting 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 “Formatting integrated server disk drives” on page 90.

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.

Configuring the private network adapter:

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. 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.

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

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.
7. Optional: For clarity, you can 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.

Installing Windows Cluster service on the Windows operating system:

The installation process of the Windows Cluster service varies depending on the version of the Windows operating system that is installed on your integrated server.

You should refer to the Microsoft documentation for instructions on installing the Windows Cluster service.

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.

This information highlights specific steps required to install the Windows Cluster service on an Integrated Windows server.

Installing Windows Cluster service on Windows 2000 Server:

Use the Cluster Service Configuration wizard to install the Windows Cluster service on your integrated server. 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

Starting 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**.

Configuring 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.

- Configure the remaining network connections according to their need

Configure the remaining network connections according to their need.

Specify the IBM i5/OS virtual Ethernet x adapter (typically Local Area Connection 2) as the primary network for the Internal Cluster Communication.

1. Uncheck the box **Enable this network for cluster use** for the IBM i5/OS virtual Ethernet Point to point (typically Local Area Connection 3)
2. Select the option **Internal cluster communications only** for the IBM i5/OS virtual Ethernet x where x matches the *VRTETHx specified on the cluster configuration connection port (typically Local Area Connection 2)

Installing Windows Cluster service on Windows Server 2003:

Install the Windows Cluster service on your integrated server.

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**.

Installing and configuring the Windows Cluster service:

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**.

Joining 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, then 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 i5/OS 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 i5/OS 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 i5/OS 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 i5/OS virtual Ethernet point to point and select **Properties**.
15. Uncheck the box **Enable this network for cluster use** for this network.

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.

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

Install the drivers for the ATI Radeon 7000M video chip for your integrated 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.

Adjusting 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.

Responding 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**.

Setting 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 (CFGTCIP) command.
2. Choose Option 1 Work with TCP/IP interfaces and press Enter.
3. Specify 2 (change) in the Option field next to the interface for the point to point virtual Ethernet (virtual Ethernet point to point) line description for the server, and press Enter.

Note: The point to point virtual Ethernet line description has a name that consists of the network server description (NWSD) name followed by 'PP' for the virtual Ethernet point to point LAN. For example, if the NWSD name is MYSVR, then the point to point virtual Ethernet LAN line description is MYSVRPP.

4. Change the **Autostart** parameter value to *YES and press Enter. The integrated server automatically varies on when you start TCP/IP.

Note:

- a. 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.
- b. Be aware that an IP address entered at the integrated console for the point to point virtual Ethernet overrides the value set in the NWSD for the TCPPRTCFG parameter *VRTETHPTP port. However, operations such as SBMNMWSCMD use the value set in the NWSD to find the server. Both values must be consistent.

Code fixes

IBM i5/OS 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 i5/OS 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 69.

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

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

Use this information to learn about the types of code fixes and the methods for applying them to the integrated server.

Types of code fixes

There are four types of code fixes can be used for integrated servers.

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/series/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 i5/OS 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/series/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 i5/OS 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.

Synchronizing the integration software level using the integrated Windows server console

To use the i5/OS 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.

Synchronizing the integration software level by using System i Navigator

Use System i Navigator to synchronize the integration software for your integrated server.

Updating the integration software: System i Navigator:

Do these steps to update the integrated server support software on the integrated server.

1. In System i Navigator, click **Integrated Server Administration** → **Servers**.
2. Right click the integrated server you want to synchronize and select **Synchronize iSeries Integration Software**. (If the i5/OS server you are accessing is not a V5R3 or later server, you will be presented with a list of earlier options, allowing you to install and uninstall service packs individually, or to perform a release update only.)
3. Click **Synchronize** to confirm the action.
4. You will receive a message indicating the synchronization is in progress followed by a completion message indicating that a reboot is about to take place. You will not be asked whether to reboot now or later.

Determining the software levels for the integration software:

View which levels of software are installed on i5/OS and the integrated server.

1. In System i Navigator, click **Integrated Server Administration** → **Servers**.
2. Right click the integrated server you are interested in and select **Properties**.
3. click the **Software** tab. The software levels will be displayed there.

Synchronizing the integration software level using a remote command

Use the `lvlsync` command at the integrated server console to synchronize the integration software.

Entering the command `lvlsync` at an integrated Windows server console command prompt will cause the integrated server to synchronize. The principle utility of this command-line program is that it allows you to synchronize an integrated server by remotely submitting a command. This functionality would be useful if you, for example, wanted to write a CL program to periodically synchronize your integrated servers. To learn more about remotely submitted commands, see “Guidelines for submitting remote commands to your integrated Windows server” on page 80.

Here is a simple procedure to remotely synchronize an integrated server by remotely submitting the `lvlsync` command from the i5/OS console.

1. At the i5/OS character-based interface, type `SBMNWSCMD` and press **F4**.
2. Enter `lvlsync` in the **Command** field and press **Tab**.
3. Enter the NWSD name of your integrated server in the **Server** field and press enter.

The `lvlsync` program allowed optional parameters in the past. These parameters no longer function, although their presence in the command will not affect its functionality.

`Lvlsync` returns the following error codes:

lvlsync error codes

Error Code	Error
0	No errors
01	Must be an administrator to run lvlsync
02	Release level on integrated Windows server higher than on i5/OS
03	Service pack level on integrated server higher than on i5/OS
04	Cannot install release from i5/OS - language files not on i5/OS
05	Syntax not valid
06	Cannot access service pack information on i5/OS
07	Cannot map network drive
08	Cannot access service pack information in registry
09	Cannot open qvnacfg.txt file
10	No service pack installed on i5/OS
11	NWSD not found
13	NWSD not active
20	No service pack available on i5/OS
21	Cannot start InstallShield application
31	Unexpected error while starting lvlsync
44	Unexpected error during lvlsync

Note: The error message NTA0218 is a diagnostic (*DIAG) message for syntax, authorization, and NWSD not found errors.

Managing virtual Ethernet and external networks for integrated servers

Learn how to use the three different types of networks available to integrated servers.

This section contains procedures to help you create and understand virtual Ethernet and external networks described in “Networking concepts for IXS and IXA-attached integrated servers” on page 16.

Configuring IP address, gateway and MTU values for integrated servers

Configure IP address, gateway and MTU values for your integrated server from i5/OS.

The IP address, gateway, and maximum transmission unit (MTU) values for virtual and physical network adapters for the integrated server are managed from the Microsoft Windows operating system, except for the following cases.

- The IP address and subnet mask for a new virtual Ethernet line description can be assigned by the i5/OS Install Windows Server (INSWNTSVR) CL 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 Troubleshooting on System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

- 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.

Configuring virtual Ethernet networks for integrated servers

Do the following steps to configure a virtual Ethernet network between integrated servers.

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 System i logical partitions, see “Configuring inter-partition virtual Ethernet networks for integrated servers.”

1. Configure a virtual Ethernet port and line description for the integrated server.
 - a. Expand **Integrated Server Administration** → **Servers**.
 - b. Right-click the integrated server and select **Properties**.
 - c. On the server properties panel, click the **Virtual Ethernet** tab.
 - d. click the **Add...** button to add a new virtual Ethernet port.
 - e. On the virtual Ethernet properties panel, specify the values for the new virtual Ethernet port
 - 1) Select the virtual Ethernet port number.
 - 2) Type the IP address that the integrated server will use.
 - 3) Type the subnet mask that the integrated server will use.
 - 4) You can leave the default line description name or change it to something else. The default line description name is the NWSD name followed by a v followed by the port number. For example, if adding port 3 to an NWSD named *Mynwsd*, then the default line description name is *Mynwsdv3*.
 - 5) Leave the associated port set to **None**.
 - 6) Leave the maximum frame size set to the default **8996**.
 - 7) If the server is an iSCSI attached server, select the network server host adapter corresponding to the iSCSI HBA that you want i5/OS to use for this virtual Ethernet configuration to reach the hosted system.
 - 8) Click **OK** to add the new port to the **Virtual Ethernet** tab on the server properties panel.
 - f. On the server properties panel, click **OK** to save the changes. This will update the NWSD and create a line description for the new virtual Ethernet port.
 - g. If you want this integrated server to be connected to more than one virtual Ethernet network, repeat all of the above steps to create a virtual Ethernet port and a line description for each network, using different virtual Ethernet port numbers.
2. Repeat Step 1 for each integrated server that you want to connect to the network. Use the same virtual Ethernet port for each server.
3. Restart the integrated servers. A virtual Ethernet adapter device driver will be automatically installed and set to the Windows TCP/IP address that has been specified for it in the NWSD. However, an IP address entered at the integrated server console overrides the values that are set in the NWSD.
4. Test to see that the virtual Ethernet network is functioning, for example by pinging from one server to the IP addresses you specified for the other servers.

Configuring inter-partition virtual Ethernet networks for integrated servers

Configure inter-partition virtual Ethernet networks for integrated servers on systems with or without a Hardware Management Console.

Configuring inter-partition networks with the Hardware Management Console

If you want an integrated server to communicate with other logical partitions, or with integrated servers controlled by other i5/OS partitions, you need to configure one or more inter-partition networks. Inter-partition networks are configured differently on System i models with the Hardware Management Console (HMC) than on other systems. In an System i 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 for the port the server will use if one does not exist. You can use ports 0 through 9. See step 1 of the “Configuring virtual Ethernet networks for integrated servers” on page 72 topic. Select an associated port name (Cmnxx) for the appropriate 268C resource.
3. Continue with step 2 of the “Configuring virtual Ethernet networks for integrated servers” on page 72 topic (in all i5/OS partitions that control a participating integrated server), and step 3 of “Configuring virtual Ethernet networks for integrated servers” on page 72.
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.

Configuring Inter-partition networks without the Hardware Management Console

In a system other than an System i 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 System i 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 “Configuring virtual Ethernet networks for integrated servers” on page 72. Leave the associated port name set to **None**.
3. Continue with step 2 in “Configuring virtual Ethernet networks for integrated servers” on page 72 (in all i5/OS partitions that control a participating integrated server), and step 3 in “Configuring virtual Ethernet networks for integrated servers” on page 72.
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 “Configuring virtual Ethernet networks for integrated servers” on page 72. 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.

Managing point to point virtual Ethernet networks for integrated servers

Each integrated server has a point-to-point virtual Ethernet network connection with the System i model, which allows the System i model to control the integrated server.

These connections are automatically configured during installation. You can view and manage these connections from the i5/OS operating system or the integrated Windows server console.

Viewing point-to-point virtual Ethernet connections from i5/OS

Point to point Ethernet connections in i5/OS are composed of a line description and an entry in an integrated server's NWSD.

1. To view the line description issue the command `WRKCFGSTS *NWS` from the i5/OS character-based interface.
2. Find the cascade of entries corresponding to your integrated server. One of the entries in the Line Description column will have the same name as your NWSD and end with the characters PP. Enter 8 to its left and press enter.
3. Now you are in the Work with Line Descriptions menu. Enter a 5 to the left of your line description and press enter to display its information.
4. Press **F3** until you return to the base menu.
5. Now issue the command `CFGTCP` and select option 1, **Work with TCP/IP interfaces**.
6. One entry in the Line Description column should have the same name as your NWSD and end with the letters PP.
7. Option 5 will display the TCP/IP Interface information, while options 9 and 10 will allow you to enable and disable it. Note the internet address. It will be used later.
8. Now we will take a quick look at the entry in the integrated server's NWSD. Issue the command `WRKNWSD`. Find your integrated server's NWSD and enter 5 to display it. Press enter to page through the NWSD attributes.
9. One of the screens will be titled **Attached lines** and will display Port number *VRTETHPTP and the name of the line description that the network is using.
10. Back in the **Work with Network Server Descriptions** menu you can use option 2 to change this information.

Viewing point to point virtual Ethernet connections from the integrated Windows server console

1. At the console of your integrated server, click **Start → Settings → Control Panel**.
2. Select **Network and Dial-up Connections**.
3. Double-click **virtual Ethernet point to point**. A dialog box will appear.
4. Click **Properties**
5. Double-click **Internet Protocol (TCP/IP)** in the next dialog box.
6. In this final dialog box you should see the IP address associated with the integrated server side of the point to point virtual Ethernet connection. It should be the i5/OS IP address augmented by one so as to be even instead of odd.
7. Close all of the windows that you opened, click **Start → Run**, and enter the command `cmd`. Press enter. This will start an instance of the Windows command prompt.
8. At the `C:\>` command prompt which appears, enter the command `ping` followed by the i5/OS IP address that you used in the last step. For example `ping 192.168.3.1`. The command should return `Reply from`. The ping command sends a packet of data to a certain internet address and times how long it takes to make a round trip.
9. Optional: Return to the i5/OS character-based interface and enter the command `call qcmd`. (This will increase the display space so that you can see the results of your commands.) Use the i5/OS command to ping the integrated server. For example, enter `ping '192.168.3.2'`.

Configuring external networks for integrated servers

If you install a new network adapter in an open PCI slot in the System i product, you also need to configure the new adapter on the integrated Windows server.

Refer to the Install iSeries features topic collection in the V5R3 i5/OS Information Center for information about installing a new network adapter card. Choose your model of System i hardware and find the instructions labeled **Install PCI Card and Integrated xSeries Adapter Card**.

To set up a new network adapter, see “Installing network adapter device drivers and adding adapter address information to an integrated Windows server.”

To create a virtual Ethernet connection, see “Configuring virtual Ethernet networks for integrated servers” on page 72.

To remove a network adapter, see “Removing network adapters from an integrated Windows server.”

Installing network adapter device drivers and adding adapter address information to an integrated Windows server


Install network adapter device drivers and add adapter address information for the new adapters on an integrated Windows server.

The adapters and device drivers in the Windows operating system 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 Server from Windows NT 4.0 to Windows 2000 Server, remove the old adapter before adding the new one. See “Removing network adapters from an integrated Windows server.”

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. Select 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 .

Removing network adapters from an integrated Windows server

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

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.

Administering integrated Windows servers

Start and stop the server, run integrated server commands remotely, view and change configuration information, and monitor message and error logs.

Starting and stopping an integrated server

Start and stop your integrated server from i5/OS or partially shut it down from the Windows console.

An integrated Windows server has no power button; its state is controlled by the i5/OS. Normally you start and shut down integrated servers from System i 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 System i Navigator or the character-based interface.

Ensure that integrated servers are varied off before shutting down your System i hardware, otherwise, data corruption can occur. Some commands used to shutdown the System i hardware will initiate a shutdown in attached integrated servers and wait a certain amount of time for them to power down before shutting down the System i hardware. Other commands will shut down the System i hardware immediately.

If you use the power off/on scheduling program QEZPWROFFP, you will need to configure it to work with your integrated server.

Starting and stopping an integrated Windows server using System i Navigator

Do these steps to stop an integrated Windows server using System i Navigator.

1. Select **Integrated Server Administration** → **Servers**.
2. Right-click the server you want to stop and select **Shut Down**. If you want to shut down all integrated servers, right-click the Integrated Servers icon in the left navigation and select **Shut Down All**. The status changes to **Shutting down...**, **Partially shut down**, and eventually **Shutdown**.

Starting and stopping an integrated Windows server using the character-based interface

Use the Work with Configuration Status (WRKCFGSTS) CL command to shut down an integrated Windows server.

1. Enter WRKCFGSTS *NWS.

2. Find the integrated server to stop and enter 2 to cause a *vary off*. 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**.

3. To start the integrated server use the same command `WRKCFGSTS *NWS`, and type 1 to *vary on* or start the integrated server.
4. 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.

Shutting down an integrated server from the Windows console

Shut down or restart the operating system for your integrated server from the Windows console.

Follow these steps.

1. From the **Start** menu, choose **Shut down**.
2. Select **Restart** from the drop-down menu and click **Ok**. The Windows operating system stop sand displays the the screen *It is now safe to turn off your computer*.
3. Vary off the server using System i Navigator or the character-based interface.

Shutting an integrated server from the Windows console:

Follow these steps.

1. From the **Start** menu, choose **Shut down**.
2. Select **Shut down** from the drop-down menu and click **Ok**.

Shutting down your System i hardware when integrated Windows servers are present

Select a method to shut down your System i hardware.

The easiest way to ensure your integrated servers will be shut down safely is to always manually shut them down before shutting down the System i hardware. The CL command `PWRDWN SYS *CNTRL D` will attempt to power-down each of the integrated servers, giving each of them a period of time (the NWSD attribute `SHUTDTIMO`, by default 15 minutes) in which to shut down. Note that there is no guarantee that they will finish shutting down within this time period.

CAUTION:

The CL command `PWRDWN SYS *IMMED` is not recommended. This will power down the System i hardware immediately, without attempting to shut down any integrated servers.

Table 4.

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 <code>pwrwnsys *cntrl d</code> .	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.
Issue the CL command <code>pwrwnsys *immed</code> .	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 `PWRDWN SYS` 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 (JOBID) 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.

Connecting to the 4812 IXS virtual serial console

Use Telnet to connect to the Windows console on a 4812 IXS virtual server that is running Windows Server 2003.

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 for integrated servers” on page 13 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.

Connecting to a virtual serial console using the IBM Personal Communications client

Connect to a virtual serial console using the IBM Personal Communications client.

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.

Connecting to the virtual serial console from a DOS command prompt

Use Telnet to connect to the virtual serial console from the Windows operating system.

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 Enter.
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.

Viewing or changing integrated Windows server configuration information

Use either System i Navigator or CL commands to change integrated server configuration information.

System i Navigator allows you to view and change most integrated server configuration information.

1. In System i Navigator, select **Integrated Server Administration** → **Servers**.
2. Right-click an integrated server and select **Properties**.

Using the character-based interface you can view and change all integrated server configuration information. The following table summarizes the relevant CL commands.

Table 5. CL commands for changing integrated server configuration information

Tasks	CL Command
Vary on and off integrated servers, check the status of the integrated server and objects that are associated with the network server description (NWS).	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

Finding integrated server message logs

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 System i Navigator

1. Click **Work Management** → **Active Jobs**.
2. One of the jobs listed under the QSYSWRK section will have the same name as your integrated server. Right-click it and select **Job log**.
3. The integrated server job log window opens. Double-click a message ID to see details.

To find the job log in the character-based interface

1. At an i5/OS command line enter WRKACTJOB SBS(QSYSWRK).
2. One of the jobs listed will have the same name as your integrated server. Select option 5 (Work with job).
3. Type 10 and press Enter to display the job log.
4. Press F10 to see the detailed messages.

There are other relevant job logs that you may want to check as well. The IBM Redbooks publication, Microsoft Windows Server 2003 Integration with iSeries, SG24-6959, has an excellent section concerning integrated server event logs in i5/OS and at the Windows console.

Running integrated Windows server commands remotely

Windows server commands can run on your integrated server in batch mode without user interaction. Use i5/OS to remotely submit batch commands.

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 *LCLPWDGMT 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 *LCLPWDGMT value is *NO, then network authentication (Kerberos) is used. The user must access the System i operation through Kerberos enabled applications (like System i Navigator single sign-on). See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 82 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 to your integrated Windows server.”

To run integrated server commands from System i Navigator

1. In System i Navigator, select **Integrated Server Administration** —> **Servers**.
2. Right-click the server on which to run the batch command and select **Run command**.
3. On the **Run Command** panel, type the Windows command to run (such as dir \).

Tip: You can select the command from a list of 10 commands that you have run previously on the server.

4. Click **Run** to run the command.

Note: A command using the Run Command panel uses *PRIMARY as the authentication domain. For alternative domains use SBMNWSCMD.

To run integrated Windows server commands from the character-based interface

1. Type CALL QCMD and press Enter.
2. Type SBMNWSCMD and press F4.
3. Type the command you want to run on the remote server. Page down.
4. Enter the NWSD of the server you want to run the command on and press enter.
5. The i5/OS account which you are using should be enrolled to the integrated server in order to be granted authentication to run the remote command. The Authentication domain field allows you to specify where to attempt to authenticate your user ID.
6. The output returned from the command will be displayed on the console. Press F10 to see all messages.

Guidelines for submitting remote commands to your integrated Windows server

Remember these guidelines when you submit remote commands to your integrated Windows server from i5/OS.

Note: Many of the Submit Network Server Command (SBMNWSCMD) CL command parameters listed in this section are not available when running Windows commands from using System i Navigator.

If you need to use a parameter that System i Navigator does not support, then you must use Submit Network Server Command (SBMNWSCMD) directly.

- The requested command is run under the Windows console command "cmd.exe." SBMNWSCMD will not return control to its caller until the command has finished running on Windows and the cmd.exe program terminates.
- The authentication domain field of SBMNWSCMD indicates the Windows domain where your user ID is to be authenticated. The default, *PRIMARY, logs on to the primary domain of the server, if the server is a domain member. *LOCAL logs on to the server itself. The name of a trusted domain may also be specified.
- The QSECOFR user profile is handled differently than all other user profiles. User authentication is not performed on Windows when SBMNWSCMD is run by the QSECOFR profile. The requested Windows command is run under the Windows Local System Account. The Local System Account is used even if the QSECOFR profile is enrolled. The Local System Account does not have a password and lacks network access rights.
- Do not use the "/u" parameter with the Windows "cmd" command.
- SBMNWSCMD has limited support of Kerberos v5 authentication. Kerberos will only be used when the LCLPWD MGT user profile attribute is *NO. See "SBMNWSCMD and file level backup support for Kerberos v5 and EIM" on page 82.
- 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 System i NetClient and Submit Network Server Command (SBMNWSCMD) functions. In i5/OS V5R3 or later, these functions provide limited Kerberos v5 support (also known as System i Network Authentication).

Keep these guidelines in mind if you want to use network authentication with file level backup for your integrated Windows server.

1. In order to enable System i to use Kerberos authentication, you must configure these things on the System i model:
 - System i Navigator Security option
 - Network authentication service
 - Enterprise Identity Mapping (EIM)
2. i5/OS NetServer should be configured to use Password/Kerberos v5 authentication and i5/OS NetServer must be active.
3. The Kerberos KDC must be a Windows Active Directory domain controller (Windows 2000 Server or Windows Server 2003). For more information, see "Enabling Kerberos with a Windows Server 2003 Active Directory Server" on page 66.
4. Kerberos authentication will only be used when the i5/OS job's user profile has the LCLPWDGMT attribute set to *NO. When LCLPWDGMT 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 LCLPWDGMT = *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**.

Using hot spare integrated server hardware

If a Windows server fails, you can quickly and easily switch the server's storage spaces to different integrated server hardware without restarting your System i product.

System i and System x integration and storage virtualization provide options that can enable you to enhance the reliability and recoverability of your Windows server environment. This may reduce the total number of servers needed to provide increased availability. It also adds flexibility by enabling one spare server to be used to protect multiple production servers.

The procedures for hot sparing an integrated server's hardware are shown below.

Switching to hot spare integrated server hardware using System i Navigator

1. Expand **Integrated Server Administration**.
2. Select **Servers**.
3. If the server for which you want to swap hardware is not already shut down:
 - a. Right-click the server and select **Shut Down**.
 - b. Click **Shut Down** on the confirmation panel.
4. Change the server configuration to point to the hot spare server hardware.
 - a. Right-click the server and select **Properties**.
 - b. Select the **System** tab and change one of the following:
 - Select the new **Resource name and type**.

Click **OK**.

5. To start the integrated server, right-click the server and select **Start**.

Switching to hot spare integrated server hardware using the character-based interface

1. If the server for which you want to swap hardware is not already varied off, use the **Vary Configuration (VRYCFG)** command to vary it off.
2. To change the server configuration to point to the hot spare server hardware, use the **Change Network Server Desc (CHGNWSD)** command to change one of the following:
 - a. Change the value for the **Resource name (RSRCNAME)** parameter to specify the new IXS or IXA hardware resource name.
3. To start the integrated server, use the **Vary Configuration (VRYCFG)** command.

Managing storage for integrated servers

Use these tasks to manage storage for integrated servers.

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 for integrated servers.” You can also read about “Predefined disks for integrated Windows servers” on page 87 and “Disks for integrated Windows servers” on page 85.

i5/OS storage management for integrated servers

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 System i products.

i5/OS and disk drives

i5/OS, the operating system that runs on a System i model, 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 “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 - 32. You can use disk pools to distribute your i5/OS data over different groups of disks. You can also use this concept to move less important applications or data to your older, slower disk drives. Support for independent ASPs (33-255) is provided through System i Navigator. Both the Information Center and System i Navigator refer to ASPs as Disk Pools.

Disk protection

i5/OS disks can be protected in 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 System i, you can attach controllers to more than one bus. Attaching the two disk controllers that form a mirrored pair to two different buses increases availability even more.

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

Disks 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 virtual 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 “Creating an integrated server disk drive” on page 88 and “Linking a disk drive to an integrated server” on page 89. 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 “Formatting integrated server disk drives” on page 90.

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.
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 IXS and IXA-attached integrated servers see 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.

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 System i virtual disk drive features supported for various types of server network server descriptions (NWSDs) with i5/OS V5R4 or later.

Table 6. Disk features supported

Feature	NWSD type ⁴ *WINDOWSNT or *IXSVR with OS type *WIN32
Number of fixed (static) links	16
Number of dynamic links	16
Number of cluster quorum links	1
Number of cluster shared links	15
Maximum number of virtual disks that can be linked to the server	48 with clustering ¹ ; 32 otherwise
Maximum capacity per virtual disk	1000 GB
Maximum total virtual disk capacity, assuming 1000 GB per disk	46.9 TB with clustering ¹ ; 31.3 TB otherwise
Can link virtual disks while the server is active?	Yes. Exceptions: fixed links
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
Virtual disk format types allowed when linking ²	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN
Virtual disk access types allowed when linking	Exclusive update, shared update ³
Disk links requiring exclusive update access type	All fixed disk links and all dynamic links
Disk links requiring shared update access type	Cluster quorum link and all cluster shared disk links

Note:

1. Windows server clustering requires use of Microsoft Cluster Service (MSCS) to control access to the shared disks in the cluster.
2. See the Create NWS Storage Space (CRTNWSSTG) command help text for a description of the format types.
3. 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.
4. See the Create Network Server Description (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 i5/OS NetServer.

The IBM i5/OS Integrated Server Support installation process creates several disk drives that are used to install and run integrated Windows servers. See the topic on “Predefined disks for integrated Windows servers.”

For information about creating drives, see “Creating an integrated server disk drive” on page 88

Predefined disks for integrated Windows servers

The IBM i5/OS Integrated Server Support installation process creates two disk drives (network server storage spaces) for installing and running integrated servers.

Predefined disks and naming conventions for integrated Windows servers

Integrated Windows servers have these predefined disks:

Boot and system drive (C)

This drive serves as the system drive. i5/OS names this drive *server1*, where *server* is the name of the network server description (NWSD). This disk drive resides in the integrated file system and is automatically linked as the first drive.

The C drive ranges from 1,024 to 1,024,000 MB.

Note: If you plan to create NWSD configuration files, be aware that support for these files exists only for disk drives that are formatted as FAT or FAT32. See “Network server description configuration files” on page 123. A system drive that has been converted to NTFS is not accessible for NWSD configuration files. For more information about the different file systems, see Comparison of FAT, FAT32, and NTFS file systems.

Installation source drive (D)

The D drive can be 200 - 2,047 MB and holds a copy of the Windows server installation code and the IBM i5/OS Integrated Server Support code. i5/OS names this drive *server2*, where *server* is the name of the NWSD. This disk drive resides in the integrated file system and is automatically linked as the second drive. i5/OS formats the D drive as a file allocation table (FAT) disk.

Attention:

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

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

Administering integrated Windows server disk drives from i5/OS

Administering integrated server disk drives (network server storage spaces) from i5/OS includes these tasks:

Accessing the i5/OS integrated file system from an integrated server

You can access the i5/OS integrated file system from an integrated server through IBM i5/OS Support for Windows Network Neighborhood (i5/OS NetServer). This allows you to easily work with file system resources on i5/OS.

For information about using i5/OS NetServer, see:

- Creating i5/OS NetServer file shares

- Configuring and connecting your PC clientSet up your PC client
- Access i5/OS NetServer file shares with a Windows client

For more information, see “Enabling i5/OS NetServer” on page 38.

Viewing information about integrated server disk drives

Obtain information what percentage of an integrated server disk drive (network server storage space) is in use or the format of the disk from within i5/OS.

To obtain disk drive information, follow these steps:

1. In System i Navigator, select **Integrated Server Administration** → **All Virtual Disks**.
2. Select a disk drive from the list available
3. Right-click the disk drive and select **Properties** or click the appropriate icon on the System i Navigator toolbar

If you want to use the CL command, see Work with Network Server Storage Spaces (WRKNWSSTG).

Adding 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 “Disks for integrated Windows servers” on page 85. To add an integrated server disk drive (network server storage space), perform these tasks:

Creating 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.

After creating the disk drive, you must link it to the network server description of your integrated server and format it. See “Linking a disk drive to an integrated server” on page 89 and “Formatting integrated server disk drives” on page 90. The time that you need to create a disk drive is proportional to the size of the drive.

To create an integrated server disk drive, follow these steps:

1. In System i Navigator, select **Integrated Server Administration**.
2. Right-click the **All Virtual Disks** folder and select **New Disk** or click the appropriate icon on the System i Navigator toolbar.
3. Specify a disk drive name and description.
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.

Note:

1. To link the new disk drive as a separate operation, see “Linking a disk drive to an integrated server.”
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.

Linking 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 disk to the integrated server.

You must create a disk drive before you can link it. See “Creating an integrated server disk drive” on page 88. 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 “Formatting integrated server disk drives” on page 90.

To link a disk drive to an integrated server, follow these steps:

1. If you are not linking a disk drive dynamically, then shut down your integrated server. See “Starting and stopping an integrated server” on page 76.
2. In , select **Integrated Server Administration** —> **All Virtual Disks**.
3. Right-click an available disk drive and select **Add Link**, or select the drive and click the appropriate icon on the System i Navigator toolbar.
4. Select the server you want to link the disk to.
5. Select one of the available link types and the link sequence position.
6. If you are linking the disk to an iSCSI attached server, select one of the available storage paths.
7. Select one of the available data access types.
8. Click **OK**.
9. If you are not linking a disk drive dynamically, then start your integrated server. See “Starting and stopping an integrated server” on page 76.

If you want to use the CL command, see ADDNWSSTGL.

If the disk drive is new and has not previously been formatted, refer to “Formatting integrated server disk drives” on page 90.

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.

Formatting 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 “Creating an integrated server disk drive” on page 88) and link (see “Linking a disk drive to an integrated server” on page 89) the disk drives, then start the Windows server from i5/OS (see “Starting and stopping an integrated server” on page 76).

Note: Servers can dynamically link disk drives while the server is varied on using the dynamic storage link parameter of the Add Server Storage Link (ADDNWSSTGL) command.

To format disk drives, follow these steps.

1. On the integrated Windows server console, from the **Start** menu, select **Programs**, then **Administrative Tools**, then **Computer Management**.
2. Double-click **Storage**.
3. Double-click **Disk Management**.
4. To create a new partition, right-click the unallocated space on the basic disk where you want to create the partition, and then click **New Partition**.
5. Follow the prompts to format the new drive.
 - a. Specify the storage space name for the volume label.
 - b. Select the file system you specified when you created the disk drive.
 - c. Select the quick format for a storage space that has just been created. It has already been low level formatted by i5/OS when it was allocated.

Copying an integrated server disk drive

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 System i Navigator toolbar.
4. Specify a disk drive name and description.

5. Specify the disk capacity. See the online help for details on valid disk sizes associated with a particular file system format. If you want to increase the size of the disk while copying it, you can specify a larger size. The extended portion of the disk will be unpartitioned free space.

Note: 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).

Expanding an integrated server disk drive

Expand a virtual disk (network server storage space) without copying the disk.


For information about expanding a boot disk, see “Expanding an integrated Windows server system drive” on page 92.

To expand a disk drive, follow these steps:

1. Expand **Integrated Server Administration** → **All Virtual Disks**.
2. Select a disk drive from the list available.
3. Right-click the disk drive and select **Properties** or click the appropriate icon on the System i Navigator toolbar.
4. Click on the **Capacity** tab of the disk drive property sheet.
5. Specify the increased disk size in the **New capacity** field. See the online help for details on valid disk sizes associated with a particular file system format. The extended portion of the disk will be unpartitioned free space.
6. Click **OK**.
7. If the disk is linked to an active server, a confirmation panel is shown to indicate that the disk drive will be temporarily unavailable to the server while the disk is being expanded. Click **Change** on the confirmation panel to confirm that this is acceptable, or click **Cancel** on the confirmation panel to cancel the disk expansion operation.

Note:

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.

Expanding an integrated Windows server system drive

To expand an integrated Windows server system disk, unlink the disk from the integrated server, expand the disk, and then relink the disk to the server.

Attention: You should back up your system drive before you expand it. See the Microsoft  web page (www.microsoft.com) for more information about using the DISKPART utility.

To expand a system drive, do the following steps.

1. Shut down the server. See “Starting and stopping an integrated server” on page 76.
2. Unlink the system drive disk from the server. See “Unlinking integrated Windows server disk drives.”
3. Change the size of the disk. See “Expanding an integrated server disk drive” on page 91.
4. Link the disk to a temporary server network server description as a data disk. See “Linking a disk drive to an integrated server” on page 89.
5. Start the temporary server. See “Starting and stopping an integrated server” on page 76.
6. On the temporary server Windows console, extend the partition of the disk using the DISKPART utility.
7. Shut down the temporary server. See “Starting and stopping an integrated server” on page 76.
8. Unlink the disk from the temporary server. See “Unlinking integrated Windows server disk drives.”
9. Link the expanded disk to the original server as the system disk. See “Linking a disk drive to an integrated server” on page 89.
10. Start the original server. See “Starting and stopping an integrated server” on page 76.

Unlinking 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 “Disks for integrated Windows servers” on page 85.

To unlink a disk drive, follow these steps:

1. If you are not unlinking a disk drive dynamically, shut down your integrated server. See “Starting and stopping an integrated server” on page 76.
2. In System i 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: **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.

Deleting integrated Windows server disk drives

Deleting a disk drive (network server storage space) destroys the data on the disk drive and frees the System i 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 “Unlinking integrated Windows server disk drives.” Once you have unlinked it, you can delete it.

To delete the disk drive, follow these steps:

1. In System i Navigator, select **Integrated Server Administration** → **All Virtual Disks**.
2. Select a disk drive from the list available.
3. Right-click the disk drive and select **Delete** or click the appropriate icon on the System i Navigator toolbar.
4. Click **Delete** on the confirmation panel.

If you want to use the CL command, see Delete NWS Storage Space DLTNWSSTG.

To find out what disk drives are associated with your server, see the topic “Viewing information about integrated server disk drives” on page 88

Deleting a disk 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 (NWS) for that server. You should also delete any additional disks that have been created for the that server.

The Delete Windows Server (DLTWNTSVR) command is provided to remove objects created by the Install Windows server (INSWNTSVR) CL command. It removes the network server description (NWS), line descriptions (LIND), storage spaces (NWSSTG), TCP interfaces, controller descriptions (CTLD), and device descriptions (DEV). 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.

Windows disk management programs and 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 NWS, the optical drive typically appears as drive E.

Sharing devices between i5/OS and integrated servers

Use System i devices on integrated servers.

One advantage integrated Windows servers have is the ability to use System i devices. You can use System i optical drives, tape drives, and printers from your Windows server.

Finding the device description and hardware resource names for System i devices

System i and Windows servers refer to devices by different names, so you first need to learn the appropriate device descriptions and hardware resource names you plan to use.

When you refer to System i devices on i5/OS, you need to use the device description name. When you refer to those devices from an integrated Windows server, you need to use the 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. Verify that the values in the Resource name and Device description fields match.

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.

Using System i optical drives with integrated Windows servers

To use an optical drive on an integrated server, vary it on from i5/OS.

Windows server can use an System i optical drive just as it does a local optical drive. The System i optical drive appears as a normal local optical drive in the **My Computer** folder on Windows server.

Locking an optical device

If you have logical partitions on your System i, the optical drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions and the optical drive must be allocated (locked) to a NWSD to be used.

To lock an optical drive, follow the steps below:

1. Click **Start**, then **Programs**, then **IBM 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 System i optical drive from an integrated Windows server, see Troubleshooting on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Transferring control of an optical drive from i5/OS to an integrated server

The optical drive must be varied on before you can allocate it to an integrated Windows server. If the optical drive is not varied on, follow these steps to vary it on:

1. Vary on the optical device.
 - a. At the i5/OS command line, type `WRKCFGSTS *DEV *OPT` and press Enter.
 - b. In the Opt column next to the correct optical device, typically OPT01, type 1 to vary on the optical drive.
 - c. Press Enter and the optical drive varies on.
2. Lock the optical device.
 - a. Click **Start**, then **Programs**, then **IBM 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 device name.

- f. Right-click and select **All Tasks, Lock Device**.

Note: If the integrated server fails before unlocking an optical device, the optical device may be unavailable to i5/OS or other integrated servers. You will need to vary off the optical device using `WRKCFGSTS *DEV *OPT` and vary it back on to free the lock.

Transferring control of an optical device from an integrated server to i5/OS

To use the optical drive from i5/OS, you must first unlock it from the integrated server. To unlock the optical drive from the integrated server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of the System i optical drive from an integrated server to System i, 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**.

Using System i tape drives with an integrated Windows server

Tasks for configuring a System i tape device to work with your integrated Windows server include allocating drives to integrated Windows servers, formatting tapes, transferring drives between servers, and transferring drives back to i5/OS.

System i tape drives can perform significantly faster than drives you normally attach to a PC server, and you can allocate them to integrated servers, therefore providing a faster tape access method than available to PC servers. See “Tested System i tape devices” on page 97.


Because multiple integrated servers in the same System i product can all access the same tape drive (although not at the same time), you need to allocate only one tape drive for multiple integrated servers.

Notes:

1. Although you can dedicate tape drives to the integrated server and to i5/OS, both systems cannot simultaneously use the same tape drive. The two operating systems require different tape formats. You cannot use the same tape on an integrated server and on i5/OS without reformatting it.
2. If you have logical partitions on your System i model, the tape drive is allocated to a single partition. It cannot be shared by integrated servers that are in other partitions.

To use an System i tape drive from an integrated server you must perform the following tasks:

- “Formatting a tape on i5/OS for use with integrated Windows servers” on page 96.
- Allocate an System i tape drive to an integrated server by varying off the tape drive from i5/OS and locking it on the integrated server. See “Allocating a System i tape drive to an integrated Windows server” on page 96.
- Transfer control of an System i tape drive to a different integrated server. See “Transferring control of System i tape and optical drives between integrated Windows servers” on page 98.
- 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 “Returning control of a tape drive from an integrated Windows server to i5/OS” on page 97.

If you have problems with an System i tape drive, see Troubleshooting  on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).


Installing tape device drivers for integrated Windows servers

Some tape devices require device drivers to be installed on the Windows operating system.

For information about supported tape device drivers, see Supported tape devices for Windows servers.

No special actions are required to install the drivers. The instructions provided by the driver provider should be sufficient. Using the new tape drivers, the tape drives look identical to drives available for System x hardware. The devices are still listed by type-model number in the device locking/unlocking utility.

After the tape device has been locked once and the server has rebooted, there may appear to be an extra instance of the device in the Removable Storage Manager, and some backup applications. This behavior is normal. It may be safe to delete these extra instances. Consult your documentation. For the latest

information see Tape driver migration  on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/windows/tape_driver_migration.html).

Formatting a tape on i5/OS for use with integrated Windows servers

Use the Initialize tape (INZTAP) command to format a System i tape drive to work with your integrated Windows servers.

To format a tape, do the following steps:

1. Insert a tape in the System i tape drive.
2. At the i5/OS command line, enter `INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED) CHECK(*NO) DENSITY(*CTGTTYPE) CODE(*EBCDIC)`, where *tap01* is the name of your tape drive.
3. Press Enter.

Allocating a System i tape drive to an integrated Windows server

To use an System i 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 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. i5/OS Integrated Server Support does not support tape libraries. Therefore, if your device has a tape library description, you must vary off both the tape device and the tape library device before locking the device on the integrated server.

To transfer control of the System i tape device to an integrated server, follow these steps:

1. Vary off the tape drive on i5/OS.
 - To do this from System i Navigator
 - a. Click **Configuration and Service** → **Hardware** → **Tape Devices**.
 - b. Click **Stand-Alone Devices** or **Tape Libraries**.
 - c. Right-click a device or library and select **Make Unavailable**.
 - To do this from the i5/OS character based interface
 - a. At the i5/OS command line, type `WRKCFGSTS *DEV *TAP`, and press the Enter key. The Work with Configuration Status display appears.

Note: `WRKCFGSTS *DEV *TAPMLB` will display a list of the tape library devices.
 - b. In the Opt column next to the device name of your tape drive, type 2 to vary off the tape drive.
 - c. Press Enter. The tape drive varies off.
2. Lock the tape device on an integrated server:
 - a. From its Windows console, click **Start** → **Programs** → **IBM iSeries** → **IBM i5/OS Integrated Server Support**.

- b. Expand **IBM i5/OS Integrated Server Support**.
- c. Expand the network server description name.
- d. Select **System i Devices**.
- e. Select the tape object that you want to lock.
- f. Right-click and select **All Tasks, Lock Device**.

If you need other information about the tape device to enable an application to recognize it, see “Identifying System i tape devices for applications” on page 98. If you have problems, see

Troubleshooting  on the System i integration with BladeCenter and System x web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Returning control of a tape drive from an integrated Windows server to i5/OS

To use a tape drive currently locked on an integrated server from i5/OS, you must first unlock it from the integrated server and vary it on from i5/OS.

To unlock the tape drive from Windows server, you must either be the person who originally locked the drive or have Administrator or Backup Operator authority.

To transfer control of a System i tape drive from an integrated Windows server to i5/OS, follow these steps:

1. Unlock the tape device from the integrated Windows server console.
 - a. Click **Start**, then **Programs**, then **IBM System i**, then **IBM i5/OS Integrated Server Support**
 - b. Expand **IBM i5/OS Integrated Server Support**
 - c. Expand the network server description name.
 - d. Select **System i Devices**.
 - e. Select the tape object that you want to lock.
 - f. Select **Action**, then **All Tasks**, then **Unlock Device**.
2. Make the device available to i5/OS from the i5/OS console.

From System i Navigator:

- a. Click **Configuration and Service** → **Hardware** → **Tape Devices**.
- b. Click **Stand-Alone Devices** or **Tape Libraries**.
- c. Right-click a device or library and select **Make Available**.

From the i5/OS command line interface:

- a. Type `WRKCFGSTS *DEV *TAP`, and press Enter. The Work with Configuration Status display appears.
- b. In the Opt column next to the tape drive device name (for example, TAP01), type 1 to vary on the tape drive.
- c. Press Enter. The tape drive varies on.
- d. Change the tape to one formatted for i5/OS.

Tested System i tape devices

Your ability to use System i tape devices from integrated Windows servers depends on tape device model, tape controller, and media type.

Refer to the Backup for Windows servers  web site to see which tape devices are supported.

Tape libraries are not supported as libraries, but they might 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.

Identifying System i tape devices for applications

View information about System i tape devices and how applications represent them.

Windows applications do not refer to tape devices by device description or hardware resource name as i5/OS does. Instead they show tape devices in one of three ways:

- Manufacture-feature-model number
- Device map
- Port-bus-target id-lun

If you need these values, do this:

1. On the integrated Windows server console, click **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
2. Click on **System Tools**.
3. Click on **Device Manager**.
4. Double-Click on **Tape Devices**.
5. Right-Click on a tape device.
6. Select **Properties**.
7. The properties box has two tabs, one marked **General** and one marked **Driver**. The **General** tab shows the name of the device and the Bus Number, Target ID and LUN.

If all the tape devices on your System i product are of different types, this information is enough to distinguish between them in Windows applications. If you have multiple tape devices of the same manufacture-feature-model number, you must experiment to determine which tape drive is which.

Transferring control of System i tape and optical drives between integrated Windows servers

System i tape and optical devices can only be used by one integrated server at a time.

To transfer control of tape and optical drives from one server to another, you must unlock it on one server and lock it on the other.

Note: If you have logical partitions on your System i product, the tape and optical drive is allocated to a single partition and cannot be shared by integrated servers that are in other partitions.

To transfer control of an System i tape or optical drive between integrated servers, follow these steps:

On the integrated server console that has control of the drive:

1. Click **Start** → **Programs** → **IBM System i** → **IBM i5/OS Integrated Server Support**
2. Expand **IBM i5/OS Integrated Server Support**
3. Expand the network server description name.
4. Select **System i Devices**
5. Select the device that you want to unlock.
6. Select **Action**, then **All Tasks**, then **Unlock Device**

On the integrated server console that you want to give control, lock the tape or optical drive.

1. Click **Start**, then **Programs**, then **IBM System i**, then **IBM i5/OS Integrated Server Support**
2. Expand **IBM i5/OS Integrated Server Support**

3. Expand the **Network Server Description** name
4. Select **System i Devices**
5. Select the device that you want to lock.
6. Select **Action**, then **All Tasks**, then **Lock Device**.

Printing from an integrated Windows server to System i printers

You must configure the integrated Windows server to allow TCP/IP printing and i5/OS to recognize the System i printer.

To send a print job to i5/OS, you must set up the i5/OS printer for TCP/IP printing. You must also set up the integrated server to use that printer through the LPD/LPR protocol. Your integrated server must also have the **Microsoft TCP/IP Printing** Network Service installed. See the Windows documentation for more information about TCP/IP Printing.

To set up an integrated server to print to System i printers, perform these tasks:

1. Set up the i5/OS printer for TCP/IP printing. For more information, see TCP/IP Setup topic collection.
2. Set up the integrated server to print to i5/OS printers:
 - a. From the **Start** menu on Windows 2000 Server or Windows Server 2003, click **Settings**, then **Printers**. The **Printers** window appears.
 - b. Double-click the **Add Printer** icon. The **Add Printer Wizard** starts.
 - c. Click the **Network Printer** button.
 - d. On the **Locate your Printer** panel, type the printer name or click **Next** to browse for the printer.

Administering integrated Windows server users from i5/OS

Integrate i5/OS users into the integrated Windows server

One of the main advantages of using integrated Windows server is synchronized, simplified user administration. Existing i5/OS user profiles and groups of profiles can be enrolled to integrated Windows servers, meaning that those users can log onto Windows server with the same user ID and password pair that they use to sign on to i5/OS. If they change their i5/OS password, their Windows password changes as well.

For conceptual information, see “User and group concepts for integrated Windows servers” on page 26.

Use this information to manage user enrollment for integrated Windows servers.

Enrolling a single i5/OS user to an integrated Windows server using System i Navigator

Enroll users with i5/OS user profiles to an integrated Windows server.

Create an i5/OS user profile for the user if one does not already exist. You can find information about creating i5/OS user profiles in the Security topic collection.

To enroll a single user to the integrated Windows server, follow these steps:

1. Expand **Integrated Server Administration** → **Servers** or **Integrated Server Administration** → **Domains**.
2. Right-click an available Windows domain or server from the list and select **Enroll Users**.

Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.

3. Select to enter the user name or choose the user name from the list.

4. Optional: If you want to use a user template as a basis for user settings, specify a Windows user to use as a template when creating the user on Windows. Remember that if you change the user template after you enroll a user, the changes will not affect the user.
5. Click **Enroll**.

If you have problems enrolling users, see Troubleshooting  on the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Enrolling an i5/OS group to your integrated Windows server using System i Navigator

Enroll all users in an i5/OS group to an integrated Windows server.

You can find information about creating i5/OS user and group profiles in the Security topic collection.

To enroll an i5/OS group and its members to the integrated Windows server, follow these steps:

1. Expand **Integrated Server Administration** → **Servers or Domains**.
2. Right-click an available Windows domain or server from the list and select **Enroll Groups**.

Note: Do not select a Windows workgroup. Enrollment to a workgroup is not supported.

3. Enter a group name or select an unenrolled group from the list.
4. Optional: To use a template to create new users, specify a Windows user to use as a template when creating users in the group on Windows. If you change the user template after you enroll a user, the changes do not affect the user.
5. Select **Global** if the group is being enrolled in a domain and the group should be visible to the domain. Otherwise, select **Local**. Windows server local groups can contain users and Windows server global groups, while Windows server global groups can contain only users. See the Windows online help for more information about group types.
6. Click **Enroll**.

If you have problems enrolling groups, see Troubleshooting  on the System i integration with BladeCenter and System x Web site (www.ibm.com/systems/i/bladecenter/troubleshooting.html).

Enrolling i5/OS users to an integrated Windows server using the character-based interface

Use the Change Network Server User Attributes (CHGNWSUSRA) command to enroll an i5/OS user to an integrated Windows server.

1. At the i5/OS character-based interface, type CHGNWSUSRA and press **F4**.
2. In the **User profile** field, type the name of the i5/OS user profile you want to enroll to the Windows environment.
3. Press **enter** twice. More fields should appear.
4. **Page down** and enter those Windows domains and Windows local servers you want to enroll the user to.
5. Press **enter** to accept the changes.

Table 7. CL commands for user enrollment

WRKUSRPRF	Work with i5/OS user profiles.
WRKNWSENR	Work with i5/OS user profiles enrolled to the Windows environment.
CHGNSWUSRA	Enroll i5/OS users to the Windows environment.

Creating user templates for integrated Windows servers

Use user enrollment templates to automatically configure users on your integrated Windows server.

A user enrollment template is a tool to help you enroll users from i5/OS to the Windows environment more efficiently. You do not have to manually configure many new users with identical settings.

You can make a user template a member of any Windows server group, whether you enrolled that group from i5/OS or not. You can enroll users with a template that is a member of a group that was not enrolled from i5/OS. If you do this you can only remove users from the group by using the User Manager program on Windows server.

If you are creating a template that will be used to enroll administrators, you may want to make the template a member of the Windows server group *Administrators*. Likewise, if you want to protect Windows users from accidental deletion from i5/OS, enroll the template in the *AS400_Permanent_Users* (or *OS400_Permanent_Users*) group.

Follow these steps to create a Windows template.

Creating user profiles for a Windows 2000 Server or Windows Server 2003 domain

Do these steps at the integrated server console.

1. Click **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Click the domain name.
3. Right-click **Users**, then select **New** → **User**.
4. In the **Username** and **Logon name** fields, enter a distinctive name for the template, such as *stduser* or *admtemp*. Click **Next**.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **User cannot change password**, **Password never expires**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access the integrated server.
6. Do not enter a password for a template account.
7. Click **Finish**.
8. To set up group memberships, double-click the template name in the list of domain users and groups that appear in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

Creating user profiles on Windows 2000 Server or Windows Server 2003 server

Do these steps at the integrated server console.

1. Open the Local Users and Groups window.
 - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
 - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
2. Select **System Tools** → **Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. In the **User name** field, enter a distinctive name for the template, such as *stduser* or *admtemp*.
5. It is recommended that you also deselect the **User must change password at next logon** check box and select the **Password never expires**, **User cannot change password**, and **Account is disabled** checkboxes. This prevents anyone using the template account itself to access Windows server.
6. Click **Create**, then **Close**.
7. Click **Users** or refresh to show the new user template.

8. To set up group memberships, double-click the template name in the list of domain users and groups that appears in the right pane. Click the **Member of** tab and then click **Add** to add the groups that you want.

Specifying a home directory in a template

Follow these steps to specify a home director in a user template.

To allow integrated Windows servers to manage users in the most portable way possible, a home directory can be set up for each user to store user-specific information generated by applications. To minimize the amount of work that must be done, specify home directories in the template accounts so that each new profile created by the enrollment process has a home directory created for it automatically. To provide scalability, it is important not to lock home directories to a particular disk drive. Use the Universal Naming Convention (UNC) names to give portability.

To customize your template profiles to include a home directory, follow these steps from the integrated Windows server console:

1. Create the home directory folder on the appropriate server, and share it.
2. In a domain, click **Start** → **Programs** → **Administrative Tools** → **Active** → **Directory Users and Computers** from the Windows console. On a local server, click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
3. Double-click the template (model user) to display its properties.
4. Click the Profile tab.
5. In the Home folder segment, click **Connect**. Select a drive letter (such as Z:). Move to the **To:** dialog, and enter the directory path of the home directory using a UNC name, for example: `\\systemiWin\homedirs\%username%`. In this example, **systemiWin** is the name of the server where the home directory folder resides, and **homedirs** is the name of the home directory folder. If you use the variable `%username%`, instead of the logon or user name, Windows server automatically substitutes the user's name in place of the variable name when each new Windows server account is created. It also creates a home directory for the user.

Changing the LCLPWDMGT user profile attribute

Use these steps to change the Local Password Management (LCLPWDMGT) user profile attribute.

1. Type CHGUSRPRF and the user profile name you want to change.
2. Press F4 to prompt.
3. Press **F9** to view all attributes and **F11** to view their abbreviations.
4. Find the attribute LCLPWDMGT and set it to *YES or *NO.
5. Press enter.

Enterprise Identity Mapping (EIM)

Use this information to configure a user account to use EIM.

What is EIM?

Enterprise Identity Mapping (EIM) is a way to consolidate a user's various UserIDs and passwords together under a single account. Using it, a user can log on just once to a system, and then EIM will work together with other services behind the scenes to authenticate the user to all of his accounts.

This is called a single sign-on environment. Authentication still takes place whenever users attempt to access a new system; however, they will not be prompted for passwords. EIM reduces the need for users to keep track of and manage multiple user names and passwords to access other systems in the network. Once a user is authenticated to the network, the user can access services and applications across the enterprise without the need for multiple passwords to these different systems.

The EIMASSOC user profile attribute

EIMASSOC is a user profile attribute specifically designed to aid in configuring EIM. At the i5/OS command prompt type CHGUSRPRF and the user profile name and then press F4 to prompt. Then page down to the very bottom and you will see a section labeled EIM association. Here is a summary of what the fields mean:

- **Element 1: EIM identifier** This is the UserID that EIM uses to identify you. Think of it as your Master ID under which all your other user IDs will be stored. If you specify *USRPRF the system will use your i5/OS user profile name as the EIM identifier. Alternatively, you can specify any valid character-string. If you enter *DLT in this field and press enter, you will be presented with a list of changed options for deleting EIM associations.
- **Element 2: Association type** This value specifies how the i5/OS user profile that you are editing will be associated with the EIM identifier. The values of *TARGET, *TGTSRC, or *ALL will allow auto-creation or deletion of i5/OS target and Windows source associations.
- **Element 3: Association action** The special values are:
 - *REPLACE The Windows source associations will be removed from all EIM identifiers that have an association for this user profile. For the enrolled user, a new Windows source association will be added to the specified EIM identifier.
 - *ADD For the enrolled user, a Windows source association will be added.
 - *REMOVE The Windows source association will be removed.
- **Element 4: Create EIM identifier** This value specifies whether the EIM identifier should be created if it does not already exist. The special values allowed are, *NOCRTEIMID, an EIM identifier will not be created, or, *CRTEIMID, an EIM identifier will be created if it does not exist.

Automatic and Manual EIM associations

In a typical EIM configured environment, which uses single sign-on, i5/OS target associations and Windows source associations are typically defined. With integrated Windows server user administration, the system administrator may decide to define enrolled Windows users to have EIM associations automatically defined. For instance, if an enrolled Windows user has EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) specified, i5/OS will automatically create an i5/OS target and a Windows source association. The EIMASSOC information is not stored in the user profile. Also, this information is not saved or restored with the user profile. And, if the i5/OS system is not configured for EIM, then no association processing is done and the EIMASSOC information is ignored.

If i5/OS is configured to use EIM and EIMASSOC processing is defined for the enrolled user, integrated Windows server user administration will auto create or delete Windows source associations for the user in the Windows EIM registry. For a user enrolled locally to the Windows environment, the Windows EIM registry name is the fully qualified, local Domain Name System (DNS) name. The Windows EIM registry type is defined to be Windows 2000. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be Kerberos - case ignore. If EIMASSOC is defined for a user, and i5/OS is configured to use EIM, and the Windows EIM registry doesn't exist, integrated Windows server user administration will create the Windows EIM registry.

Use EIM associations to allow different Windows user profile names

EIM provides a mechanism to associate user profiles in a directory system. EIM allows for an EIM identifier to have an i5/OS user profile target association defined and a Windows user profile source association to be defined. It is possible for a user administrator to define a Windows source association using a different Windows user profile name than the i5/OS target association user profile name. Integrated Windows user administration will use the defined EIM Windows source association Windows user profile, if it exists, for Windows user enrollment. The i5/OS target association needs to be defined. Using the EIM identifier, the Windows source association needs to be defined by the administrator. The

Windows source association needs to be defined for the same EIM identifier in the correct Windows EIM registry name and type. For a user enrolled locally to Windows, the Windows EIM registry name is the fully qualified, local domain name server (DNS) name. The Windows EIM registry type is defined to be EIM_REGTYPE_WIN2K. For users enrolled to a Windows domain, the Windows registry name is the fully qualified domain DNS name and the Windows registry type is defined to be EIM_REGTYPE_KERBEROS_IG.

End user enrollment to integrated Windows servers

To end the enrollment of a user to Windows domains and servers, do these steps at the Windows console.

To end the enrollment of a user to Windows domains and servers, follow these steps on the integrated Windows server console:

1. Expand **Integrated Server Administration** —> **Servers or Domains**.
2. Expand the domain or server that contains the user that you want to unenroll.
3. Select **Enrolled Users**.
4. Right-click the user that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** on the confirmation window.

Effects of ending user enrollment to the integrated Windows server

When you end user enrollment from the Windows environment, you also remove the user from the list of enrolled Windows server users, as well as from the Windows server group AS400_Users (or OS400_Users). Unless the user is a member of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users), you also delete the user from the Windows environment.

You cannot delete users who are members of the Windows server group AS400_Permanent_Users (or OS400_Permanent_Users) from Windows server by either ending enrollment or deleting them from i5/OS. However, ending enrollment does remove the user from the list of enrolled Windows server users and from the Windows server group AS400_Users (OS400_Users).

You can keep users on the Windows environment after you have ended their enrollment on i5/OS. This practice is not recommended, since it makes it possible to add these users to groups on i5/OS and change passwords on i5/OS without these updates ever appearing in the Windows environment. These discrepancies can make it difficult to keep track of users on either system.

You can end user enrollment in a number of ways. Actions that end user enrollment include the following:

- Intentionally ending enrollment for the user.
- Deleting the i5/OS user profile.
- Ending enrollment for all i5/OS groups to which the user belongs.
- Removing the user from an enrolled i5/OS group when the user does not belong to any other enrolled groups.

Ending group enrollment to an integrated Windows server

To end the enrollment of a group to Windows environment domains and servers, follow these steps.

When you end enrollment of a group to the integrated Windows server, all users whose enrollment is limited to that group also have their enrollment ended. If the group has only members that were enrolled through it, the group is deleted from the integrated Windows server.

However, if the group has any members that were added from the Windows operating system rather than enrolled from i5/OS, the group is not deleted. The only members that the group can still have are nonenrolled users.

To end the enrollment of a group to Windows domains and servers, follow these steps in System i Navigator:

1. Expand **Integrated Server Administration** → **Servers or Domains**.
2. Expand the domain or server that contains the group that you want to unenroll.
3. Select **Enrolled Groups**.
4. Right-click the group that you want to unenroll.
5. Select **Unenroll**.
6. Click **Unenroll** in the confirmation window.

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 these situations.

- You are enrolling on a domain through a member server.
- You are enrolling on a local server using a template which specifies a home directory path
- You are enrolling on a domain through an i5/OS partition which contains both domain controllers and member servers on the same domain.

You do not need to set up the QAS400NT user in order to successfully enroll an i5/OS user or group profile on a domain or local server in the following cases:

- You are enrolling on a domain through an i5/OS partition which contains a domain controller but no member servers on the same domain.
- You are enrolling on a local server (or locally on a member server) using a template which does not specify a home directory path.

If you need to set up the QAS400NT user, follow these steps:

1. Create the QAS400NT user profile on i5/OS with User class *USER. Take note of the password because you need it in the next step. Make sure that the password complies with the rules for Windows passwords if you are enrolling on a domain.
2. Create the QAS400NT user account on the Windows console of the integrated Windows server you are enrolling through. Note that the i5/OS user profile password and Windows user account password must be the same for the QAS400NT user.
 - a. Setting up QAS400NT on a domain controller

On the domain controller of the domain you are setting up enrollment for, create the QAS400NT user account as follows:

- 1) From the integrated server console
 - a)
 - In Windows 2000 Server click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
 - In Windows Server 2003 click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
 - b) Select **System Tools** → **Local Users and Groups**.
- 2) Right-click the **Users** folder (or the folder that the user belongs to), and select **New** → **User...**
- 3) Enter the following settings:

Full name: qas400nt
User logon name: qas400nt
- 4) Click **Next**. Enter the following settings:

Password: (the same password as you used for QAS400NT on i5/OS)
Deselect: User must change password at next logon
Select: User cannot change password
Select: Password never expires

- 5) Click Next, then Finish
- 6) Right click the QAS400NT user icon and select Properties.
- 7) Click the **Member Of** tab and then Add.
- 8) Enter Domain Admins in the box and click OK, then OK again. This gives the QAS400NT user account sufficient rights to create users.

b. Setting up QAS400NT on a local server

On the local server (or member server if you are enrolling locally) you are setting up enrollment for, create the QAS400NT user account as follows:

- 1) From the integrated server console
 - In Windows 2000 Server click **Start → Programs → Administrative Tools → Computer Management → Local Users and Groups**.
 - In Windows Server 2003 click **Start → Programs → Administrative Tools → Computer Management → System Tools → Local Users and Groups**.

- 2) Right-click the **Users** folder, and select **New User....**

- 3) Enter the following settings:

User name: qas400nt
Full name: qas400nt
Password: (the same password as you used for QAS400NT on i5/OS)
Deselect: User must change password at next logon
Select: User cannot change password
Select: Password never expires

- 4) Click Create, then Close.
- 5) Right click the QAS400NT user icon and select Properties.
- 6) Click the Member Of tab and then Add.
- 7) Enter Administrators in the box and click OK, then OK again. This gives the QAS400NT user account rights to the User Administration Service.

3. Enroll the i5/OS QAS400NT user profile on the domain or local server using System i Navigator or the CHGNWSUSRA command. Do not try to use a template when enrolling QAS400NT.
4. Use System i Navigator or the WRKNWSENDR command to confirm that QAS400NT has been successfully enrolled. You may now enroll i5/OS user profiles through domain controllers or member servers on the domain.

Notes:

- You may change the QAS400NT password from i5/OS since it is now an enrolled user.
- If there are multiple integrated servers that belong to different domains on a single i5/OS partition, you must set up QAS400NT for each domain. All QAS400NT user accounts must have the same password as the i5/OS user profile. Alternatively, consider using Active Directory or trust relationships between domains, and enroll users on only a single domain.
- If you have multiple i5/OS partitions and multiple integrated servers, QAS400NT passwords on different i5/OS partitions can be different as long as each domain does not contain integrated servers on more than one i5/OS partition. The rule is, all i5/OS QAS400NT user profiles and corresponding Windows user accounts must have the same password for a single domain.
- Be sure not to delete the QAS400NT user profile on i5/OS, or let the password expire. To minimize the risk of the QAS400NT password expiring on one of multiple i5/OS partitions on the same Windows domain, it is recommended that you allow only one i5/OS partition to propagate changes to the QAS400NT user profile.
- If you have multiple i5/OS partitions, each with an integrated Windows server on the same domain, failing to keep the QAS400NT password synchronized across all i5/OS partitions can cause enrollment

problems. To minimize this problem, it is recommended that you limit propagation of changes to the QAS400NT password to just one i5/OS partition, but still allow other partitions to keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only.

Preventing enrollment and propagation to an integrated Windows server

Use these tasks to prevent users from being enrolled or propagated to an integrated Windows server.

There are several reasons why you might want to prevent i5/OS user profile propagation to a particular integrated server:

- If there are multiple integrated servers that belong to the same domain, and they are all on the same i5/OS partition, user profile enrollment will, by default, go through all of the integrated servers in that partition. To reduce network traffic you can turn off enrollment to all integrated servers on the domain except one. This single integrated server would normally be the domain controller, if it is in the partition.
- If there are multiple integrated servers that belong to the same domain, but they are all on different i5/OS partitions, there is a risk of the QAS400NT passwords getting out of synchronization and causing problems with user profile enrollment. By preventing propagation of the QAS400NT user profiles from all i5/OS partitions except one, you can reduce the risk of enrollment problems. Notice that the other i5/OS partitions keep sufficient authority to enroll users. Then, failure to change a password on one of the other partitions prevents user enrollment from that partition only.

There are two methods to prevent i5/OS user profile propagation to a particular integrated server:

- Use the Propagate Domain User (PRPDMNUSR) parameter. See below for a description of how to do this.
- Create data areas with the Create data area (CRTDTAARA) command. See below for a description of how to do this.

Notes:

- Do not turn enrollment off for all of the integrated servers on the domain. Otherwise all your users may go to update pending (*UPDPND) status, and no further propagation takes place.
- You may want to leave two integrated servers enabled for user enrollment so that you can still make changes if one of the servers is down.

Using the PRPDMNUSR parameter to prevent enrollment to a domain through a specific integrated server

The Propagate domain user (PRPDMNUSR) parameter of the Change network server description (CHGNWSD) command can be used to prevent user enrollment to a domain through a specific integrated server.

You can also set this parameter when installing an integrated server using the Install Windows Server (INSWNTSVR) command. This option may be useful in the case where there is a single i5/OS partition which controls multiple integrated Windows servers that belong to the same domain, because it can turn off enrollment for all integrated servers except one.

To use the PRPDMNUSR parameter to prevent user enrollment, do these steps.

1. Using the Work with Network Server Description (WRKNWSD) command, select the integrated server you wish to stop enrollment on. (You do not need to vary off the server.)
2. Enter the command: CHGNWSD NWSD(nwsdname) PRPDMNUSR(*NO)

Using the CRTDTAARA command to prevent enrollment of QAS400NT to a specific integrated server

The Create Data Area (CRTDTAARA) command can be used to prevent enrollment of the QAS400NT user profile only, for the specified integrated server. The propagation of other user profiles is not affected.

This option may be useful in the case where there are multiple integrated servers that belong to the same domain, but they are all on different i5/OS partitions. You want to enroll user profiles from these different i5/OS partitions, but not have multiple QAS400NT user profiles propagating passwords to the domain. Follow these steps:

1. Choose one i5/OS partition that you wish to use for enrollment of QAS400NT on the domain. Ensure that QAS400NT is enrolled on this i5/OS partition.
2. If QAS400NT is enrolled on other i5/OS partitions follow these steps:
 - a. On the domain controller, add the QAS400NT user account to the OS400_Permanent_Users group to ensure that it is not deleted.
 - b. On the i5/OS partitions where you want to prevent enrollment of QAS400NT, delete the QAS400NT user profile.
3. On the i5/OS partitions where you want to prevent enrollment of QAS400NT, create a data area with this command: `CRTDTAARA DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE(*NOPROP)` where **nwsdname** is the name of the network server description for the integrated server, and ***NOPROP** is the keyword that signals that QAS400NT user profile parameters (including the password) are not propagated from this i5/OS partition.
4. Create and enroll the QAS400NT user profile on each of the i5/OS partitions you created the data area on. Notice that you still need to keep the QAS400NT password current (not expired) on all these i5/OS partitions for enrollment of user profiles (other than QAS400NT) to occur. Because the QAS400NT password is not propagated, it does not matter what the password is, as long as it is not expired.

Backing up and recovering IXS or IXA-attached integrated Windows servers

Back up your integrated server files to System i tape devices or disks.

Because integrated Windows servers combine 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 i5/OS, 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 i5/OS. See “Backing up the NWSD and other objects associated with integrated Windows servers” on page 109.
- Back up individual integrated server files by using the i5/OS SAV and RST commands and i5/OS NetServer or a backup utility. See “Backing up individual integrated Windows server files and directories” on page 113.

Your recovery options depend on how you backed up your system, as well as what you need to recover.

- If you need to recover your entire system, see the Recovering your system topic collection.
- If you need to restore a network server description and its associated i5/OS disk drives, refer to “Restoring the NWSD and disk drives for an integrated Windows server” on page 117.
- To restore integrated server data (files, directories, shares, and the Windows registry) that you backed up with the Save (SAV) command, see “Restoring integrated Windows server files” on page 120.

- To restore files that you saved with Windows backup utilities or other utilities, use those utilities.

Backing up the NWSD and other objects associated with integrated Windows servers

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. 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.

See “Predefined disks for integrated Windows servers” on page 87.

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. You can 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 “Backing up individual integrated Windows server files and directories” on page 113.

Backing 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.

Backing 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 disks for integrated Windows servers” on page 87.

Note:

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 i5/OS Information Center.

The virtual disks that you create for your integrated servers are in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command..

Note: You can use the same steps for backing up predefined disks (the system disk and the installation disk) and user defined disks.

To save disk drives (network server storage spaces) from i5/OS, do this:

1. Ensure that the auxiliary storage pool (ASP) that contains the disk is varied on.
2. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
3. Shut down the integrated server to prevent users from updating files during the backup. See “Starting and stopping an integrated server” on page 76.
4. On the i5/OS command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device . For example, specify /QSYS.LIB/TAP01.DEVD in the *Device* field.
6. If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device.
For example, to use a save file named MYSAVF in library WINBACKUP, you would specify '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE' for the device.
7. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc', where stgspc is the name of the network server storage space.
For example, if the NWSD for the integrated server is named *testserver*, you can save the system and install disks by saving these network server storage spaces:
 - /QFPNWSSTG/*testserver1*
 - /QFPNWSSTG/*testserver2*
8. If you are saving a disk for an active server, specify the following values:
 - a. Specify *YES for the **Save active** parameter. This option allows the storage space to be saved while it is still being used the system.
 - b. Specify *NWSSTG for the **Save active option** parameter. This option allows network server storage spaces in directory '/QFPNWSSTG' to be saved when they are active.
9. Specify values for any other parameters that you want and press Enter to save the storage space.
10. Start the integrated server. See “Starting and stopping an integrated server” on page 76.

You can read more here: “What objects to save and their location on i5/OS” on page 111.

Backing up user-defined disk drives for integrated Windows servers

Use the Save (SAV) command to back up user-defined disks for your IXS or IXA-attached integrated Windows server.

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.

The virtual disks that you create for your integrated servers are in the integrated file system. To save these storage spaces from i5/OS, you use the Save (SAV) command..

Note: You can use the same steps for backing up predefined disks (the system disk and the installation disk) and user defined disks.

Do the following steps to back up integrated server disks from the i5/OS operating system.

1. Ensure that the auxiliary storage pool (ASP) that contains the disk is varied on.
2. If you are saving to tape, ensure that you have mounted a tape that is formatted for i5/OS.
3. Shut down the integrated server to prevent users from updating files during the backup. See “Starting and stopping an integrated server” on page 76.
4. On the i5/OS command line, type SAV and press F4.
5. If you are saving the storage space to tape, specify the name of your tape device . For example, specify /QSYS.LIB/TAP01.DEVD in the *Device* field.

6. If you are saving the storage space to a save file instead of to tape, specify the path to the save file as the device.
For example, to use a save file named MYSAVF in library WINBACKUP, you would specify `'/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE'` for the device.
7. In the Name field under Objects:, specify `'/QFPNWSSTG/stgspc'`, where stgspc is the name of the network server storage space.
For example, if the NWSD for the integrated server is named *testserver*, you can save the system and install disks by saving these network server storage spaces:
 - `/QFPNWSSTG/testserver1`
 - `/QFPNWSSTG/testserver2`
8. If you are saving a disk for an active server, specify the following values:
 - a. Specify `*YES` for the **Save active** parameter. This option allows the storage space to be saved while it is still being used the system.
 - b. Specify `*NWSSTG` for the **Save active option** parameter. This option allows network server storage spaces in directory `'/QFPNWSSTG'` to be saved when they are active.
9. Specify values for any other parameters that you want and press Enter to save the storage space.
10. Start the integrated server. See “Starting and stopping an integrated server” on page 76.

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, see “Backing up individual integrated Windows server files and directories” on page 113.

Saving and restoring user enrollment information for integrated Windows servers

Use CL commands and APIs to save and restore user profiles and enrollment information for an integrated Windows server

More i5/OS backup and recovery security information may be found in the Backup and Recovery of Security Information section in the Security reference topic collection.

User profiles may be saved using the SAVSECDTA command or the QSRSAVO API. The i5/OS system value QRETSVRSEC must be set to 1 for integrated Windows server enrollment support. User profiles saved with the SAVSECDTA command or QSRSAVO API may be restored using the RSTUSRPRF command and specifying the parameter USRPRF(*ALL). If the parameter USRPRF(*ALL) is not specified, then user profiles may be restored if the parameter and value SECDTA(*PWDGRP) is specified.

If you save user profiles using the QRSOVO API, and a previous target release value is used, the user profile enrollment definitions will not be restored. After restoring the user profiles, the enrollment needs to be defined. Use System i Navigator or the Change Network Server User Attributes (CHGNWSUSRA) command to define the enrollment.

User profiles need to be saved and restored using the above methods for integrated Windows server enrollment. User profiles saved and restored using other commands or API are not supported for Windows.

What objects to save and their location on i5/OS

Use these tables to determine which objects need to be saved when you save your integrated Windows server.

Many objects are created as a result of installing integrated servers. Some of these objects are system-related, others user-related. You need to save them all if you want to restore properly. You can

save these objects by using options of the i5/OS GO SAVE command. Option 21 saves the entire system. Option 22 saves system data. Option 23 saves all user data (which includes objects in QFPNWSSTG).

If you want to save a particular object, use one of the following tables to see the location of that object on i5/OS and the command to use. The topic Manually saving parts of your system has more information about using the save commands. In addition to saving the entire drive (storage space), you can also save and restore individual files and directories.

- Important:** Ensure that the auxiliary storage pool (ASP) is available when you save the data.

Objects to save for all types of integrated servers

Object content	Object name	Object location	Object type	Save command
Integrated server disks	Various	/QFPNWSSTG	Network server storage space	GO SAVE, option 21 or 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/TAP01.DEVD')
Messages from the integrated server	Various	Various	Message queue	GO SAVE, option 21 or 23 SAVOBJ OBJ(msgq) LIB(qlibrary) DEV(TAP01) OBJTYPE(*MSGQ)
i5/OS config objects for integrated servers	Various	QSYS	Device config objects	GO SAVE, option 21, 22, or 23 SAVCFG DEV(TAP01)
i5/OS based and Windows-based IBM iSeries Integrated Server Support code	QNTAP, NTAP and subdirectories	QSYS and /QIBM/ProdData/NTAP	Library and Directory	SAVLICPGM LICPGM(5761SS1) OPTION(29)
Windows server file shares	QNTC and subdirectories	/QNTC/servername/sharename	Directory	GO SAVE, option 21 or 22 SAV
i5/OS TCP interfaces	QATOCIFC	QUSRSYS	physical file Note: TCP/IP must be ended when you save the TCP interface physical files.	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
i5/OS TCP interfaces	QATOCLIFC	QUSRSYS	logical file Note: TCP/IP must be ended when you save the TCP interface physical files.	GO SAVE, option 21 or 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)

Backing up individual integrated Windows server files and directories

You can use i5/OS file level backup support or a third party program to back up individual integrated Windows server files.

IBM i5/OS Integrated Server Support allows you to save integrated server data (files, directories, shares, and the Windows registry) to tape, optical or disk (*SAVF) along with other i5/OS data and restore the data on an individual basis. However, you should not use this approach as your primary backup procedure. You should still periodically save your entire system and the NWSD associated with your Windows server for disaster recovery. Then you can choose to do daily backups of only the integrated server files that have changed. See “Backing up the NWSD and other objects associated with integrated Windows servers” on page 109.

For information about the file-level backup function, see these topics:

- First read “File-level backup restrictions for integrated Windows servers.”
- To do file-level backup of your integrated server, you must first refer to: “Configuring an integrated Windows server for file-level backup” on page 114.
- “Saving your integrated Windows server files” on page 116

You can also use a utility such as the Backup program that comes with Windows (see “Using the Windows Backup utility on your integrated Windows server” on page 117). 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 for integrated Windows servers

File-level backup for integrated Windows servers has some limitations and requirements for the environment.

Limitations

- This support is not available to stand-alone Windows servers because the code comes packaged with IBM i5/OS Integrated Server Support.
- This method does not back up files that are part of the IBM i5/OS Integrated Server Support code.
- You cannot stop users from signing on and accessing data on the server while the Save (SAV) or Restore (RST) command is running. IBM i5/OS Integrated Server Support can save a file that is in use as long as it can read the file. Consequently, you should back up integrated server files when you expect few users to be accessing the system. A note telling users to avoid accessing the server would be a good precaution.
- Windows Server 2003 provides function with its Volume Shadow copy Service (VSS). This allows applications that are backup aware the ability to save files while they are still in use when using file-level backup
- The QSECOFR user profile should not be used to perform a file-level backup. Even if enrolled to the integrated server, QSECOFR will not be used to back up the files. The Windows Local System Account will be used instead. It may not have the necessary authority to back up all of the requested files.
- If the user profile *LCLPWDMGT value is *YES, then the system value, QRETSVRSEC, must be set to 1 and the user password must be changed or the user have signed-on after QRETSVRSEC was changed.
- If the user profile *LCLPWDMGT value is *NO, then network authentication (kerberos) is used. The user must access the i5/OS operation through an EIM enabled application (like System i Navigator single-signon). See “SBMNWSCMD and file level backup support for Kerberos v5 and EIM” on page 82 for more information.

Requirements

- The integrated server must be active and have a working TCP/IP point to point virtual Ethernet connection with the i5/OS operating system. You must back up your integrated server files either before putting the system into restricted state to back up the rest of the i5/OS files or after completing restricted state operations.
- This procedure requires that you have the same user ID and password on the integrated server and the i5/OS operating system.
- Your integrated server user account must be a member of the Administrators group.
- File-level backup uses the QNTC file system (NetClient) to build the list of files to be saved. QNTC uses i5/OS NetServer to locate servers in the domain. You need to have the i5/OS NetServer in the same domain (see “Ensuring i5/OS NetServer and the integrated Windows server are in same domain” on page 115) 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.

Configuring an integrated Windows server for file-level backup

Do these steps to configure an integrated Windows server for file-level backup

1. Ensure that the person who is saving and restoring files has the same password on i5/OS and the integrated server. The easiest method is found at “Enrolling a single i5/OS user to an integrated Windows server using System i Navigator” on page 99. Also ensure that the user is a member of the Administrators group. Refer to “Creating user templates for integrated Windows servers” on page 101.
2. Create shares for each drive or volume that you want to save when you request to save all the files on a Windows server. IBM i5/OS Integrated Server Support accesses the file system and translates these shares into path-names. See “Creating shares on integrated Windows servers.”
3. Add members to the QAZLCSAVL file in QUSRSYS that lists the share names that you want to be able to save. See “Adding members to the QAZLCSAVL file” on page 115.
4. Ensure that i5/OS NetServer is in the same domain as the integrated server for which you want to save files. See “Ensuring i5/OS NetServer and the integrated Windows server are in same domain” on page 115.
5. Ensure that the person performing the saves or restores has *ALLOBJ authority which gives the user full access to the programs and devices required for the save or restore process. If *ALLOBJ authority cannot be provided, the user must have at least *USE authority on object QNTAP/QVNASBM so the backup or restore request can be communicated to the integrated Windows server server.

Creating 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 Windows servers, do this from the integrated server console:

1. Open the **My Computer** icon to open **Windows Explorer**.
2. Right-click the drive or volume that you want.
3. From the pop-up menu, select **Sharing**.
4. Click **Share this folder**. Provide a **Share Name** (characters in the share name must be in the more restrictive code page 500 character set). The default share name is the same as the last part of the directory name. Share names can be no longer than 12 characters and can include embedded blanks.

5. You can choose unlimited access or limit the number of users who can access the share at one time. You can also use the **Permissions** button to set up the level at which you want to share (No Access, Read, Change, or Full Control).
6. Click on **Apply** to create the share.

Adding members to the QAZLCSAVL file:

To enable file-level backup and recovery from i5/OS, add a member for each integrated 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, use the Add Physical File Member (ADDPFM) command to add a file member. Type

```
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nwsdname)
TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE).
```
2. In the file member that you just created, list all the shares that you want to be able to save. List each share name that you defined for the server on a separate line. The maximum length that the Windows share name can be is 12 characters. Share names can have embedded blanks. For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as shares on WINSVR1, your member name WINSVR1 would look like this:

```
QUSRSYS/QAZLCSAVL
WINSVR1
0001.00  cshare
0002.00  dshare
0003.00  eshare
0004.00  fshare
0005.00  gshare
0006.00  my share
```

Note: If you specify multiple share names that point to the same integrated server directory, i5/OS saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not include multiple shares that include the same directory or data.

Ensuring i5/OS NetServer and the integrated Windows server are in same domain:

To save integrated server files for file-level backup, you must have i5/OS NetServer in the same domain as the files you want to save.

For the member name, use the NWSD name of the server (*nwsdname*).

To add a member, do this:

1. On the i5/OS command line, use the Add Physical File Member (ADDPFM) command to add a file member. Type

```
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nwsdname)
TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE).
```
2. In the file member that you just created, list all the shares that you want to be able to save. List each share name that you defined for the server on a separate line. The maximum length that the Windows share name can be is 12 characters. Share names can have embedded blanks. For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as shares on WINSVR1, your member name WINSVR1 would look like this:

```
QUSRSYS/QAZLCSAVL
WINSVR1
0001.00  cshare
0002.00  dshare
```

```
0003.00  eshare
0004.00  fshare
0005.00  gshare
0006.00  my share
```

Note: If you specify multiple share names that point to the same integrated server directory, i5/OS saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not include multiple shares that include the same directory or data.

Saving your integrated Windows server files

Use the SAV command to back up your integrated Windows server files.

After you finish the necessary preliminaries (see "Configuring an integrated Windows server for file-level backup" on page 114), you are ready to back up integrated server files on i5/OS. To be able to restore a directory or file by share name, you must specify that file or share name specifically on the SAV command.

Note: To avoid duplicating data, be careful specifying what you want to save on the SAV command. If you specify multiple share names that point to the same directory on the integrated server, i5/OS saves the data multiple times.

To specify what you want i5/OS to save, do this:

1. Ensure that the integrated server is active (described in "Starting and stopping an integrated server" on page 76). Also ensure that the QSYSWRK subsystem, QSERVER, and TCP/IP are active (you can do this by using the Work with Active Jobs (WRKACTJOB) command).
2. On the i5/OS command line, type SAV and press F4.
3. In the Device field, specify the device on which you want i5/OS to save the data. For example, 'QSYS.LIB/TAP01.DEVD' saves the data to tape.
4. In the Object field, specify what you want i5/OS to save in the form '/QNTC/*servername*/*sharename*'. You can use wildcard characters. Refer to "Examples: Saving parts of integrated Windows servers" for how to specify particular parts of the integrated server.
5. Use the Directory subtree field to specify whether you want to save subtrees under a directory. The default is to save all directories.
6. To specify that you want to save changes since the last save, specify *LASTSAVE in the Change period field. You can also specify a specific range of dates and times.
7. Press Enter to save the shares that you specified.

Examples: Saving parts of integrated Windows servers:

These examples show how to use SAV or RST commands for specific parts of an IXS or IXA-attached integrated Windows server.

To save or restore this:	Specify this:
All integrated server objects.	OBJ('/QNTC/*') SUBTREE(*ALL)
All objects for <i>server1</i> .	OBJ('/QNTC/server1/*') SUBTREE(*ALL)
All objects for <i>server1</i> that changed since you last saved the files.	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
All objects for <i>server1</i> that changed during a certain period (in this case between 06/10/2007 and 08/01/2007).	SAV DEV('/bk') OBJ('/qntc/server/share/etc') CHGPERIOD('06/10/2007' *ALL '08/01/2007')

To save or restore this:	Specify this:
All directories, files, and shares to which a particular share (for example, 'fshare') refers. i5/OS does not save and restore the directory over which the share is built.	OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)
Only files to which the specified share (for example, 'fshare') refers that match the specified pattern (pay*). i5/OS does not save directories nor shares.	OBJ('/QNTC/server1/fshare/pay*')
Only directories and shares (no objects) for 'fshare' and its immediate children.	OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)
Directories, shares, and files for 'terry' and its subtrees (not directory 'terry').	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
Only the specific file 'myfile.exe'.	OBJ('/QNTC/server1/gdrive/myfile.exe')
The integrated server registry.	OBJ('/QNTC/server1/\$REGISTRY')

Using the Windows Backup utility on your integrated Windows server

You can use the Windows Backup utility and a System i tape drive to do backups from the integrated Windows server.

See "Using System i tape drives with an integrated Windows server" on page 95.

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.

Restoring the NWSD and disk drives for an integrated Windows server

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 disks for integrated Windows servers" on page 87), 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. For example, enter


```
ADDNWSSTGL NWSSTG(Storage_Name) NWSD(NWSD_Name)
```

at the i5/OS command line.

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 “Restoring integrated Windows server NWSDs” on page 119.

To restore an integrated server’s NWSD and disk drives, do these tasks:

Restoring 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. Ensure that the auxiliary storage pool (ASP) that you are restoring data to is varied on and available.
By default, a storage space that is being restored will be recreated into the ASP from which it was saved. If you want to restore the data to a different ASP than it was saved from, do the following steps.
 - a. Use the Create Network Server Storage Space (CRTNWSSTG) command to create a temporary storage space with the same name as the storage space you are restoring and specify the name of the ASP that you want the data to be restored to.
 - b. Use the following steps to restore the data to the temporary storage space. The restore command will replace the data in the temporary storage space with the data that is being restored.
2. If you are restoring from save media, ensure that you have mounted your media.
3. If there are no network server storage spaces that currently exist on the system (none appear when you use the Work With Network Server Storage Space (WRKNWSSTG) command), you must create the /QFPNWSSTG directory before you can restore network server storage spaces that you saved beneath that directory. To create the /QFPNWSSTG directory, complete these steps:
 - a. On the i5/OS command line, type CRTNWSSTG to create a network server storage space and press F4.
 - b. Provide a name for the storage space.
 - c. Use the minimal size allowed and specify the appropriate disk pool (ASP).
 - d. Press Enter to create the storage space. i5/OS creates the storage space in the /QFPNWSSTG directory.
4. To restore the storage spaces, type RST and press F4.
5. In the Name field under Objects:, specify '/QFPNWSSTG/stgspc'.
To restore the system drive, use /QFPNWSSTG/nwsdname1. To restore the installation drive, use /QFPNWSSTG/nwsdname2.

6. If you are restoring a storage space that resided in a user ASP or an independent ASP and was saved on i5/OS V5R4 or earlier releases, you must also specify the UDFS object. Starting with i5/OS V6R1, the UDFS file is not specified on the save or restore commands since it is automatically included with the storage space directory.

Note: To restore the .UDFS object to an independent disk pool, the disk pool device must be varied on. Specify `dev/independent ASP name/stgspc.UDFS` where *independent ASP name* is the name of the independent disk pool and *stgspc* is the name of the network server storage space.

7. Specify values for any other parameters that you want and press Enter to restore the storage space.
8. You also need to restore any user defined disk drives that are associated with the server and restore the NWSD. When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Note: If the integrated server was installed before V4R5, see Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems in the V5R3 i5/OS Information Center.

Restoring user-defined disk drives for integrated Windows server

Use the Create NWS Storage Space (CRTNWSSTG), Work with NWS Storage Spaces (WRKNWSSTG), and Restore Object (RST) commands to restore storage spaces for your integrated Windows servers.

Although you can now back up individual files and directories (see “Backing up individual integrated Windows server files and directories” on page 113), 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 “Backing up user-defined disk drives for integrated Windows servers” on page 110. 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 “Restoring integrated Windows server NWSDs.” When you are done restoring the NWSD and all its associated disk drives, vary on the integrated server.

Restoring integrated Windows server NWSDs

Use the Restore Configuration (RSTCFG) command to restore the Network Server Description (NWSD) for an integrated Windows server.

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.

1. On the i5/OS command line, type RSTCFG and press F4.
2. In the Objects field, specify the name of the NWSD followed by an '*'. This will restore both objects (NWSD, LIND) that have used the standard naming convention in one pass and in the proper sequence.
3. In the Device field, specify the device name if you are restoring from media. If you are restoring from a save file, specify *SAVF and identify the name and library for the save file in the appropriate fields.
4. Press Enter to have i5/OS restore the NWSD.
5. When you are done restoring the NWSD and all its associated storage spaces, start the integrated server. See "Starting and stopping an integrated server" on page 76.

Restoring integrated Windows server files

Use the Restore (RST) command to restore integrated Windows server files.

IBMi5/OS Integrated Server Support supports file-level backup and recovery of your files. You can recover a particular file from your i5/OS backup without restoring the entire disk drive. Before using this method, however, consider the amount of data you need to restore. For large amounts of data, restoring an entire disk drive object is much faster than restoring all the individual files in the disk drive. To restore a smaller amount of data, this method works great.

You should restore the directory first, then files, then the registry, then reboot for new registry entries to take effect. To restore files that you saved by this method, use the RST command:

1. Ensure that the integrated Windows server and TCP/IP are running.
2. On the i5/OS command line, type RST and press F4.
3. In the Device field, specify the device on which the data is available. (For example, 'QSYS.LIB/TAP01.DEVD' restores the data from tape.)
4. In the Object field, specify what you want i5/OS to restore in the form '/QNTC/servername/sharename'

You can use wildcard characters. Refer to "Examples: Saving parts of integrated Windows servers" on page 116 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.

Uninstalling the Windows server operating system from the integrated server hardware

Uninstall the operating system and delete software related to an integrated Windows server.

You can use the Delete Windows Server (DLTWNTSVR) command to uninstall Windows server from integrated server hardware. Prior to running the Delete Windows Server command, shut down your integrated Windows server from i5/OS. See “Starting and stopping an integrated server” on page 76.

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 “Starting and stopping an integrated server” on page 76.
2. “Unlinking integrated Windows server disk drives” on page 92.
3. “Deleting integrated Windows server disk drives” on page 92.
4. “Deleting the NWSD for an integrated Windows server.”
5. “Deleting line descriptions for integrated Windows servers” on page 122.
6. “Deleting TCP/IP interfaces associated with an integrated Windows server” on page 122.
7. “Deleting controller descriptions associated with integrated Windows servers” on page 122.
8. “Deleting device descriptions associated with an integrated Windows server” on page 123.

If you remove all your Windows and Linux servers from i5/OS and plan not to install any more, you can delete IBM i5/OS Integrated Server Support to free up the storage the product uses. See “Uninstalling IBM i5/OS Integrated Server Support” on page 123.

Deleting the NWSD for an integrated Windows server

Delete Network Server Descriptions (NWSDs) for integrated Windows servers.

Before you delete a network server description (NWSD), you need to unlink its disk drives (see “Unlinking integrated Windows server disk drives” on page 92) and delete storage spaces that are associated with that NWSD (see “Deleting integrated Windows server disk drives” on page 92). 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 i5/OS Information Center.

Deleting line descriptions for integrated Windows servers

Use the Work with Line Description (WRKLIND) command to delete line descriptions for integrated Windows server.

To delete all of an integrated server's line descriptions, follow these steps:

1. On i5/OS, type the command `WRKLIND` and press Enter.
2. Page down until you see the line description that you want to delete.

Note: The name of the line description should be the name of the network server description (NWSD) followed by 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 or V9. This depends on the port number to which you attached it.

3. Place a 4 in the Opt field to the left of the line description and press Enter. Repeat this step for any other line descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the `WRKLIND nwsdname*` command, where `nwsdname` is the name of the associated network server description.

Deleting TCP/IP interfaces associated with an integrated Windows server

Delete the TCP/IP address that are associated with the Network Server Description (NWSD) for an integrated Windows server.

To delete TCP/IP interfaces that are associated with an integrated server, follow these steps:

1. On the i5/OS console, enter the `CFGTCP` command.
2. Choose option 1. Work with TCP/IP interfaces from the Configure TCP/IP menu.
3. Type a 4 in the Opt field next to the TCP/IP interface you want to remove, then press Enter.
You can identify the TCP/IP interfaces that are associated with the network server description (NWSD) by looking at the name of the attached line description. This name consists of the NWSD name, followed by a number.
4. Repeat step 3 for each TCP/IP interface that is associated with the NWSD.

Deleting controller descriptions associated with integrated Windows servers

Use the Work with Controller Descriptions (WRKCTLD) command to delete controller descriptions associated with integrated Windows servers.

To delete all of the controller descriptions for an integrated server, follow these steps:

1. On i5/OS, type the command `WRKCTLD` and press Enter.

2. Page down until you see the controller description that you want to delete.

Note: The name of the controller description starts with the first five characters of the NWSD name, followed by 'NET' and a two-digit number. For example, if the NWSD name is MYSERVER, the controller name might be MYSERVERNET01.

3. Place a 4 in the Opt field to the left of the controller description and press Enter. Repeat this step for any other controller descriptions that are associated with the NWSD.

Note: An alternate method to steps 1 and 2 is to use the WRKCTLD MYSER* command, where MYSER is the first 5 characters of the NWSD name.

Attention: If you use this method, verify that you wish to delete all of the NWSDs on your system that begin with these 5 characters.

Deleting device descriptions associated with an integrated Windows server

Use the Work with Device Descriptions (WRKDEVD) command to 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.

Uninstalling IBM i5/OS Integrated Server Support

If you remove all integrated Windows and non-partition Linux servers from your System i product 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 "Uninstalling the Windows server operating system from the integrated server hardware" on page 121.

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.

Network server description configuration files

You can customize your integrated servers by creating your own configuration files.

NWSD configuration file format

An NWSD configuration file consists of multiple occurrences of **entry types**, each with a different function.

The entry types are:

“Removing lines from an existing integrated server configuration file with CLEARCONFIG entry type” on page 125

Use this entry type if you want to remove all lines from the integrated server file.

“Changing an integrated server file with ADDCONFIG entry type” on page 126

Use this entry type to add, replace, or remove lines in the integrated server file.

“Change an integrated server file with UPDATECONFIG entry type” on page 130

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 132

Use this entry type to set the default values for certain keywords. i5/OS uses the defaults only when processing ADDCONFIG and UPDATECONFIG entries in the current file member.

An **entry** is one occurrence of an entry type. Each entry contains a series of keywords that are followed by equal signs (=) and values for those keywords.

Format guidelines

- Source physical file record length must be 92 bytes.
- A line can have only one entry, but an entry can occupy multiple lines.
- You can use blank spaces between the entry type and the keyword, around the equal sign, and after the commas.
- You can use blank lines between entries and between keywords.

Keywords

- You can put entry keywords in any order.
- Use a comma after all keyword values except the last one in the entry.
- Enclose keyword values in single quotation marks if they contain commas, blank spaces, asterisks, equal signs, or single quotation marks.
- When you use keyword values that contain single quotation marks, use two single quotation marks to represent a quotation mark within the value.
- Keyword value strings can have a maximum length of 1024 characters.
- Keyword values can span lines, but you must enclose the value in single quotation marks. The value includes leading and trailing blanks in each line.

Comments

- Begin comments with an asterisk (*).
- You can put a comment on its own line or on a line with other text that is not part of the comment.

Creating an NWSD configuration file for your integrated server

Create an NWSD configuration file for your integrated server.

Before creating a configuration file, read the topics “NWSD configuration file format” and “Use substitution variables for keyword values” on page 134. You might also want to read “Example: NWSD configuration file for an integrated server” on page 125.

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 124. For example, you can use the Work with members using PDM (WRKMBRPDM) command:
 - a. At the i5/OS command line, type WRKMBRPDM file(yourfilename) mbr(mbrname) and press Enter.
 - b. Type 2 next to the file you want to edit.

Example: NWSD configuration file for an integrated server

This example shows some basic elements of an NWSD configuration file.

This example configuration file:

- Sets a default file path
- Deletes the time zone and uses a configuration variable to add it back
- Sets default search values that cause the display configuration lines to be added before the UserData section
- Adds lines that configure the display

```
+-----+
| ***** Beginning of data ***** |
| ***** |
| * Update D:\UNATTEND.TXT |
| ***** |
| * |
| *===== |
| * Set default directory and file name values. |
| *===== |
| SETDEFAULTS TARGETDIR = 'D:\', TARGETFILE = 'UNATTEND.TXT' |
| * |
| *===== |
| * Delete and use a substitution variable to re-add TimeZone line. |
| *===== |
| ADDCONFIG VAR      = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS' |
| ADDCONFIG ADDSTR   = 'TimeZone="%TIMEZONE%"', |
| FILESEARCHSTR      = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%' |
| * |
| * Add lines to configure the display. |
| *===== |
| * Set default search values to add new statements to the file |
| * before the UserData section header line. |
| SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%', |
| FILESEARCHPOS = 'BEFORE' |
| * |
| * Add the display statements to the file. |
| ADDCONFIG ADDSTR = '%FPA_L_BRACKET%Display%FPA_R_BRACKET%', |
| UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'ConfigureAtLogon = 0', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'BitsPerPel = 16', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'XResolution = 640', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'YResolution = 480', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'VRefresh = 60', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'AutoConfirm = 1', UNIQUE = 'YES' |
| * |
+-----+
```

Removing lines from an existing integrated server configuration file with CLEARCONFIG entry type

You can use the CLEARCONFIG entry type to remove all lines from an existing integrated server file.

Attention: Removing all lines from the integrated server file may result in your being unable to vary on the network server.

To clear an integrated server file, create an NWSD configuration file that contains the CLEARCONFIG entry type as follows.

```
CLEARCONFIG
  LINECOMMENT = '<"REM "|<comment_string>>',      (optional)
  TARGETDIR   = '<BOOT|path>',                    (optional)
  TARGETFILE  = '<file_name>',                     (required)
```

For a detailed explanation of the CLEARCONFIG keywords, use the following keyword links. You can also go back to “NWSD configuration file format” on page 124, or on to “Changing an integrated server file with ADDCONFIG entry type.”

- “LINECOMMENT keyword” on page 128
- “TARGETDIR keyword”
- “TARGETFILE keyword”

TARGETDIR keyword

Use TARGETDIR to specify the path for the integrated server file to be cleared.

Note: When changing a file, i5/OS uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword

Use TARGETFILE to specify the integrated server file to be cleared.

Changing an integrated server file with ADDCONFIG entry type

Use the ADDCONFIG entry type to change an existing integrated server Network Server Description (NWSD) configuration file.

You can use the ADDCONFIG entry type to change an integrated server file in these ways:

- Add a line to the beginning or end of the file.
- Add a new line before or after a line that contains a specific string.
- Delete a line in the file.
- Replace the first, last, or all occurrences of a line in the file.
- Specify in which directory to change the file.

To change an integrated server file, create an NWSD configuration file that contains the ADDCONFIG entry type as follows:

```
ADDCONFIG
  VAR           = '<variable_name>',              (conditionally required)
  ADDSTR        = '<line to process>',              (optional)
  ADDWHEN       = '<ALWAYS|NEVER|<expression>>',    (optional)
  DELETEWHEN    = '<NEVER|ALWAYS|<expression>>',    (optional)
  LINECOMMENT   = '<"REM "|<comment_string>>',      (optional)
  LOCATION      = '<END|BEGIN>',                    (optional)
  FILESEARCHPOS = '<AFTER|BEFORE>',                  (optional)
  FILESEARCHSTR = '<search_string>',                  (conditionally required)
  FILESEARCHSTROCC = '<LAST|FIRST>',                  (optional)
  REPLACEOCC    = '<LAST|FIRST|ALL>',                 (optional)
  TARGETDIR     = '<BOOT|path>',                      (optional)
  TARGETFILE    = '<CONFIG.SYS|<file_name>>',        (optional)
  UNIQUE       = '<NO|YES>',                          (optional)
```

For a detailed explanation of the ADDCONFIG keywords, use the following keyword links. You can also go back to “NWSD configuration file format” on page 124 or on to the “Change an integrated server file with UPDATECONFIG entry type” on page 130.

VAR keyword

VAR specifies the value on the left side of the equal sign that identifies the line you want to add to or delete from the file.

For example:

```
ADDCONFIG
VAR = 'FILES'
```

i5/OS requires the keyword if you do not specify REPLACEOCC,

ADDSTR keyword

Use ADDSTR to specify the string that you want to add to the integrated server Network Server Description (NWSD) configuration file.

For example:

```
ADDCONFIG
VAR = 'FILES'
ADDSTR = '60'
```

ADDWHEN keyword

Use ADDWHEN to specify when during processing you want i5/OS to add the new line or string to the Network Server Description (NWSD) configuration file for an integrated server.

You can specify:

- ALWAYS if you want i5/OS to add the line or string every time it processes the configuration file. (ALWAYS is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- NEVER if you want i5/OS to never add the line or string.
- An expression that directs i5/OS to add the line or string when the specified condition is true. Expressions are composed of operators (see “ADDWHEN and DELETEWHEN expression operators”) and must equate to either TRUE or FALSE.

Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to add a line when the NWSD type is *WINDOWSNT, you might use this:

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

ADDWHEN and DELETEWHEN expression operators:

Use these operators for expressions in the Network Server Description (NWSD) configuration file for an integrated server.

You can use these operators for expressions:

Operator	Description
==	Returns TRUE if operands are equivalent, FALSE if they are not.
!=	Returns FALSE if operands are equivalent, TRUE if they are not.
>	Returns TRUE if the operand on the left is greater than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<	Returns TRUE if the operand on the left is less than the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.

Operator	Description
>=	Returns TRUE if the operand on the left is greater than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
<=	Returns TRUE if the operand on the left is less than or equal to the operand on the right, FALSE if it is not. If the operands are strings, the ASCII values are compared.
&&	Logical AND. Returns TRUE if both operands have a value other than 0. Operands must be integers.
	Logical OR. Returns TRUE if either operand has a value other than 0. Operands must be integers.
+	If the operands are both integers, the result is the sum of the integers. If the operands are both strings, the result is the concatenation of the two strings.
-	Subtracts integers.
*	Multiplies integers.
/	Divides integers.
()	Parentheses force an evaluation order.
!	Logical NOT. Returns TRUE if the value of a single operand is 0. Returns FALSE if it is not 0.
ALWAYS	Always returns TRUE.
NEVER	Always returns FALSE.

DELETEWHEN keyword

Use DELETEWHEN to specify when during processing you want i5/OS to delete a line or string from the Network Server Description (NWSD) configuration file for an integrated server.

You can specify:

- ALWAYS if you want i5/OS to delete the line or string every time it processes the configuration file.
- NEVER if you want i5/OS to never delete the line or string. (NEVER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member)
- An expression that directs i5/OS to delete the line or string when the specified condition is true. Expressions are composed of operators (see “ADDWHEN and DELETEWHEN expression operators” on page 127) and must equate to either TRUE or FALSE.

Note: If you do not want i5/OS to interpret an expression (such as one that contains an asterisk (*)) as a mathematical operation, enclose the expression in quotation marks. For example, to delete a line when the NWSD type is *WINDOWSNT, you can use this:

```
DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

LINECOMMENT keyword

LINECOMMENT specifies the prefix string that identifies comments in a Network Server Description (NWSD) configuration file for an integrated server.

Use the default value if you want LINECOMMENT to use 'REM' to identify comments. You can specify a different value. For example, to use a semicolon to identify comments, use LINECOMMENT = ';' within the **first** entry that refers to that file. (i5/OS ignores the LINECOMMENT keyword on any other entry.)

LOCATION keyword

LOCATION specifies where in the file to add the new line in a Network Server Description (NWSD) configuration file for an integrated server.

The default value END directs i5/OS to add the line at the end of the file. If you want i5/OS to add the line at the beginning of the file, specify BEGIN.

LINESEARCHPOS keyword

Use LINESEARCHPOS to specify whether to add the string you specify with the ADDSTR keyword value AFTER (the default) or before the line search string.

e

LINESEARCHSTR keyword

Specifies the string to search for within the lines.

Note: Only the right side of the equal sign is searched for the LINESEARCHSTR value.

LINELOCATION keyword

Use LINELOCATION to specify where in the line to add the string that you specify with the ADDSTR keyword value.

Use the default value of END if you want i5/OS to add the string at the end of the line. If you want i5/OS to add the string at the beginning of the line instead, specify BEGIN.

FILESEARCHPOS keyword (ADDCONFIG entry type)

Specify where to locate a line relative to the file search string. You can specify:

- AFTER if you want i5/OS to add the line after the line that contains the file search string. (AFTER is the default unless you defined a different default value by using a SETDEFAULTS entry in the member.)
- BEFORE if you want i5/OS to add the line before the line that contains the search string.

FILESEARCHSTR keyword

Use FILESEARCHSTR with the REPLACEOCC keyword to specify the line to replace. You must specify the entire line as the value.

When you are adding a new line, FILESEARCHSTR can be any part of a line you want to find.

There is no default value, unless you defined a default value by using a SETDEFAULTS entry in the member.

FILESEARCHSTROCC keyword

Specifies which occurrence of a string that appears multiple times in the file to use for positioning the new line.

The default value of LAST specifies the last occurrence of the search string. If you want i5/OS to use the first occurrence of the search string, specify FIRST.

REPLACEOCC keyword

Specifies which occurrence of a line you want to replace:

- Use LAST if you want i5/OS to replace the last occurrence of the FILESEARCHSTR.
- Use ALL if you want i5/OS to replace all occurrences of the FILESEARCHSTR.
- Use FIRST if you want i5/OS to replace the first occurrence of the FILESEARCHSTR.

Use FILESEARCHSTR to specify the entire line that you want to replace.

i5/OS deletes the line that matches the FILESEARCHSTR and adds the specified VAR and ADDSTR to the file at this location.

Note: REPLACEOCC has precedence over LOCATION and FILESEARCHPOS. If i5/OS does not find the FILESEARCHSTR value used with a REPLACEOCC keyword, it adds a new line based on the value of the LOCATION keyword but does not replace a line.

TARGETDIR keyword

Use TARGETDIR to specify the path for the integrated server file to be changed.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify the path for UNATTEND.TXT or your own integrated server file. (This keyword defaults to BOOT, which directs i5/OS to change the file in the root directory of the C drive.)

Notes:

1. Support for NWSD configuration files exists only for predefined disk drives that are formatted as FAT. Storage spaces that are converted to NTFS are not accessible for configuration files.
2. When changing a file, i5/OS uses only the first directory for that file. It ignores any other entries that specify a different target directory.

TARGETFILE keyword

TARGETFILE specifies the integrated server file to be changed. The value of UNATTEND.TXT directs i5/OS to change the integrated server unattended install setup script file.

Unless you first use a SETDEFAULTS entry to change the default, you need to specify UNATTEND.TXT or your own integrated server file. (This keyword defaults to CONFIG.SYS.)

UNIQUE keyword

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 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 “NWS configuration file format” on page 124 or on to “Set configuration defaults with the SETDEFAULTS entry type” on page 132.

- “VAR keyword” on page 127
- “ADDSTR keyword” on page 127
- “ADDWHEN keyword” on page 127
- “DELETEWHEN keyword” on page 128
- “LINECOMMENT keyword” on page 128
- “LINELOCATION keyword” on page 129
- “LINESEARCHPOS keyword” on page 129
- “LINESEARCHSTR keyword” on page 129
- “FILESEARCHPOS keyword (UPDATECONFIG entry type)”
- “FILESEARCHSTR keyword (UPDATECONFIG entry type)”
- “FILESEARCHSTROCC keyword (UPDATECONFIG entry type)” on page 132
- “TARGETDIR keyword” on page 130
- “TARGETFILE keyword” on page 130
- “VAROCC keyword” on page 130
- “VARVALUE keyword” on page 130

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” on page 133
- “FILESEARCHPOS keyword (SETDEFAULTS entry type)” on page 133
- “FILESEARCHSTR keyword (SETDEFAULTS entry type)” on page 133
- “TARGETDIR” on page 133
- “TARGETFILE” on page 133

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 127) 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 = '(%FPAWSDTYPE%=="*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 127) 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 = '(%FPAWSDTYPE%=="*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) *
%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
%FPASYSDDRIVE%	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

Substitution variable	Description
%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('Configuration file variables')
```

The member 'nwsdname' contains data in fixed columns formatted as:

- A variable name in column 1-15 padded with blanks and
- A value that starts in column 16

For example:

```
Columns:
12345678901234567890123456789012345678901234567890...
myaddr      9.5.9.1
```

where %myaddr% is added to the list of available substitution variables and has a value of "9.5.9.1".

Appendix. Notices

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
BladeCenter
DB2
IBM
iSeries
Netfinity
NetServer
i5/OS
Redbooks
ServerGuide
System i
System x
xSeries

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Pentium is a trademark or a registered trademark of Intel Corporation in the United States, other countries, or both.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, 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